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.

selbe Staat, der für die Informationssicherheit verantwortlich ist, hat also Schwachstellen in den für das Funktionieren von Staat und Gesellschaft wesentlichen Informationsinfrastrukturen generiert und genutzt – mit anderen Worten: er hat die IT-Sicherheit kompromittiert –, um seine Aufgabe der allgemeinen Sicherheitsgewährleistung wahrzunehmen. Das Informationssicherheitsrecht wird auf diese Weise zur Arena gegenläufiger Sicherheitskonzepte und -interessen.[41]

Die Ambivalenz der Thematik beschränkt sich nicht auf den staatlichen Innenbereich. Vielmehr ist der „Cyber- und Informationsraum" – so der Sprachgebrauch der Bundeswehr – bzw. die „Cyberdomain" – so der Jargon der U.S. Army – im Zuge der allgemein steigenden geopolitischen Differenzen zu einem hochaktiven Feld der außenpolitischen Auseinandersetzung geworden.[42] Das Spektrum an Beeinträchtigungen reicht von Online-Desinformationskampagnen bis hin zu internetbasierten Angriffen auf physische Ziele wie kritische Infrastrukturen.[43] Die Tatsache, dass in der Praxis oftmals nicht erkennbar ist, wer Urheber einer konkreten Bedrohungslage ist – ob staatlicher oder privater Akteur –, stellt dabei grundlegende Annahmen des (Völker-)Rechts über die Zuschreibung von Verantwortlichkeit in Frage.[44] Infolgedessen wird auch das Außenwirtschaftsrecht zunehmend zur Arena der Informationssicherheitspolitik.[45] Denn angesichts des komplexen und globalen Ökosystems digitaler Technologien bekommt die Frage, wer wo IT-sicherheitsrelevante Produkte oder Dienstleistungen anbieten darf und wie die maßgeblichen Lie-

[41] Hierzu im Überblick *Dunn Cavelty/Egloff*, The Politics of Cybersecurity: Balancing Different Roles of the State, St Antony's Int'l Rev. 15 (2019), S. 37 (48), die drei Phasen unterscheiden: in den 1980er-Jahren ist der Staat als „owner" der gefährdeten Netzwerke betroffen; in den 1990er-Jahren rückt der Staat als „problem owner" in die Rolle des Garanten für Informationssicherheit ein; ab etwa 2000 tritt der Staat in Form seiner Sicherheitsbehörden zunehmend als „originator of the problem" auf. Zum staatlichen Umgang mit Schwachstellen siehe ausführlich unten § 7.

[42] Siehe neben den in § 1 Fn. 17, 22 und 31 angeführten Dokumenten auch *M. Knoll*, Streitkräfteeinsatz zur Verteidigung gegen Cyberangriffe, 2020, S. 20, 37 ff.

[43] Eine Rekonstruktion der strategischen Interessen, die hinter den aggressiven Praktiken zahlreicher Staaten im Cyberraum stehen, findet sich bei *B. Buchanan*, The Cybersecurity Dilemma, 2017.

[44] Zum sog. Attributionsproblem ausführlich unten § 4 II. 2. b). Zur Reaktion der Europäischen Union in Gestalt der Schlussfolgerungen des Rates zu einem Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten („Cyber Diplomacy Toolbox") v. 19.6.2017 (10474/17), die eng mit dem Sanktionsregime (siehe dazu auch unten § 2 Fn. 29) verzahnt ist, ausführlich *Miadzvetskaya/Wessel*, The Externalisation of the EU's Cybersecurity Regime, European Papers 7 (2022), S. 413 (427 ff.).

[45] Vgl. Art. 4 Abs. 1 VO (EU) 2019/452 vom 19.3.2019 zur Schaffung eines Rahmens für die Überprüfung ausländischer Direktinvestitionen in der Union (EU-Screening-Verordnung). Siehe vertiefend *H. Lin/J. Trachtman*, Diagonal Export Controls to Counter Diagonal Transnational Attacks on Civil Society, EJIL 31:3 (2020), S. 917 ff.; *G. Gagliani*, Cybersecurity, Technological Neutrality, and International Trade Law, Journal of International Economic Law 23:3 (2020), S. 723 ff.

ferketten strukturiert sind, eine hohe politische Bedeutung. Dies gilt nicht nur für den Aufbau zukunftsfähiger Telekommunikationsnetze (5G), sondern allgemein für Hard- und Softwarekomponenten, cloudbasierte Dienste, Künstliche Intelligenz (KI) etc.[46]

IV. Informationssicherheit als Herausforderung für Recht und Rechtswissenschaft

Die in diesem Feld entstehende Rechtsmaterie verdient schon deswegen wissenschaftliche Aufmerksamkeit, weil sie von zahlreichen, bisher nur teilweise befriedigend gelösten normativen Spannungslagen durchzogen ist. Altbekannt ist die Frage, wie sich funktionierende Datensicherheit und guter Datenschutz vereinbaren lassen.[47] Noch weitgehend ungeklärt ist hingegen, wie darauf zu reagieren ist, dass die traditionellen juristischen Mechanismen der Verantwortungszuschreibung im digitalen Raum weitgehend versagen, weil sich für Attacken oft kein Urheber identifizieren lässt.[48] Offen ist ferner, wie gut die rechtlichen Vorgaben in der Praxis tatsächlich umgesetzt werden. Vor allem aber nötigt die ambivalente Rolle des Staates, der als Garant der Informationssicherheit auftritt, zugleich aber in Form seiner Sicherheitsbehörden ein Interesse an niedrigen Sicherheitsstandards hat, zur Reflexion.

Es erstaunt daher, dass das IT-Sicherheitsrecht, was den wissenschaftlichen Grad seiner Durchdringung betrifft, klar hinter Materien wie dem Informationsverwaltungs-, dem Datenschutz- oder dem E-Government-Recht zurückbleibt. Zwar existieren mittlerweile Untersuchungen zu einzelnen Sektoren, etwa zur Informationssicherheit der Betreiber kritischer Infrastrukturen. Doch fehlt es an einer umfassenden Perspektive auf die Materie, welche die einzelnen Stränge der Diskussion zusammenführt, vermisst und ordnet. Dies ist das *erste Ziel*, dessen sich die vorliegende Arbeit annimmt.

Die Befassung mit der Materie erscheint *zweitens* auch unter übergeordneten Gesichtspunkten wissenschaftlich lohnend. Mehr noch als in anderen Feldern des Rechts der Digitalisierung stellt sich hier die Frage, wie es gelingen soll, für diese bislang weitgehend privat organisierte, stark von den Eigenge-

[46] Zur 5G-Problematik siehe *Europäische Kommission*, Empfehlung zur Cybersicherheit von 5G-Netzen, C/2019/2335; *NIS Cooperation Group*, Cybersecurity of 5G networks. EU Toolbox of risk mitigating measures, 29.1.2020 („5G Toolbox"); *Europäische Kommission*, Mitteilung: Sichere 5G-Einführung in der EU – Umsetzung des EU-Instrumentariums, COM(2020) 50. Aus rechtswissenschaftlicher Sicht *M. Varju*, 5G Networks, (Cyber)security Harmonisation and the Internal Market, European L. Rev. 45 (2020), S. 471 ff. Zur Diskussion um eine „Lex Huawei" im IT-SiG 2.0 (§ 9b BSIG; § 165 Abs. 4 TKG; § 55a Abs. 1 Nr. 1 und 2 AWV) siehe unten § 6 II. 4. c) bb). und § 6 II. 6. b).

[47] Siehe unten § 5 I. 1. b).

[48] Zum Problem näher unten § 4 II. 2. b) und § 6 II. 4.

setzlichkeiten der Technik geprägte und, jedenfalls in Teilbereichen, inhärent global strukturierte Konstellation rechtliche Ordnungsstrukturen zu etablieren.[49] Zwar wird allgemein darauf hingewiesen, dass auch die digitale Technik in Objekten – Kabeln, Rechnern, Nutzern – wurzelt, der vom Recht beherrschte physische Raum seine Bedeutung als Medium von Herrschaft also nicht ganz verloren hat. Aber auch die Herrschaft über das „Physische" des Digitalen bedarf eines spezialisierten Wissens und entsprechender Fähigkeiten, über die Staaten bisher nur in Ansätzen verfügen. Aktuell jedenfalls ist nicht gesichert, dass sich der staatliche Steuerungsanspruch in Gestalt des von ihm gesetzten Rechts gegenüber dem – immer stärker konzentrierten[50] – privaten Sektor durchsetzen kann.[51] Die Analyse der Verrechtlichungsprozesse zur Bewältigung von Informationssicherheitsrisiken auf staatlicher und überstaatlicher Ebene berührt damit grundsätzliche Herausforderungen rechtsstaatlich verantworteter Regulierung unter den Bedingungen der Digitalisierung und Globalisierung.

Mit diesem Befund verknüpft ist eine *dritte* Problemebene. Sicherheitsgewährleistung ist traditionell eine Kernfunktion von Staatlichkeit, zentraler Rechtfertigungsgrund für staatliche Herrschaft und Hauptindikator für staatliche Souveränität. Im Verfassungsstaat ist die Gewährleistung von Sicherheit in staatliche Institutionen eingebettet und durch Recht geleitet. Private spielen zwar eine wichtige Rolle bei deren Ausgestaltung, handeln jedoch stets im Rahmen der hoheitlichen Ordnung.[52] Der Staat hat sich diese Stellung als primärer Sicherheitsgarant historisch erkämpft, auch wenn er sich heute bei der Wahrnehmung der damit verbundenen Aufgaben in Form der Verfassung selbst Zügel anlegt. Im digitalen Raum stößt dieser Anspruch des Staates jedoch an enge Grenzen. Hier kann der Staat aus im Einzelnen noch zu erör-

[49] Nicht weiter thematisiert wird im Folgenden die Frage, ob und inwieweit durch den Aufstieg der Informationstechnologie das Konzept rechtlicher Ordnung an sich herausgefordert wird, vgl. dazu grundlegend *K.-H. Ladeur*, Computerkultur und Evolution der Methodendiskussion in der Rechtswissenschaft, ARSP 74 (1988), S. 218 ff.; *ders.*, Die Textualität des Rechts, 2015, S. 306 ff.; *T. Vesting*, Die Medien des Rechts: Computernetzwerke, 2015. Allgemein zum Zusammenhang zwischen den Kategorien des Rechts und dem „medialen *environment*" *T. Vesting*, Rechtstheorie, 2. Aufl. 2015, S. 89.

[50] Zu den Konzentrationstendenzen der Internetwirtschaft als Herausforderung für die Informationssicherheit siehe die Beiträge in der Special Issue „Consolidation of the Internet" des Journal of Cyber Policy, insbes. *D. Geer/E. Jardine/E. Leverett*, On market concentration and cybersecurity risk, Journal of Cyber Policy 5:1 (2020), S. 9 ff. Aufgegriffen auch durch *Europäische Kommission/Hoher Vertreter der Union für Außen- und Sicherheitspolitik*, Die Cybersicherheitsstrategie der EU für die digitale Dekade, JOIN(2020) 18 final, unter I.

[51] Zur Leistungsfähigkeit des Rechts im Umgang mit der (Informations-)Technik siehe unten § 3. Zum Wissensproblem und zur Globalisierung als Herausforderungen für das Recht der Informationssicherheit siehe unten § 6 II. 2. und § 6 II. 3.

[52] *C. Gusy*, Vom Polizeirecht zum Sicherheitsrecht, Staatswissenschaft und Staatspraxis 5 (1994), S. 187 ff.; *G. Nitz*, Private und öffentliche Sicherheit, 2000. Weiter dazu unten § 4 I.

ternden Gründen nicht – oder jedenfalls nicht ohne private Unterstützung – jene Leistungen erbringen, die in der „analogen" Welt seine herausgehobene Position im realen Gewaltengefüge begründen. Der strukturelle Bedarf nach Sicherheit bleibt bei alldem aber mindestens konstant. Agiert der Staat nicht, treten andere ein. Schon jetzt ist ein bemerkenswertes Ungleichgewicht an technologischen Fähigkeiten zwischen einzelnen privaten Akteuren und vor allem kleineren und mittleren Staaten zu beobachten.[53] So übernehmen im Bereich Informationssicherheit Private nicht nur faktisch die Aufgabe der Sicherheitsgewährleistung, sondern werden vermehrt auch selbst als „norm entrepreneurs" tätig.[54] Teilweise wird daher bereits die Disruption einer staatlichen Kernfunktion diagnostiziert.[55] In jedem Fall verschieben sich Machtstrukturen, und Rechtfertigungsfragen müssen neu gestellt werden. Diese Zusammenhänge bilden den staatstheoretischen Horizont der Frage nach der Regulierung von Informationssicherheit.

Vor vorschnellen Schlüssen ist allerdings bereits an dieser Stelle zu warnen. Der pauschale Befund vom Verlust „digitaler Souveränität" – eine neue Variante der These von der „Krise regulativer Politik" – greift zu kurz.[56] Vielmehr haben Staaten, wie berichtet, die Bedeutung der Materie mittlerweile durchaus erkannt. Hinreichende Fähigkeiten zur aggressiven und defensiven Nutzung von Informationstechnologie gelten heute als wesentlicher Bestandteil staatlicher Macht – von „Cyberpower".[57] Cybersicherheit spielt daher auch in den politischen Sicherheitsstrategien eine zentrale Rolle.[58]

---

[53] *K. Bannelier/T. Christakis*, Cyber-Attacks – Prevention-Reactions, 2017, S. 10 und passim.

[54] *L. Hurel/L. Lobato*, Unpacking Cyber Norms, Journal of Cyber Policy 3:1 (2018), S. 61 ff.; *N. Katagiri*, Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks, Journal of Cybersecurity 7:1 (2021), S. 1 ff.

[55] In diese Richtung *L. Kello*, The Virtual Weapon and International Order, 2017, S. 229 ff., der vom „sovereignty gap" spricht.

[56] Zum wenig konturierten Diskurs um „digitale Souveränität" siehe nur die verschiedenen Perspektiven bei *J. Pohle/T. Thiel*, Digital Sovereignty, Internet Policy Review 9:4 (2020), S. 1 ff.; *C. Ernst*, Der Grundsatz digitaler Souveränität, 2020; *BMWi*, Schwerpunktstudie Digitale Souveränität, 2021. Zum davon zu unterscheidenden (allerdings ebenfalls diffusen) Konzept der „Datensouveränität" siehe *G. Hornung/S. Schomberg*, Datensouveränität im Spannungsfeld zwischen Datenschutz und Datennutzung, CR 2022, S. 508 ff. Zur wirkmächtigen These von der Krise regulativer Politik vgl. nur die Hinweise bei *A. Voßkuhle*, Neue Verwaltungsrechtswissenschaft, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 3. Aufl. 2022, § 1 Rn. 10.

[57] Zu diesem Konzept und seinen Bestandteilen einflussreich *J. Nye*, The Future of Power, 2011, S. 113 ff. Zur Cybersicherheit aus Sicht der Theorie der Internationalen Beziehungen umfassend *Kello*, The Virtual Weapon and International Order, 2017. Siehe dazu auch unten § 4 II. 1. b).

[58] Siehe neben den oben in § 1 Fn. 17, 22 und 31 angeführten Dokumenten auch *Europäische Kommission*, Gestaltung der digitalen Zukunft Europas, COM(2020) 67 final. Die „Neue strategische Agenda 2019–2024" des Europäischen Rats räumt Maßnahmen zur Stär-

Gleiches gilt für die pessimistische Annahme, das Recht sei der Technik ausgeliefert oder auf eine „katechontische" Funktion beschränkt.[59] Derartige Diagnosen verkennen die Kontingenz und Plastizität technischer Entwicklungsprozesse und unterschätzen die Fähigkeit des Rechts zur Einhegung der Technik. Sie verkürzen Recht auf Verbote und Strafnormen und übersehen, dass Recht durch Institutionen, Verfahren oder Anreize einen Rahmen schaffen kann, um staatliche und gesellschaftliche Abwehrkräfte zu aktivieren. Diesen Leistungen, die staatliches Recht auch im Bereich der Informationssicherheitsgewährleistung erbringen kann, wird daher im Folgenden besondere Aufmerksamkeit gelten.

Den soeben aufgeworfenen theoretischen und dogmatischen Fragen will die vorliegende Untersuchung nachgehen. Ihr Anliegen ist es, die unterschiedlichen Teilstränge der Diskussion zusammenzuführen und die Grundlagen eines Rechts der Informationssicherheit zu erarbeiten. Getragen ist das Projekt von der Überzeugung, dass die Gewährleistung von Informationssicherheit zentrale Bedeutung für die Informationsordnung hat und dass dem Informationsrecht ohne Einbeziehung der entsprechenden Rechtsmaterie eine entscheidende Dimension fehlt.

---

kung der Informationssicherheit ebenfalls eine hohe strategische Priorität ein. Für die USA: *V. Weber*, Linking Cyber Strategy with Grand Strategy, Journal of Cyber Policy 3 (2018), S. 236 ff.

[59] In diese Richtung noch *B. Schlink*, Die Bewältigung der wissenschaftlichen und technischen Entwicklungen durch das Verwaltungsrecht, in: VVDStRL 48 (1990), S. 235 (259); kritisch hierzu bereits *E. Schmidt-Aßmann*, Das allgemeine Verwaltungsrecht als Ordnungsidee, 2. Aufl. 2006, 1/32; vgl. auch *A. Taeihagh/M. Ramesh/M. Howlett*, Assessing the regulatory challenges of emerging disruptive technologies, Regulation & Governance 15 (2021), S. 1009 ff. Spezifisch für Cybersicherheit *Katagiri*, Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks, Journal of Cybersecurity 7:1 (2021), S. 1. Ausführlich hierzu unten § 3 II.

§ 2 Recht der Informationssicherheit – Annäherungen an einen regulatorischen Diskurs

> „Cyber security is the suite of practices, processes and policies that have emerged to counter less desirable outgrowths of the global information society."[1]

Die vorliegende Untersuchung zum Recht der Informationssicherheit ist Teil einer Literatur zum Verhältnis von Recht und Digitalisierung, die derzeit Hochkonjunktur hat.[2] Im Fokus entsprechender Untersuchungen aus der Perspektive des Öffentlichen Rechts stehen bislang die *Folgen*, die der Einsatz digitaler Technik für die Rechtsordnung mit sich bringt – sei es, dass neue Güter entstehen, die zugeordnet und verteilt werden müssen, oder dass neue Grundrechtseingriffe rechtlich eingehegt werden müssen. Die *Voraussetzungen*, auf denen die technische Entwicklung beruht, werden weit seltener thematisiert.[3] Dies gilt auch für die Informationssicherheit.[4] Wenn überhaupt nimmt die Li-

[1] *T. Stevens*, Cybersecurity and the Politics of Time, 2016, S. 3.

[2] Vgl. nur aus jüngster Zeit die Habilitationsschriften von *N. Marsch*, Das europäische Datenschutzgrundrecht, 2018; *L. Specht*, Diktat der Technik, 2019; *E. Peuker*, Verfassungswandel durch Digitalisierung, 2020; *C. Krönke*, Öffentliches Digitalwirtschaftsrecht, 2020; *P. Hacker*, Datenprivatrecht, 2020; *J. Eichenhofer*, e-Privacy, 2021.

[3] Eine wichtige Ausnahme ist das Telekommunikationsrecht, das jedoch mit den Leitzielen der Wettbewerbsförderung, des Infrastrukturaufbaus und der angemessenen Versorgung (vgl. § 1 Abs. 1 TKG; Art. 1 Abs. 2 EKEK) eine ganz andere Stoßrichtung als das Informationssicherheitsrecht hat.

[4] Der lange zersplitterte Diskurs hat jüngst in Form verschiedener Praxishandbücher eine erste Konsolidierung erfahren, vgl. D. Gabel/T. Heinrich/A. Kiefner (Hrsg.), Rechtshandbuch Cyber-Security, 2019; *P. Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022; G. Hornung/M. Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021; D.-K. Kipker (Hrsg.), Cybersecurity, 2020; S. Ritter (Hrsg.), Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2022; U. Schläger/J.-C. Thode (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, 2022. In diesen Werken steht die Darstellung des geltenden Rechts ganz im Vordergrund; eine umfassende Bestimmung der regulatorischen Aufgabe und eine dogmatische Durchdringung der regulatorischen Strukturen findet sich nur in Ansätzen. Auch das einschlägige monographische Schrifttum zum Informationssicherheitsrecht konzentriert sich bislang meist nur auf einzelne Facetten der Problematik, insbesondere auf die grundrechtliche Dimension, bzw. auf einzelne Sektoren und Anwendungsfelder, vgl. insbes. *C. Freimuth*, Gewährleistung der IT-Sicherheit Kritischer Infrastrukturen, 2018; *H. Leisterer*, Internetsicherheit in Europa, 2018; *S. Leuschner*, Sicherheit als Grundsatz, 2018; *A. Schmid*, IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme, 2019.

teratur hier zu Einzelfragen Stellung. Um einen Eindruck vom Stand dieser Forschung zu vermitteln, sollen zunächst vier Spezialdiskurse, die je einzelne Facetten des Problems ausleuchten, zusammengeführt und kurz dargestellt werden (I.). In einem zweiten Schritt ist die in den Einzeldiskursen oft unterschiedlich verwendete Begrifflichkeit zu konsolidieren und der hier gewählte Begriffsgebrauch zu rechtfertigen (II.). Auf die Skizze des Gangs der weiteren Darstellung (III.) folgen abschließend Anmerkungen zu den methodischen Herausforderungen des Themas (IV.).

I. Bestandsaufnahme: Vier Schlaglichter

1. Informationssicherheit im Informationsverwaltungsrecht und im Recht des E-Government

Seit den 1990er-Jahren sind die durch den Einsatz digitaler Technik motivierten Transformationsprozesse von Staat und Verwaltung in der Wissenschaft vom öffentlichen Recht in zwei sehr unterschiedlichen Diskursen analysiert worden: in der sich primär als Projekt der Wissenschaft verstehenden Literatur zum sogenannten Informationsverwaltungsrecht und in der eher anwendungsorientierten Literatur zum E-Government.[5]

Das Schrifttum zum Informationsverwaltungsrecht zielt darauf, die informationellen Beziehungen zwischen Staat und Bürgern sowie zwischen verschiedenen Hoheitsträgern theoretisch und dogmatisch zu erfassen.[6] Die Untersuchungsgegenstände reichen von der informationellen Dimension des Ver-

[5] Zu den Ursprüngen des Informatisierungsdiskurses in der Verwaltungsrechtswissenschaft umfassend *A.-B. Kaiser*, Die Kommunikation der Verwaltung, 2009, S. 243 ff. (insbes. 259 f.).

[6] Rechtsdogmatischer und -theoretischer Zugriff bedingen und ergänzen dabei einander. Auf ersterem liegt der Fokus etwa im grundlegenden Beitrag von *R. Pitschas*, Allgemeines Verwaltungsrecht als Teil der öffentlichen Informationsordnung, in: Hoffmann-Riem/Schmidt-Aßmann/Schuppert (Hrsg.), Reform des Allgemeinen Verwaltungsrechts, 1993, S. 219 (242), der ebenda das Informationsverwaltungsrecht als Gesamtheit der öffentlichrechtlichen Normen definiert, die „sich auf den staatlichen Umgang mit Informationen und Kommunikationshandeln beziehen und die das Informationsverhalten der Behörden untereinander sowie gegenüber den Bürgern regeln"; vgl. weiter auch mit je eigenen Akzenten *Schmidt-Aßmann*, Das allgemeine Verwaltungsrecht als Ordnungsidee, 2. Aufl. 2006, 6/7 ff.; *A. Voßkuhle*, Der Wandel von Verwaltungsrecht und Verwaltungsprozeßrecht in der Informationsgesellschaft, in: Hoffmann-Riem/Schmidt-Aßmann (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, 2000, S. 349 (355 ff.); *J. Masing*, Transparente Verwaltung, in: VVDStRL 63 (2004), S. 377 (432 ff.); *E. Gurlit*, Informationsverwaltungsrecht, DV 44 (2011), S. 75 f. Vorrangig am „Paradigmenwechsel" weg von einer handlungs- und hin zu einer informationsorientierten Perspektive interessiert sind demgegenüber etwa *I. Augsberg*, Informationsverwaltungsrecht, 2014; *T. Vesting*, Information und Kommunikation, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 3. Aufl. 2022, § 20 Rn. 6 und passim. Nochmals anders zu den Folgen der medialen Transformation auf das Recht: *Ladeur*, Computerkultur

waltungsrechtsverhältnisses, die durch Informationsrechte und -pflichten strukturiert ist, über das Informationshandeln des Staates bis hin zur Gestaltung der inneradministrativen Informationsbeziehungen, einschließlich des (Verwaltungs-)Datenschutzes.[7] Bemerkenswert ist, dass die Diskussion zum Informationsverwaltungsrecht weitgehend technikneutral geführt wurde – dementsprechend verstand sich das Informationsverwaltungsrecht gerade nicht als Fortsetzung des älteren Technisierungsdiskurses der Verwaltung.[8] So geriet allerdings teilweise aus dem Blick, welche Voraussetzungen vorliegen müssen, damit Informationsgewinnung, -weitergabe und -speicherung gefahr- und verlustlos vonstattengehen können. Auch der an verschiedenen Stellen thematisierte Geheimnisschutz wurde nicht mit Blick auf spezifisch technische Bedrohungen entfaltet. Mit anderen Worten: Die Sicherheit der Informationsordnung[9] spielt weder in Grundlagentexten zum Informationsverwaltungsrecht noch in stärker anwendungsorientierten Beiträgen eine bedeutende Rolle, sondern wird üblicherweise schlicht als gegeben unterstellt. Zugleich führt die informationsverwaltungsrechtliche Literatur jedoch deutlich vor Augen, in welchem Maße das Handeln des Staates und seiner Institutionen heute Informationsverarbeitung ist, welche Abhängigkeit mittlerweile also von der digitalen Technik besteht.

In der Praxis ist der Informationsaustausch zwischen Staat und Bürgern sowie innerhalb der Verwaltung für Angriffe und Ausfälle der digitalen Technik anfällig. Die Manipulationsmöglichkeit elektronischer Akten (vgl. § 6 EGovG

---

und Evolution der Methodendiskussion in der Rechtswissenschaft, ARSP 74 (1988), S. 218 ff.; *Ladeur*, Die Textualität des Rechts, 2015, S. 306 ff.; *Vesting*, Die Medien des Rechts: Computernetzwerke, 2015.

[7] Eine umfassende Aufarbeitung des Diskussionsstands boten erstmals die „Grundlagen des Verwaltungsrechts" (Bd. II) mit (in Erst- und Zweitauflage) den Beiträgen von *Vesting* (§ 20), *Ladeur* (§ 21), *Albers* (§ 22), *Gusy* (§ 23), *Holznagel* (§ 24), *von Bogdandy* (§ 25) und *Britz* (§ 26). Konsolidierend dann *Augsberg*, Informationsverwaltungsrecht, 2014. Nunmehr umfassend aktualisiert und teils mit neuen Autoren die Drittauflage des Werks (Bd. I von 2022): *Vesting* (§ 20), *Ladeur* (§ 21), *Albers* (§ 22), *Gusy* (§ 23), *Wischmeyer* (§ 24), *von Bogdandy/Hering* (§ 25) und *Britz/Eifert* (§ 26).

[8] In der Drittauflage der „Grundlagen des Verwaltungsrechts" wird in den dem Informationsverwaltungsrecht gewidmeten Beiträgen der (digitalen) Technik eine größere Rolle eingeräumt, vgl. etwa *M. Albers*, Umgang mit personenbezogenen Informationen und Daten, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 3. Aufl. 2022, § 22 Rn. 2, 3, 77 ff.; *T. Wischmeyer*, Informationsbeziehungen in der Verwaltung, in: a. a. O., § 24 Rn. 27 ff.; *G. Britz/M. Eifert*, Digitale Verwaltung, in: a. a. O., § 26 Rn. 5 ff. und passim.

[9] Zu diesem Begriff näher *Voßkuhle*, Der Wandel von Verwaltungsrecht und Verwaltungsprozeßrecht in der Informationsgesellschaft, in: Hoffmann-Riem/Schmidt-Aßmann (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, 2000, S. 349 (355 ff.); *Schmidt-Aßmann*, Das allgemeine Verwaltungsrecht als Ordnungsidee, 2. Aufl. 2006, 6/3 ff.; *ders.*, Principles of an International Order of Information, in: Anthony/Auby et al. (Hrsg.), Values in Global Administrative Law, 2011, S. 117 (119); kritisch-differenzierend *T. Vesting*, „Informationsordnung", in: Badura/Dreier (Hrsg.), FS 50 Jahre BVerfG, Bd. 2, 2001, S. 219 (227 ff.).

des Bundes) ist nur ein besonders eindeutiger Fall.[10] In der stärker anwendungsorientierten Literatur zum Recht des E-Government[11] wurde Informationssicherheit daher stets mitgedacht – und auch mitgeregelt.[12] Denn ein rechtssicherer Datenaustausch mit und zwischen Behörden muss auch technisch sicher sein. Die konkrete Ausformung einer den Sicherheitsbedürfnissen angemessenen, gleichzeitig aber auch aus Nutzersicht noch praktikablen Kommunikationsarchitektur erwies sich jedoch als Herausforderung, die bis heute nicht bewältigt ist.[13] Gleiches gilt für den Umgang mit weiteren Problemen, die sich unter dem Gesichtspunkt der Informationssicherheit bei der Digitalisierung der Verwaltungskommunikation auftaten. Hierzu zählen etwa die mit Informationssicherungspflichten verbundene Tendenz zur Hochzonung – die technisch naheliegende Lösung, Sicherheitsvorgaben möglichst zentral zu regeln, steht in Spannung zur föderalen Gewaltengliederung – sowie der Zielkonflikt zwischen Informationssicherheit und dem Grundsatz der effektiven behördlichen Aufgabenwahrnehmung, geht effektive Informationssicherheit doch oftmals mit Einschränkungen der Funktionalität einher.[14]

---

[10] Dazu nur *M. Eifert*, Elektronische Verwaltung, in: Bultmann/Grigoleit et al. (Hrsg.), FS Battis, 2014, S. 421 (426); *Britz/Eifert*, Digitale Verwaltung, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 3. Aufl. 2022, § 26 Rn. 43.

[11] Informationsverwaltungsrechts- und E-Government-Diskurs operieren trotz zahlreicher inhaltlicher und methodischer Berührungspunkte und diverser Bemühungen um Brückenschläge – insbes. *M. Eifert*, Electronic Government, 2006; *G. Britz*, Elektronische Verwaltung, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR, Bd. 2, 2. Aufl. 2012, § 26; jetzt *Britz/Eifert*, Digitale Verwaltung, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 3. Aufl. 2022, § 26 – im Wissenschaftsalltag bisher weitgehend unabhängig voneinander.

[12] Vgl. beispielhaft § 5 OZG i. V. m. der IT-Sicherheitsverordnung Portalverbund v. 6.1.2022, BGBl. I S. 18.

[13] Für das inneradministrative Verhältnis siehe insbesondere Art. 91c Abs. 2 Satz 1 GG, §§ 1 Abs. 1 Nr. 2; 2 Abs. 1 IT-Planungsrat-Staatsvertrag, § 10 EGovG sowie dessen landesrechtlichen Parallelnormen. Die Bemühungen um den Aufbau sicherer und gleichzeitig praxistauglicher Kommunikationsstrukturen im Staat-Bürger-Verhältnis (vgl. § 3a Abs. 2 VwVfG), die zunächst in Form des (2017 aufgehobenen) Signaturgesetzes (dazu nur *Eifert*, Electronic Government, 2006, S. 82 ff.), dann durch das DE-Mail-Gesetz (dazu nur *A. Roßnagel*, Das De-Mail-Gesetz, NJW 2011, S. 1473 ff.) sowie jetzt durch die eIDAS-Verordnung (EU) Nr. 910/2014 (zu den Reformplänen oben § 1 Fn. 9) und das diese ergänzende Vertrauensdienstegesetz (dazu nur *A. Roßnagel*, Das Vertrauensdienstegesetz, MMR 2018, S. 31 ff.; *ders.*, IT-Sicherheitsinfrastrukturen und -dienste, in: Hornung/Schallbruch [Hrsg.], IT-Sicherheitsrecht, 2021, § 14) vorangetrieben wurden, sind bisher auf geringe Resonanz in der Bevölkerung gestoßen.

[14] Hierzu bereits *M. Eifert*, Electronic Government, ZG 2001, S. 115 ff.; *K. Lenk*, Abschied vom Zuständigkeitsdenken, VM (2007), S. 234 ff.; *D. Heckmann*, Perspektiven des IT-Einsatzes, DV 46 (2013), S. 1 (12 ff.); *Eifert*, Elektronische Verwaltung, in: Bultmann/Grigoleit et al. (Hrsg.), FS Battis, 2014, S. 421 (430 f.); *T. Wischmeyer*, in: Huber/Voßkuhle, GG, 8. Aufl. i. E., Art. 91c, Rn. 21 ff.; *Britz/Eifert*, Digitale Verwaltung, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 3. Aufl. 2022, § 26 Rn. 151 ff.

Diese Punkte sind in der vorliegenden Untersuchung allerdings nur insoweit aufzunehmen, als sie auch die Kommunikationsprozesse im Verhältnis zwischen Privaten betreffen. Die Spezifika der IT-Sicherheit im E-Government, die vor allem die föderale Verteilung von Gesetzgebungs- und Verwaltungskompetenzen betreffen, bleiben demgegenüber ebenso wie andere rein sektorale Problemstellungen ausgeklammert.[15]

2. Informationssicherheit im Datenschutzrecht

Auch im Datenschutzrecht wurde früh erkannt, dass das Recht auf informationelle Selbstbestimmung leerläuft, wenn rechtmäßig erhobene personenbezogene Daten nicht sicher sind, bzw. dass Gefährdungen des Persönlichkeitsrechts auch durch Verletzungen der Verfügbarkeit, Integrität und Vertraulichkeit dieser Daten drohen.[16] Schon die allerersten Datenschutzgesetze enthielten daher Verpflichtungen zum Schutz rechtmäßig gesammelter Daten gegen den unbefugten Zugriff durch Dritte.[17] Lange Zeit hat dies jedoch keine vertiefte Auseinandersetzung mit dem Konzept der Daten- oder Informationssicherheit veranlasst. Und auch wenn im Zuge der umfassenden Reform des Datenschutzrechts der Stellenwert der Datensicherheit – im öffentlichen wie im privaten Sektor – heute allgemein anerkannt ist (vgl. Art. 5 Abs. 1 lit. f DSGVO), bleibt die Spannungslage von Datenschutz und Datensicherheit für die Datenverarbeitungspraxis herausfordernd.[18] Dennoch kann schon hier festgehalten werden, dass das Datenschutzrecht heute übergreifend als wesentlicher Impulsgeber für das Recht der Informationssicherheit fungiert. Das Datenschutzrecht wird daher im Folgenden immer wieder als Referenzmaterie heranzuziehen sein, und auf die umfangreiche Befassung mit der Thematik im datenschutzrechtlichen Schrifttum wird zurückzukommen sein.

---

[15] Dazu im Überblick *S. Klein/C. Drews*, Informationssicherheit, in: Lühr/Jabkowski/Smentek (Hrsg.), Handbuch Digitale Verwaltung, 2019, S. 213 ff.; *C. Sorge*, Sichere Informationstechnik, in: Seckelmann (Hrsg.), Digitalisierte Verwaltung – Vernetztes E-Government, 2. Aufl. 2019, S. 439 ff.; *W. Schünemann*, Cybersicherheit, in: Klenk/Nullmeier/Wewer (Hrsg.), Handbuch Digitalisierung in Staat und Verwaltung, 2020, S. 199 ff.

[16] Siehe nur ausführlich *W. Heilmann/G. Reusch*, Datensicherheit und Datenschutz, 1984. In der Rückschau erstaunt, dass für die dem „Datengeheimnis" (§ 5 BDSG a. F.) weitgehend analogen sonstigen Geheimhaltungspflichten der Verwaltung (vgl. etwa § 30 VwVfG, § 30 AO, §§ 67 ff. SGB X) keine entsprechenden Überlegungen zur Datensicherheit angestellt wurden.

[17] Vgl. § 2 des Hessischen Datenschutzgesetzes v. 7.10.1970 (GVBl. I S. 625): „Die vom Datenschutz erfaßten Unterlagen, Daten und Ergebnisse sind so zu ermitteln, weiterzuleiten und aufzubewahren, daß sie nicht durch Unbefugte eingesehen, verändert, abgerufen oder vernichtet werden können. Dies ist durch geeignete personelle und technische Vorkehrungen sicherzustellen."

[18] Hierzu die Nachweise unten § 5 Fn. 30.

3. Informationssicherheit im Recht der kritischen Infrastrukturen

Nicht verwechselt werden darf die Frage nach Informationssicherheit mit der vielschichtigen Diskussion um das Verhältnis von Freiheit und Sicherheit, die sich in der letzten Dekade vor allem mit Blick auf staatliche Eingriffe in die informationelle Selbstbestimmung entsponnen hat. Wenn komplexe Techniken der Überwachung digitaler Informationsflüsse zur Bekämpfung von Terrorismus und schwerer Kriminalität eingesetzt werden, dient dies nur in einzelnen, dann allerdings sehr sensiblen Fällen der Sicherheit der Informationsinfrastrukturen selbst.

Darüber hinaus hat das Recht der Informationssicherheit jedoch weitere Berührungspunkte mit dem „allgemeinen" Sicherheitsrecht. Dabei ist zu berücksichtigen, dass der Sicherheitsbegriff und mit ihm das Sicherheitsrecht in den vergangenen Dekaden eine semantische Entgrenzung erfahren haben.[19] Mehr und mehr werden unter Sicherheitsgewährleistung nicht nur Maßnahmen zur Verhinderung von Angriffen durch Personen auf Rechtsgüter, sondern auch Regelungen zur Daseinsvorsorge („Versorgungssicherheit") sowie die für die vorliegenden Fragestellungen besonders einschlägigen technischen Sicherheitsvorgaben („Produktsicherheit") subsumiert. In diesem „neuen" Sicherheitsrecht ist die traditionelle Kluft zwischen Rechtsgebieten wie dem Polizei-, Katastrophen- und Technikrecht weitgehend eingeebnet.[20] Besonders weit fortgeschritten ist die Debatte im Bereich der sogenannten kritischen Infrastrukturen (KRITIS).[21] Die Verwundbarkeit der IT etwa von Krankenhäusern, Energieversorgern, Wasserbetrieben und sonstigen Anbietern wesentlicher Dienste[22] hat hier den nationalen und den europäischen Gesetzgeber zu weitreichenden Maßnahmen in Form von sektorspezifischen Mindestanforderungen für die Informationssicherheit der KRITIS-Betreiber motiviert.[23] Das und die Tatsache, dass digitale Netze KRITIS-Betreiber miteinander verbinden und so gewissermaßen eine Super-Infrastruktur bilden, deren Beeinträchtigung Kaskadeneffekte und systemische Schäden verursachen kann, dürften dafür verantwortlich sein, dass unter dem KRITIS-Paradigma bisher wohl die intensivste rechtswissenschaftliche Auseinandersetzung mit Fragen der Informationssicherheit erfolgt ist.[24] Die Fortschritte, die hier bei der Analyse des

[19] Hierzu ausführlich unten § 4 I.

[20] Grundlegend zu „altem" und „neuem" Sicherheitsrecht *C. Gusy*, Neuer Sicherheitsbegriff, VerwArch 2010, S. 309 ff.; *P. Wiater*, Sicherheitspolitik zwischen Staat und Markt, 2013. Zum Begriff des „Sicherheitsrechts" instruktiv *C. Gusy*, Sicherheitsrecht als Rechtsgebiet?, in: Dietrich/Gärditz (Hrsg.), FS Graulich, 2019, S. 9 ff.

[21] Hierzu ausführlich unten § 4 I. 2. d) und § 6 II. 5.

[22] Beispiele hierzu oben bei § 1 I.

[23] Siehe dazu bereits die Nachweise oben § 1 Fn. 24 und 29.

[24] Vgl. an dieser Stelle nur die grundlegenden Beiträge von *D. Heckmann*, Staatliche Schutz- und Förderpflichten zur Gewährleistung von IT-Sicherheit, in: Rüßmann (Hrsg.),

Informationssicherheitsrechts gemacht wurden, sind beachtlich. Dies gilt insbesondere für die Verbindungslinien, die zwischen dem Informationsrecht einerseits und dem Infrastruktur-, Gewerbe- und Technikrecht andererseits geschlagen wurden und die, wie noch im Detail zu diskutieren sein wird, für erfolgreiche Regulierung in diesem Bereich essenziell sind. Bereits der Blick in die einschlägigen Normen zeigt jedoch, dass auch hier nur ein begrenzter Ausschnitt der Gesamtproblematik thematisiert wird. So bringt die Orientierung von KRITIS am katastrophenrechtlichen Paradigma die Konzentration auf einzelne Sektoren und ausgewählte Stellen mit sich; dies wird dem hohen Vernetzungsgrad von Informationssicherheitsrisiken nicht umfassend gerecht. Darüber hinaus hat der KRITIS-Diskurs die größeren verfassungs- und völkerrechtlichen Implikationen des Informationssicherheitsproblems nur in Ansätzen reflektiert.

4. Informationssicherheit im Völkerrecht

Die völkerrechtlichen Implikationen unsicherer Informationsinfrastrukturen sind seit 2007 – in diesem Jahr erfolgte eine konzertierte Cyberattacke auf Estland[25] – Gegenstand einer intensiven Debatte in der Völkerrechtswissenschaft um „cyber war" und „cyber terrorism". Gestritten wird unter anderem um Möglichkeiten und Grenzen legitimer Selbstverteidigung gegenüber Cyberattacken, Regeln für den offensiven Einsatz von Cyberwaffen und die Reichweite der Staatenverantwortlichkeit.[26] Auch Spionage[27] sowie Versuche zur

FS Käfer, 2009, S. 129 ff.; *C. Möllers/L. Pflug*, Verfassungsrechtliche Rahmenbedingungen des Schutzes kritischer IT-Infrastrukturen, in: Kloepfer (Hrsg.), Schutz kritischer Infrastrukturen, 2010, S. 47 ff.

[25] Zum Sachverhalt *J. Davis*, Hackers Take Down the Most Wired Country in Europe, Wired, 21.8.2007. Zum Effekt dieses Angriffs, der das Thema Cybersicherheit erstmals prominent auf die politische Agenda der EU und ihrer Mitgliedstaaten setzte, siehe *Kello*, Cyber Defence, in: Meijer/Wyss (Hrsg.), The Handbook of European Defence Policies and Armed Forces, 2018, S. 658 (661 ff.).

[26] Aus der umfangreichen Literatur siehe nur als wichtige Referenzpunkte des Diskurses *D. Hollis*, e-SOS, Harv. Int'l L. J. 52 (2011), S. 373 ff.; *M. Waxman*, Cyber-Attacks and the Use of Force, Yale J. Int'l L. 36 (2011), S. 421 ff.; *O. Hathaway/R. Crootof et al.*, The Law of Cyber-Attack, Calif. L. Rev. 100 (2012), S. 817 ff.; *H. Krieger*, Krieg gegen anonymus, AVR 50 (2012), S. 1 ff.; *H. Harrison Dinniss*, Cyber Warfare, 2012; *M. N. Schmitt* (Hrsg.), Tallinn Manual, 2013; *J.-C. Woltag*, Cyber Warfare, 2014; *M. Roscini*, Cyber Operations, 2014; *B. Mazanec/B. Thayer*, Deterring Cyber Warfare, 2014; *C. Walter*, Cyber Security als Herausforderung für das Völkerrecht, JZ 70 (2015), S. 685 ff.; *S. Schmahl*, Cybersecurity, in: Dethloff/Nolte/Reinisch (Hrsg.), Cyberwelt, 2016, S. 159 ff.; *M. N. Schmitt* (Hrsg.), Tallinn Manual 2.0, 2017; *F. Delerue*, Cyber Operations and International Law, 2020; *Bundesregierung*, On the Application of International Law in Cyberspace, 2021. Aus der deutschen Debatte siehe auch *J. Thümmel*, Computernetzwerkoperationen innerhalb internationaler bewaffneter Konflikte, 2013; *S.-H. Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, 2015; *J. Dornbusch*, Das Kampfführungsrecht im internationalen Cyberkrieg, 2019;

destabilisierenden Einflussnahme unterhalb der Schwelle völkerrechtlich relevanten Handelns[28] werden zunehmend von Cyberoperationen begleitet. Die Europäische Union hat hierauf bereits mit Sanktionen für die Urheber entsprechender Attacken reagiert.[29]

Die hiesige Untersuchung, die ihren Schwerpunkt im deutschen Recht und im Unionsrecht hat, muss diese Fragen von Krieg und Frieden weitgehend ausblenden. Die völkerrechtliche Perspektive macht jedoch darauf aufmerksam, dass eine angemessene Analyse des Informationssicherheitsproblems nicht introvertiert vorgehen kann. Im Gegenteil: Die globale Bedrohungslage, die insbesondere aus der umfassenden Vernetzung von IT-Systemen über das Internet resultiert, stellt jeden Versuch einer ausschließlich nationalen oder auch supranationalen Antwort auf Informationssicherheitsrisiken vor kaum lösbare Schwierigkeiten. Umgekehrt wird sich allerdings zeigen, dass der globale „Cyberspace" – dieser einst esoterische Begriff hat sich mittlerweile als politisch-juristischer Begriff fest etabliert – nach wie vor mit den Mitteln des (Völker-)Rechts nur schwer fassbar ist. Praktisch bedeutet dies, dass Fragen der Internetarchitektur und -infrastruktur in die Diskussion um die nationale und unionale Informationssicherheitsregulierung einbezogen und damit gewissermaßen „territorialisiert" werden müssen.[30] Langfristig gilt es zudem, die Diskussion um globale Internetregulierung um den bisher fast gänzlich vernachlässigten Aspekt der Informationssicherheit zu ergänzen.[31] Das weitge-

H. Lahmann, Die völkerrechtliche Dimension der IT-Sicherheit, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 6. Aus (wehr-)verfassungsrechtlicher Sicht *C. Marxsen*, Verfassungsrechtliche Regeln für Cyberoperationen der Bundeswehr, JZ 72 (2017), S. 543 ff.; *Knoll*, Streitkräfteeinsatz zur Verteidigung gegen Cyberangriffe, 2020, S. 147 ff.; *S. Spies-Otto*, Aufgaben und Befugnisse der Bundeswehr, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 19. Vgl. für die USA die Dokumentation bei *anon.*, U.S. Military Undergoes Restructuring to Emphasize Cyber and Space Capabilities, AJIL 113:3 (2019), S. 634 ff.

[27] Dazu *R. Buchan*, Cyber Espionage and International Law, 2019.

[28] *C. Whyte*, Cyber conflict or democracy "hacked"?, Journal of Cybersecurity 6:1 (2020), S. 1 ff.; *H. Lin/J. Kerr*, On Cyber-Enabled Information/Influence Warfare and Manipulation, in: Cornish (Hrsg.), Oxford Handbook of Cyber Security, 2021, S. 251 ff. Zu den völkerrechtlichen Maßstäben *B. Baade*, Fake News and International Law, EJIL 29:4 (2018), S. 1357 (1362 ff.). Zur Rolle der Technik, insbesondere der sozialen Medien *K. Pearce*, Democratizing kompromat, Information, Communication & Society 18:10 (2015), S. 1158 ff.

[29] Zum rechtlichen Hintergrund siehe oben § 1 Fn. 44. Die konsolidierte Fassung der VO (EU) 2019/796 des Rates v. 17.5.2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen, ist abrufbar unter https://eur-lex.europa.eu/eli/reg/2019/796/deu.

[30] Vertiefend hierzu unten § 6 III. und § 6 II. 2.

[31] Aus der reichhaltigen Literatur zu einem „Völkerrecht des Internets" siehe *S. Schmahl*, Zwischenstaatliche Kompetenzabgrenzung im Cyberspace, AVR 47 (2009), S. 284 ff.; *R. Uerpmann-Wittzack*, Principles of International Internet Law, German L. J. 11 (2010), S. 1245 ff.; *J. Kulesza*, International Internet Law, 2012; *M. Land*, International Law of the Internet, Harv. Int'l L. J. 54 (2013), S. 393 ff.; Tsagourias/Buchan (Hrsg.), Research Hand-

hende Fehlen verbindlicher völkerrechtlicher Koordinationsregime führt fast nirgends zu so drängenden Problemen wie im Bereich der Informationssicherheit.[32]

5. Zur Notwendigkeit einer integrativen Perspektive

Diese Stichproben lassen bereits zentrale Probleme erkennen, mit denen sich Untersuchungen des Informationssicherheitsrechts auseinandersetzen müssen. Sie weisen auch darauf hin, wie zersplittert die bestehenden rechtlichen Regelungen sind, welchen Rückstand das Recht gegenüber dem Potential und den Gefahren der Technik hat und welche Schwierigkeiten sich aus der globalen Natur der entsprechenden Risiken für deren Regulierung ergeben.[33] Nach wie vor besteht daher erheblicher gesellschaftspolitischer Reform- und rechtswissenschaftlicher Analysebedarf. Um dem abzuhelfen, müssen zunächst die unterschiedlichen Perspektiven zusammengeführt, die einzelnen Spezialdiskurse miteinander vernetzt und je im Hinblick auf die Dimension Informationssicherheit vertieft werden. Nur auf diese Weise lassen sich Schutzlücken vermeiden.[34] Zu integrieren sind an gegebener Stelle auch weitere, hier noch ausgesparte Diskussionsstränge, etwa zur Rolle des Haftungsrechts als Anreizmechanismus zur Stärkung von Informationssicherheit sowie zum Informationsstrafrecht. Dass darüber hinaus das speziell informationssicherheits-

book on International Law and Cyberspace, 2015; *Kettemann*, The Normative Order of the Internet, 2020; *C. Haake*, Technik – Recht – Raum, 2022, S. 69 ff.; sowie die Beiträge in der Special Issue „International Law and the Internet" der ZaöRV mit der Einführung von *M. Kettemann/R. Kunz/A. Golia*, Introduction, ZaöRV 81 (2021), S. 597 ff. Speziell zu Fragen der Cybersicherheit siehe aber *M. Mueller*, Will the Internet Fragment?, 2017, S. 9 ff.; *Schmahl*, Cybersecurity, in: Dethloff/Nolte/Reinisch (Hrsg.), Cyberwelt, 2016, S. 159 ff.; *I. Pernice*, Global Cybersecurity Governance, Global Constitutionalism (2018), S. 112 ff. Zur Frage, inwieweit das Völkerrecht überhaupt auf den Cyberspace anwendbar ist, siehe ausführlich unten § 4 II. 2. b).

[32] Auch dort, wo eine politische Übereinstimmung in den etablierten Formaten nicht zu erreichen ist, bemühen sich Staaten im Bereich der Informationssicherheit vielfältig um Kooperation. Diese erfolgt nicht nur intergouvernemental; vielmehr existieren verschiedene Initiativen, in denen staatliche und private Akteure über allgemeine Grundsätze der Cybersicherheit verhandeln. Diese Initiativen haben allerdings bisher nur geringe Erträge gezeitigt. Dennoch optimistisch *Pernice*, Global Cybersecurity Governance, Global Constitutionalism (2018), S. 112 (124, 131 ff.).

[33] Dass die angemessene Beschreibung und Verortung des Problems auch unter kompetenzrechtlichen Aspekten Voraussetzung für eine gelingende Regulierung ist, zeigt an der Entwicklung des U.S.-Rechts *J. Lewallen*, Emerging technologies and problem definition uncertainty, Regulation & Governance 15 (2021), S. 1035 ff.

[34] Wenn etwa das Datenschutzrecht die datenschutzrechtlich verantwortlichen Stellen zur Gewährleistung von Informationssicherheit verpflichtet, diese sich ihre technischen Komponenten jedoch auf einem gänzlich unregulierten Markt beschaffen müssen, lässt dies Sicherheitslücken.

rechtliche Schrifttum umfassend auszuwerten ist, versteht sich von selbst. Gleiches gilt für die in der letzten Dekade rasant gewachsene Literatur zur Informationssicherheit in den Sozial- und Politikwissenschaften.[35] Dass die folgende Arbeit angesichts der Fülle an Themen nicht alle Problemstellungen aufgreift und vertieft diskutiert, ist unvermeidbar.

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

Die Vielzahl der konkurrierenden Begriffsverwendungen verlangt nach definitorischen Vorklärungen. Beide Glieder des Kompositums Informationssicherheit bedürfen, auch in ihrer Verbindung, der Erläuterung. Da der Teilbegriff „Sicherheit" sowohl in der Sache besonders sensibel ist als auch für den konzeptionellen Zugriff auf die Materie entscheidende Weichen stellt, ist auf ihn gesondert einzugehen (siehe § 4 I.). An dieser Stelle soll daher nur erläutert werden, weshalb die untersuchten Phänomene unter den Begriff der *Informations*sicherheit gefasst werden.[36]

Als Alternative bietet sich zunächst der vom Gesetzgeber als Komplement zum Datenschutz entwickelte und nach wie vor bemühte Begriff der *Daten*sicherheit an.[37] Allerdings erscheint im Lichte sowohl der einschlägigen technischen Standards der ISO/IEC 2700x-Reihe als auch der in der Wissenschaft breit akzeptierten Unterscheidung der Bedeutungsgehalte von „Daten" und „Informationen" der Begriff der Informationssicherheit konzeptionell stimmiger.[38]

[35] Zu den Faktoren für diese noch junge Entwicklung siehe *Dunn Cavelty/Wenger*, Cyber Security Meets Security Politics, Contemporary Security Policy 41:1 (2020), S. 5 (8 ff.). Zu den ersten spezialisierten Zeitschriften gehören das Journal of Cybersecurity (Oxford University Press, seit 2015) und das Journal of Cyber Policy (Taylor & Francis, seit 2016).

[36] Angemerkt sei bereits an dieser Stelle, dass es angesichts der polysemantischen Natur der in Rede stehenden Begriffe kaum gelingen wird, einen einheitlichen oder auch nur einen für die Rechtssprache verbindlichen Verwendungsstandard zu etablieren. Bekanntlich unterlaufen zahlreiche Rechtsnormen – nicht zuletzt das Datenschutzrecht – die Unterscheidung von Information und Datum (dazu gleich § 2 Fn. 38). Dies entwertet definitorische Bemühungen nicht, begrenzt allerdings ihre Reichweite.

[37] So insbesondere § 9a S. 1 BDSG a. F. Der Begriff ist aber auch im aktuellen Gesetzgebungs- und Verordnungsrecht präsent. So ergibt die Volltextsuche auf http://www.gesetze-im-internet.de immerhin 362 Treffer, während „Informationssicherheit" nur auf 74 Treffer kommt (Stand: 1.9.2022). Enger wird der Begriff hingegen teilweise im technischen Diskurs verwendet, vgl. *C. Eckert*, IT-Sicherheit, 10. Aufl. 2018, S. 6, wo Datensicherheit als die „Eigenschaft eines funktionssicheren Systems, nur solche Systemzustände anzunehmen, die zu keinem unautorisierten Zugriff auf Systemressourcen und insbesondere auf Daten führen", bezeichnet wird.

[38] Zu der schon ritualisierten Abgrenzung der Begriffe „Daten", „Information" und „Wissen" siehe nur *I. Spiecker gen. Döhmann*, Wissensverarbeitung, Rechtswissenschaft 1 (2010), S. 247 (254 ff.); *Augsberg*, Informationsverwaltungsrecht, 2014, S. 28 ff. Alternative Ansätze bei *P. Adriaans*, „Information", in: SEP, Fall 2020 Edition.

Denn primäres Schutzgut entsprechender rechtlicher Schutzgarantien ist nicht das einzelne fixierte Zeichen. Den normativen Horizont der Materie bildet vielmehr die „Information" als dasjenige, was durch die Daten in einer re-interpretierbaren Form dargestellt bzw. repräsentiert wird. So geht es bereits beim Verbot der Datenmanipulation (§§ 202a Abs. 2, 303a StGB) letztlich darum, Fehldeutungen durch das interpretierende Programm zu verhindern, d. h. um die semantische Ebene, die dem Informationsbegriff zugerechnet wird. Sofern die Regulierung dennoch teils beim syntaktischen Datum anknüpft, ist dies eine Frage der Regelungstechnik innerhalb einer letztlich an der Integrität von Informationen interessierten Regelungsarchitektur. Noch gewichtiger ist, dass sich die Materie nicht auf Regeln zum Umgang mit Datenbeständen im eigentlichen Sinne beschränken darf, sondern etwa auch IT-Produkte, IT-Systeme und Informationsnetzwerke einbeziehen muss.[39] Während ein Bezug zur *Daten*sicherheit hier oft nur mittelbar gegeben ist, lässt sich eine solche Ausweitung ohne Schwierigkeiten unter den Begriff der Gewährleistung von Informationssicherheit subsumieren.[40] Schließlich ist der Begriff der Datensicherheit historisch eng mit dem Datenschutz verbunden und wird daher regelmäßig mit der Sicherung *personenbezogener* Daten assoziiert.[41] Auch diese Engführung vermeidet der weitere Begriff der Informationssicherheit.

Gegen den Begriff der *Informations*sicherheit scheint allerdings zu sprechen, dass er technik- und medienneutral und daher zu breit ist: Informationen in Papierform müssen ebenso wie elektronische Akten vor unbefugtem Zugriff und sonstigen Integritätsbeeinträchtigungen geschützt werden.[42] Dennoch ist die weitgehende Gleichsetzung von Informationssicherheit und Sicherheit der vernetzten Informationstechnik (IT), wie sie in der heutigen Diskussion regelmäßig erfolgt und wie sie auch der folgenden Untersuchung zu

[39] Ausführlich hierzu unten § 6 II.

[40] Vgl. entsprechend nur *IT-Planungsrat*, Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung, 6.12.2018, S. 10.

[41] Hierzu oben § 2 I. 2.

[42] Vgl. *BSI*, IT-Grundschutz-Methodik, BSI-Standard 200–2, Version 1.0, Oktober 2017, https://www.bsi.bund.de/grundschutz, S. 12: „Informationssicherheit umfasst den umfangreicheren Bereich des Schutzes von Informationen, zwar in und mit IT, aber auch ohne IT bzw. über IT hinaus. Somit ist IT-Sicherheit ein Teilbereich der Informationssicherheit und beschäftigt sich gezielt mit dem Schutz der eingesetzten IT." Unter einen medienunabhängigen bzw. „analogen" Begriff der Informationssicherheit lassen sich daher etwa auch die rechtlichen Vorschriften zur Geheimhaltung in der Verwaltung (vgl. § 30 VwVfG, § 30 AO, §§ 67 ff. SGB X), die Archiv- und Registergesetze sowie im Bereich der Unternehmen der Geheimnisschutz etwa nach GeschGehG (dazu im vorliegenden Kontext näher *Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022, Rn. 144 ff.) subsumieren. Dass Informationen nicht erst Angriffsziel sind, seit Daten digital gespeichert und IT-Systeme miteinander vernetzt werden, beschreiben u. a. K. Leeuw/J. Bergstra (Hrsg.), History of Information Security, 2007. Für eine „analoge" Fallkonstellation: BVerwG, NVwZ-RR 2006, S. 556.

Grunde liegen soll, angesichts der heute überragenden Bedeutung von IT für den Umgang mit Informationen in der Praxis plausibel.[43] Dass die vorliegende Untersuchung dennoch nicht unter den Oberbegriff der *IT-*, *Computer-* oder *Internet*sicherheit[44] gestellt wird, markiert, dass es sich beim hiesigen Untersuchungsgegenstand nicht um eine Randmaterie des Technikrechts oder einen Ausschnitt des IT-Rechts, sondern um eine grundlegende regulatorische Herausforderung für das Recht in der Informationsgesellschaft handelt.[45] Auch wenn IT-Systeme, Hardware, Software etc. den unmittelbaren Gegenstand der Regulierung bilden, steht mit der Sicherheit der Informationsgesellschaft mehr auf dem Spiel.[46] Gleichwohl werden Begriffe wie IT-Sicherheit im Folgenden dort Verwendung finden, wo der Sprachgebrauch des Gesetzgebers dies erfordert oder wo auf die durch diesen Begriff aufgerufene spezifisch technische Dimension des Problems Bezug genommen wird.[47]

Pragmatisch ist auch zu verfahren, was den im internationalen und im unionsrechtlichen Diskurs heute fest etablierten Begriff der *Cyber*sicherheit betrifft, der in erster Linie die Sicherheit der *vernetzten* Informationstechnik in

[43] Vgl. in diesem Sinne etwa auch die Aufgabenbeschreibung des BSI in §§ 1 S. 2; 3 BSIG. Entsprechend Art. 4 Nr. 1 NIS-RL.

[44] Verwendet etwa von *Leisterer*, Internetsicherheit in Europa, 2018, der „Internetsicherheit" dann allerdings wieder durch den Begriff der Informationssicherheit definiert (a. a. O., S. 12).

[45] Hierzu oben § 1 IV.

[46] Zum Begriff der Informationsgesellschaft grundlegend die als Trilogie mit dem Titel „The Information Age: Economy, Society and Culture" versehenen Bände von *M. Castells*, The Rise of the Network Society (1996), 2. Aufl. 2009; *ders.*, The Power of Identity (1997), 2. Aufl. 2009; *ders.*, End of Millennium (1998), 2. Aufl. 2010. Kritischer *C. May*, The Information Society, 2002. Vgl. weiter nur den Überblick über die Debatte bei *F. Webster*, Theories of the Information Society, 4. Aufl. 2014.

[47] Vgl. entsprechend *BSI*, IT-Grundschutz-Methodik, BSI-Standard 200–2, Version 1.0, Oktober 2017, https://www.bsi.bund.de/grundschutz, S. 14: „Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl in IT-Systemen, aber auch auf Papier oder in Köpfen gespeichert sein. IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung. Das Aktionsfeld der klassischen IT-Sicherheit wird bei der Cyber-Sicherheit auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein. Der Begriff ‚Informationssicherheit' statt IT-Sicherheit oder Cyber-Sicherheit ist daher umfassender. Der IT-Grundschutz verfolgt seit Langem einen ganzheitlichen Ansatz, mit dem auch geschäftsrelevante Informationen und Geschäftsprozesse geschützt werden, die nicht oder nur teilweise mit IT unterstützt werden. Da aber in der Literatur noch überwiegend der Begriff ‚IT-Sicherheit' zu finden ist, wird er auch in dieser sowie in anderen Publikationen des IT-Grundschutzes weiterhin verwendet, allerdings werden die Texte sukzessive stärker auf die Betrachtung von Informationssicherheit ausgerichtet."

den Blick nimmt.[48] In diesem Kontext hat das Begriffsfeld „Cyber" jenen techno-anarchistischen Anklang verloren, den es in der Frühzeit des Internets erworben hatte.[49] Stattdessen findet der Begriff routinemäßig in ganz unterschiedlichen Kontexten und Kombinationen Verwendung, darunter etwa *cyber war*, *cyber power* oder eben auch *cybersecurity*/Cybersicherheit. Angesichts des weiten Verbreitungsgrads stellt sich die Frage nicht mehr, ob diese Begriffsbildung glücklich ist. Im Folgenden wird daher immer wieder von Cybersicherheit die Rede sein, wo dieser Begriff in den ausgewerteten Rechtsquellen oder in der herangezogenen Literatur seinerseits Verwendung findet. Im Allgemeinen ist dies dort der Fall, wo es gilt, die europäische, globale und strategische Dimension des Informationssicherheitsproblems zu akzentuieren.[50] Der Versuch einer eindeutigen definitorischen Unterscheidung von Cyber- und Informationssicherheit[51] verspricht angesichts der zahlreichen divergierenden Sprachgebräuche in unterschiedlichen Teildisziplinen und Sprachräumen keinen Erfolg.

III. Gang der Untersuchung

Vor diesem Hintergrund lässt sich das Erkenntnisinteresse der vorliegenden Arbeit nochmals präziser fassen.[52] Ihr Ziel ist es, die Grundzüge des Informationssicherheitsrechts zu erarbeiten. Dabei leiten drei Perspektiven die Untersuchung an.

Zunächst widmet sie sich Grundlagenfragen des Rechts der Informationssicherheit und nimmt zentrale Positionsbestimmungen vor. Geklärt werden muss, in welchen Formen das Recht überhaupt auf die Technik einwirken kann (§ 3), inwieweit hierbei so etwas wie „Sicherheit" erzeugt wird (§ 4) und welche unions- und verfassungsrechtlichen Rahmenbedingungen zu beachten sind (§ 5).

Hierauf aufbauend ist das rechtliche Instrumentarium, das Vorgaben zur Gewährleistung der Informationssicherheit enthält, einer systematisierenden

---

[48] Im internationalen Diskurs hat der seit etwa zwanzig Jahren nachweisbare Begriff der *cybersecurity* den älteren Begriff der *information security* weitgehend ersetzt. Vgl. dazu *Dunn Cavelty/Egloff*, The Politics of Cybersecurity: Balancing Different Roles of the State, St Antony's Int'l Rev. 15 (2019), S. 37 (40).

[49] Siehe dazu unten § 6 II. 2. a).

[50] Siehe auch *M. Finnemore/D. B. Hollis*, Constructing Norms for Global Cybersecurity, AJIL 110 (2016), S. 425 (431).

[51] Siehe hierzu etwa den Vorschlag von *R. von Solms/J. van Niekerk*, From Information Security to Cyber Security, Computers & Security 38 (2013), S. 97 ff.

[52] Vorarbeiten zu der folgenden Untersuchung finden sich insbesondere bei *T. Wischmeyer*, Informationssicherheitsrecht, DV 50 (2017), S. 155 ff.; *T. Wischmeyer/A. Mohnert*, Recht der Informationssicherheit, in: Frenz (Hrsg.), Handbuch Industrie 4.0, 2019, S. 215 ff.

Zusammenschau zu unterziehen. Um einen Maßstab für die in die Untersuchung einzubeziehenden Normen zu gewinnen, sind unter Rückgriff auf die informationstechnische Literatur die Natur der Gefährdungslage und die technischen Rahmenbedingungen zu analysieren, bestimmen diese doch über den Umfang der Regulierungsaufgabe. Die Rekonstruktion des auf die Bewältigung dieser Aufgabe gerichteten Rechtsregimes ist dann – der komplexen Natur der Aufgabe durchaus entsprechend – herausfordernd. Um hier Ordnungsstrukturen zu etablieren, gilt es, die mit den bestehenden Regelungen je verfolgten regulatorischen Strategien herauszuarbeiten und die Institutionen, Instrumente und Prinzipien des Rechtsgebiets zu entfalten (§ 6).

Anschließend wechselt erneut die Perspektive: In den Blick genommen werden nun jene Aktivitäten, in denen der Staat selbst zum „Autor" von Cyberunsicherheit wird, also Informationstechnik manipuliert oder bekannte Schwächen der Technik für eigene Zwecke, etwa die Überwachung zu Strafverfolgungszwecken, ausnutzt. Gezeigt wird, dass sich auch dieses Themenfeld ohne angemessene Würdigung der Bedeutung sicherer Informationstechnik nicht hinreichend erschließen lässt (§ 7).

Ein Ausblick (§ 8) und eine Zusammenfassung in Thesen (§ 9) schließen die Arbeit ab.

Bestandsaufnahme und Begriffsanalyse lassen bereits erkennen, wie weit das hier in den Blick genommene Untersuchungsfeld ist. Deutlich wird, dass das Recht der Informationssicherheit nicht nur aus jenen Rechtsakten wie dem BSIG oder der NIS-Richtlinie besteht, die als erste in den Sinn kommen, wenn vom Informationssicherheitsrecht die Rede ist. Diese Regelungen bilden zwar das positiv-rechtliche Rückgrat der Materie, finden sich doch vor allem hier die für die Entwicklung und Implementierung gehaltvoller normativer Standards unerlässlichen Organisations- und Verfahrensvorgaben. Sie werden jedoch durch einen Kranz weiterer Normen ergänzt, die als regulatorischer Beitrag zur Bewältigung des Informationssicherheitsproblems gleichfalls Beachtung verlangen. Eine derart ausgreifende Themenstellung zwingt zur Begrenzung. Verschiedene mit dem Thema verbundene Fragestellungen können hier nur am Rande behandelt oder müssen ganz ausgeklammert werden. Neben den völkerrechtlichen Themen sind dies – wie erwähnt – die Besonderheiten der IT-Sicherheit im E-Government oder auch das Verhältnis von Cybersicherheit und Demokratiegefährdung.

Am Ende will die Arbeit die verschiedenen Dimensionen der Aufgabe Informationssicherheit konkretisieren, die auf die Bewältigung dieser Aufgabe bezogene Rechtsmaterie strukturieren und davon ausgehend Grundbausteine eines Informationssicherheitsrechts entwickeln. Darüber hinaus verfolgt sie das Anliegen, die Herausforderungen zu konturieren, die die Digitalisierung und Globalisierung für das Recht bedeuten, und fragt, inwieweit der Staat unter den Bedingungen der Digitalisierung seinem Anspruch, als Garant für die

Sicherheit seiner Bürger zu agieren, noch gerecht werden kann. Gleichzeitig gilt es auszuloten, inwieweit diese Bemühungen mit den Bestrebungen des Staates kollidieren, Schwächen der Informationstechnik für eigene Zwecke auszunutzen.

IV. Zur Methode: Nach der Neuen Verwaltungsrechtswissenschaft

Die vorliegende Arbeit betrachtet Informationssicherheit als regulatorische Aufgabe. Dies entspricht einer im heutigen (digital-)rechtlichen Diskurs gängigen Positionierung. Die Analyse und Bewertung rechtlicher Regulierungsregime wird daher nicht allein am Maßstab des geltenden (Verfassungs-) Rechts vorgenommen, sondern auch mit Blick auf ihre Aufgabenadäquanz untersucht. In methodischer Hinsicht wirft dieser Zugriff Fragen auf, die hier vorab diskutiert werden sollen. Diese betreffen das mit dem Regulierungsbegriff verbundene staats- und gesellschaftstheoretische Vorverständnis (1.) und die methodischen Standards, denen sich ein solcher Ansatz verpflichtet sieht (2.). Schließlich bestehen immer noch Irritationen darüber, ob ein solcher Ansatz als Gegenentwurf zu einer „dogmatisch" arbeitenden Rechtswissenschaft verstanden werden muss (3.).

1. Informationssicherheit als regulatorische Aufgabe

Der Regulierungsbegriff steht in der Tradition jener Leitbegriffe, mit deren Hilfe versucht wird, den Charakter des Rechts als Mittel zur Gestaltung und Veränderung gesellschaftlicher Prozesse mit seinem normativen Ordnungsanspruch in ein Verhältnis zu setzen.[53] Stritt man ursprünglich um den „Zweck" im Recht, kreist die Debatte seit geraumer Zeit vorwiegend um die Begriffe Steuerung, Regulierung und Governance. Jeder dieser Begriffe fängt einzelne Facetten des Problems ein. Mit jedem verbindet sich zudem ein bestimmtes Vorverständnis bezüglich der Fähigkeiten von Staat und Recht, auf die Gestaltung der sozialen Welt einzuwirken.[54]

[53] Die Überzeugung, dass das Recht (auch) ein Mittel zur Gestaltung sozialer Ordnungen ist, hat sich im 19. Jahrhundert durchgesetzt und ist heute so selbstverständlich geworden, dass sie tatsächlich als „trivial" gelten kann, vgl. *W. Kahl*, Über einige Pfade und Tendenzen, DV 42 (2009), S. 463 (490 Fn. 204). Zur Genealogie dieses Rechtsbegriffs ausführlich *T. Wischmeyer*, Zwecke im Recht, 2015. Zum Gestaltungsauftrag des Rechts allgemein auch: *Schmidt-Aßmann*, Das allgemeine Verwaltungsrecht als Ordnungsidee, 2. Aufl. 2006, 1/33, 2/20 ff.

[54] Vgl. *A. Voßkuhle/T. Wischmeyer*, The 'Neue Verwaltungsrechtswissenschaft' against the backdrop of traditional administrative law scholarship in Germany, in: Lindseth/Rose-Ackerman (Hrsg.), Comparative Administrative Law, 2. Aufl. 2017, S. 85 ff.

Auch wenn man diesen Vorverständnissen nie ganz entgehen kann, sollen mit dem hier vorrangig verwendeten Regulierungsbegriff allerdings nur schlanke Annahmen verbunden werden.[55] Angelehnt an *Martin Eifert* wird unter Regulierung jede Form der gezielten hoheitlichen[56] Beeinflussung individuellen Verhaltens und sozialer Prozesse verstanden, die einen über den Einzelfall hinausreichende Regelung[57] trifft und dabei „im Recht zentrales Medium und Grenze findet".[58] Dieser Regulierungsbegriff ist nicht auf bestimmte

[55] Das ausufernde Schrifttum zum Regulierungsbegriff wird auch aus diesem Grund hier nicht umfassend ausgewertet. Vgl. die Überblicksdarstellungen bei *J. Masing*, Grundstrukturen eines Regulierungsverwaltungsrechts, DV 36 (2003), S. 1 (2 ff.); *C. Franzius*, Gewährleistung im Recht, 2009, S. 416 ff.; *A. Hellgardt*, Regulierung und Privatrecht, 2016, S. 15 ff. Zur Kontroverse um den Begriff ferner auch *M. Bullinger*, Regulierung als modernes Instrument zur Ordnung liberalisierter Wirtschaftszweige, DVBl. 2003, S. 1355 ff., und – den Regulierungsbegriff auf Regelungen der Daseinsvorsorge begrenzend – *T. von Danwitz*, Was ist eigentlich Regulierung?, DÖV 2004, S. 977 ff.

[56] Der Regulierungsbegriff ist nicht auf (national-)staatliches Handeln beschränkt, sondern bezieht die Aktivitäten supra- und internationaler Organisationen sowie transnationale Koordinierungsaktivitäten von Hoheitsträgern ein.

[57] „Regelung" steht hier als Oberbegriff für alle Sätze, die sich auf kollektive Ordnungsvorstellungen stützen, einen gewissen Allgemeinheitsanspruch erheben und Verhaltenserwartungen an menschliche Akteure formulieren; „rechtliche Regelungen" sind eine Teilmenge aller Regelungen. Zu den verschiedenen, kaum in ein konsistentes Gesamtbild zu integrierenden Verwendungen der Begriffe Regel/Regelung, Norm und Gesetz, die sich zudem je nach Disziplin (Soziologie, Philosophie, Politikwissenschaft und Rechtswissenschaft) stark unterscheiden, vgl. die Beiträge in M. Iorio/R. Reisenzein (Hrsg.), Regel, Norm, Gesetz, 2010, sowie speziell *M. Iorio*, Regel und Grund, 2012. Der hiesige Begriff von Regelung ist zu unterscheiden vom Begriff der „Regelung" (Gegenbegriff: Rechtssatz) bei *K. Larenz*, Methodenlehre der Rechtswissenschaft, 6. Aufl. 1991, S. 264 ff., der dort zur Bezeichnung einer Subklasse von Rechtssätzen dient. Die weitgehende Ausklammerung von Akten, die keinen Allgemeinheitsanspruch aufweisen können, ist rein pragmatisch begründet, da solche Einzelakte für die vorliegende Untersuchung kaum interessant sind.

[58] *M. Eifert*, Regulierungsstrategien, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 3. Aufl. 2022, § 19 Rn. 5, der jedoch nicht den Regelungscharakter von Regulierung in den Vordergrund stellt, sondern Regulierung primär durch die Orientierung an einem „Ordnungszweck" (ebd.) bzw. später durch ihre Gemeinwohlorientierung definiert. Ähnlich auch *Hellgardt*, Regulierung und Privatrecht, 2016, S. 50, der Regulierung als eine der zentralen „Funktionen" des Rechts und als den „Einsatz von Recht als staatliches Instrument mit einer über den Einzelfall hinausreichenden Steuerungsintention, die auf die Implementierung politischer Allgemeinwohlziele gerichtet ist", definiert. Als solche steht die Regulierungsfunktion weiteren Rechtsfunktionen gegenüber, insbes. der Infrastruktur- und der Interessenausgleichsfunktion, wobei sich die allermeisten hoheitlichen Regeln zumindest auch der Regulierungsfunktion zuordnen lassen sollen. Ähnlich weit auch *J.-H. Binder*, Regulierungsinstrumente und Regulierungsstrategien, 2012, S. 38 f. (der allgemein von „Schutzzielen" spricht). Die hiesige Definition entlastet den Regulierungsbegriff demgegenüber von der kaum zu klärenden Frage, wann eine hoheitliche Intervention (k)einen Ordnungszweck bzw. Gemeinwohlbezug hat und stärkt mit dem Merkmal der Regelung die auch bei den hier angeführten Autoren schon präsente Differenzierung zwischen Einzelfallentscheidung und Regulierung.

Dass der hiesige Regulierungsbegriff wiederum weitgehend dem Begriff der „Norm" entspricht – vgl. zu diesem Begriff instruktiv für den vorliegenden Kontext *Finnemore/Hollis*,

Rechtsmaterien beschränkt, etwa – in U.S.-amerikanischer Tradition – auf hoheitliche Interventionsrechte im Bereich des privaten Wirtschaftslebens[59] oder – nach Maßgabe der § 3 ERegG, § 2 PostG, § 2 TKG, § 1 Abs. 2 EnWG – auf das sogenannte Regulierungsverwaltungsrecht.[60] Auch konzeptionelle Beschränkungen – etwa auf die eingreifende Staatstätigkeit – sind damit nicht verbunden.[61] Schließlich ist der hiesige Regulierungsbegriff nicht mit einem übergeordneten Wert (etwa: Effizienz)[62] oder einer metarechtlichen, insbesondere

Constructing Norms for Global Cybersecurity, AJIL 110 (2016), S. 425 (438 ff.), in Anlehnung an die in der Politikwissenschaft einflussreiche Definition von *P. Katzenstein*, Introduction, in: Katzenstein (Hrsg.), The Culture Of National Security, 1996, S. 1 (5) –, zeigt erneut, dass eine Arbeit am Regulierungs*begriff* nur bzw. jedenfalls in erster Linie zur Vermeidung von Missverständnissen notwendig ist, darüber hinaus jedoch einen begrenzten Erkenntniswert hat. Dezidiert anders als hier etwa der (von anderen Formen rechtlicher Intervention explizit unterschiedene) Gebrauch des Begriffs bei *R. Brownsword/E. Scotford/K. Yeung*, Law, Regulation, and Technology, in: dies. (Hrsg.), The Oxford Handbook of Law, Regulation, and Technology, 2017, S. 1 (6).

[59] Dieses in der U.S.- Literatur und dann auch in der ökonomischen Wissenschaft herrschende Verständnis des Begriffs, das für entsprechende Akte der Regulierung zudem eine ökonomische Rechtfertigung („Marktversagen") verlangt (dazu gleich unten § 2 Fn. 63), ist stark durch die Entstehungsgeschichte des U.S.-amerikanischen „regulatory state" geprägt. Dazu konzise *S. Breyer/R. Stewart et al.*, Administrative Law and Regulatory Policy, 9. Aufl. 2022, S. 29 ff. Ausführlich weiterhin *J. Landis*, The Administrative Process, 1938, S. 30 ff.; *R. Rabin*, Federal Regulation in Historical Perspective, Stan. L. Rev. 38 (1986), S. 1189 ff.; *C. Sunstein*, After the Rights Revolution, 1990; *M. Horwitz*, The Transformation of American Law, 1992, S. 215 ff.; *O. Lepsius*, Verwaltungsrecht unter dem Common Law, 1997, S. 78 ff.; *ders.*, Regulierungsrecht in den USA, in: Fehling/Ruffert (Hrsg.), Regulierungsrecht, 2010, § 1; vergleichend *J. Reich*, Regulierung, Regulierungsrecht und Regulatory State, Forum Historiae Iuris, 22.5.2013. Detailliert zur historischen Genese: *S. DeCanio*, Democracy and the Origins of the American Regulatory State, 2015.

[60] „Regulierung" in *diesem* Sinne bezeichnet also im Kern ein Privatisierungsfolgenrecht für netzbezogene Industrien, das charakteristische Handlungs- und Organisationsformen bündelt und vor allem durch die starke Stellung unabhängiger Regulierungsbehörden charakterisiert wird. Zu internationalen Vorbildern und weiteren Motiven für die Begriffswahl sowie zu deren Folgen vertiefend *M. Ruffert*, Regulierung im System des Verwaltungsrechts, AöR 124 (1999), S. 237 (239 f.); *Masing*, Grundstrukturen eines Regulierungsverwaltungsrechts, DV 36 (2003), S. 1 ff.; *M. Schmoeckel*, Dauerhaft engpassfreie Märkte durch «Regulierung»?, Forum Historiae Iuris, 6.2.2009, Rn. 51 ff.; *H. C. Röhl*, Soll das Recht der Regulierungsverwaltung übergreifend geregelt werden?, JZ 61 (2006), S. 831 (832); *M. Ruffert*, Begriff, in: Fehling/Ruffert (Hrsg.), Regulierungsrecht, 2010, § 7 Rn. 10 ff. Soweit Versuche unternommen wurden, die bei der Regulierung der netzgebundenen Industrien gewonnenen Einsichten im Sinne der Referenzmethode auf weitere Bereiche des Verwaltungshandelns zu übertragen, wurde auch der Anwendungsbereich *dieses* Regulierungsbegriffs erweitert. Kritisch in diesem Kontext zu einer möglichen Überdehnung des Regulierungsgedankens *M. Burgi*, Die Energiewende und das Recht, JZ 68 (2013), S. 745 (752 f.).

[61] Anders etwa *J. Braithwaite/C. Coglianese/D. Levi-Faur*, Can Regulation and Governance Make a Difference?, Regulation & Governance 1 (2007), S. 1 (3), die Regulierung und Governance (als Modus der Leistungs- und Güterverteilungspolitik) kontrastieren.

[62] Zur umfassenden Gemeinwohlorientierung von Regulierung etwa *A. Ogus*, Regulation, 2004, S. 46 ff.; *M. Feintuck*, Regulatory Rationales Beyond the Economic, in: Baldwin/

ökonomischen Theorie zur Rechtfertigung hoheitlicher Interventionen gekoppelt (Regulierung als Korrektur von „Marktversagen").[63]

Positiv charakterisiert wird der Regulierungsbegriff vielmehr durch seinen Fokus auf hoheitliches Tätigwerden und durch seinen Bezug zur – allerdings weit verstandenen – Rechtsförmigkeit.[64] Dabei werden nicht nur solche Instrumente als Formen *rechtlicher* Regulierung betrachtet, die im strengen Sinne Rechtsverbindlichkeit für sich in Anspruch nehmen können. Vielmehr wird darauf verzichtet, eine „Unterkante des Rechts" zu definieren, die überschritten sein muss, damit ein Akt in die folgende Analyse des Rechtsstoffes einbezogen werden kann.[65] Zwar gewinnen gerade die „klassischen" rechtlichen Formen wie das Parlamentsgesetz im Feld der Informationssicherheit gegenwärtig an Bedeutung. Berücksichtigt werden hier dennoch auch „alternative" hoheitliche Instrumente wie Stellungnahmen und Empfehlungen oder Innenrecht, die vor allem im überstaatlichen Kontext noch regelmäßig begegnen.[66] Klammerte man diese gänzlich aus, ließe sich nur ein stark verkürztes Bild der regulatorischen Aktivitäten in diesem Bereich zeichnen.[67] Die Bedeutung entsprechender

Cave/Lodge (Hrsg.), The Oxford Handbook of Regulation, 2010, S. 39 ff.; *Eifert*, Regulierungsstrategien, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 3. Aufl. 2022, § 19 Rn. 5.

[63] Vgl. *R. Baldwin/M. Cave/M. Lodge*, Understanding Regulation, 2. Aufl. 2012, S. 15 ff.; *Hellgardt*, Regulierung und Privatrecht, 2016, S. 34 ff. Zum konträren Problem der „regulatory capture" grundlegend *G. Stigler*, The Theory of Economic Regulation, The Bell Journal of Economics and Management Science 2 (1971), S. 3 ff. Zur (regulierungsaffinen) Verarbeitung dieses Ansatzes durch die Rechtswissenschaft einflussreich *S. Breyer*, Regulation and its Reform, 1982.

[64] Durch das Kriterium der Rechtsförmigkeit unterscheidet sich der hiesige Ansatz etwa von der einflussreichen Definition bei *P. Selznick*, Focusing Organisational Research on Regulation, in: Noll (Hrsg.), Regulatory Policy and the Social Sciences, 1985, S. 363: „sustained and focused control exercised by a public authority valued by the community".

[65] Zum Begriff *F.-C. Schroeder*, An der Unterkante des Rechts, JZ 65 (2010), S. 3611. Für den vorliegenden Zusammenhang aufgegriffen von *M. Goldmann*, Internationale öffentliche Gewalt, 2015, S. 3. Von der „Scheu" der Rechtswissenschaft, die „nicht in Rechtsformen oder rechtlich strukturierten Handlungsformen abgebildeten Maßnahmen und die von ihnen ausgelösten Wirkungen in den Blick zu nehmen" spricht *W. Hoffmann-Riem*, Rechtsformen, Handlungsformen, Bewirkungsformen, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR, Bd. 2, 2. Aufl. 2012, § 33 Rn. 26.

[66] Zum Begriff des „alternativen Instruments" vgl. *Goldmann*, Internationale öffentliche Gewalt, 2015, S. 6.

[67] Dementsprechend hat die Frage, ob und in welcher Form das Verbindlichkeitskriterium ein konstitutives Element von „Recht" ist, die in ganz unterschiedlichen Kontexten auftaucht (vgl. nur zur Diskussion um die Rechtsnatur von Verwaltungsvorschriften: *F. Ossenbühl*, Autonome Rechtsetzung der Verwaltung, in: Isensee/Kirchhof [Hrsg.], HStR, Bd. V, 3. Aufl. 2007, § 104 Rn. 60), im überstaatlichen Kontext besondere Aufmerksamkeit erhalten. Repräsentativ hierfür sind die dem seinerzeitigen „Global Administrative Law"-Projekt (GAL) zuzuordnenden Überlegungen bei *N. Krisch/B. Kingsbury*, Introduction, EJIL 17 (2006), S. 1 (12). Siehe weiter auch *M. Knauff*, Der Regelungsverbund, 2010, S. 25.

Handlungen für Recht und Rechtswissenschaft steht zudem nicht in Frage, da auch hoheitliche Akte, die nur eine mittelbare oder faktische Bindungswirkung erzeugen, im Lichte von Recht und Verfassung auf ihre Rechtfertigbarkeit geprüft werden müssen.[68] Verzichtet wird ferner darauf, diese Rechtfertigungsnotwendigkeit als Geltungserfordernis zu fassen, also nur solche (alternativen) Instrumente als „rechtlich" zu klassifizieren, die bestimmten materiellen Standards genügen.[69] Derartige Fragen sind vielmehr je separat zu prüfen.

Durch die Ausrichtung auf das hoheitliche Handeln (einschließlich des Handelns supra- und internationaler Stellen) setzt sich das hiesige Verständnis von jenen Teilen der Politik- und Sozialwissenschaften ab, die auch das Handeln privater Stellen mit einer gewissen sozialen Mächtigkeit und ohne jede Beteiligung hoheitlicher Stellen als Regulierung bezeichnen.[70] Damit soll keineswegs die Irrelevanz des Handelns Privater für die rechtswissenschaftliche Regulierungsanalyse behauptet werden. Im Gegenteil kommt den Regelungsaktivitäten Privater für die tatsächliche Verwirklichung der Informationssicherheit eine große Bedeutung zu; dies gilt etwa für die Festlegung von Stan-

---

Zur Rekonstruktion der weitgehend parallelen völkerrechtlichen Debatte zu „Soft Law", in der die Stellungnahmen für oder gegen einen engen Rechtsbegriff stark durch die jeweiligen völkerrechtstheoretischen Grundüberzeugungen geprägt sind, ausführlich *Knauff*, a. a. O., S. 213 ff.; *Goldmann*, Internationale öffentliche Gewalt, 2015, S. 169 ff. Zur Situation im Unionsrecht, in dem der Konnex von Rechtsakten und Verbindlichkeit seit jeher eher lose war, *F. von Alemann*, Notwendigkeit eines formalen Rechtsbegriffes, Der Staat 45 (2006), S. 383 ff.; *C. Bumke*, Rechtsetzung in der Europäischen Gemeinschaft, in: Schuppert/Pernice/Haltern (Hrsg.), Europawissenschaft, 2. Aufl. 2006, S. 643 (646).

[68] Pointiert *C. Möllers*, Transnationale Behördenkooperation, ZaöRV 65 (2005), S. 351 (378). *Knauff*, Der Regelungsverbund, 2010, S. 224 ff., spricht insofern von einer „Verbindlichkeit jenseits von Rechtsverbindlichkeit". Siehe auch *Goldmann*, Internationale öffentliche Gewalt, 2015, S. 7, 319 ff. Insgesamt lässt sich beobachten, dass die dichotomisierende Begriffspaarung von Recht – Verbindlichkeit – Förmlichkeit – Geltung einerseits und Nicht-Recht – Unverbindlichkeit – Informalität – Nichtgeltung andererseits einem komplexeren Analyseraster Platz macht, das die rechtliche Relevanz einer Norm mit Blick auf Kriterien wie die jeweiligen Adressaten, die Justiziabilität der Norm, ihre Eignung, als Grundlage für Eingriffe in bestimmte Rechtspositionen zu dienen, etc. prüft und auf dieser Basis differenzierte Antworten formuliert. Dieser Ansatz hebt die konstitutive Bedeutung der primären (und natürlich seinerseits streitigen) Unterscheidung von Recht/Nicht-Recht keineswegs auf. Diese Grenze bleibt zentral, um die relative Autonomie des Rechtssystems zu stabilisieren. Doch wird der exakte Grenzverlauf nicht mehr allein aus dem Begriff des Rechts hergeleitet, sondern aus der Gesamtheit der jeweiligen Rechtsordnung heraus konstruiert.

[69] Zu den entsprechenden Forderungen in Teilen der GAL-Literatur siehe *B. Kingsbury*, The Concept of 'Law' in GAL, EJIL 20 (2009), S. 23 ff. Kingsbury erklärt für das von ihm betrachtete „globale" Recht, das keinen eigentlich politischen Entstehungsprozess hat, die Befolgung bestimmter Rechtswerte zur Bedingung der rule of recognition. Plausibler erscheint demgegenüber die dialektische Konstruktion bei *Krisch/Kingsbury*, Introduction, EJIL 17 (2006), S. 1 (10).

[70] Nachgeführt wird ein solches Verständnis allerdings auch hier, wenn von (reiner) „Selbstregulierung" des Privatsektors die Rede ist.

dards im Bereich der Internetsicherheit.[71] Das entsprechende Phänomen findet sich auch in zahlreichen anderen Feldern. Entsprechend breit und facettenreich wird die Frage diskutiert, wie sich solche Aktivitäten Privater zu Formen hoheitlicher Rechtserzeugung verhalten.[72] In jüngerer Zeit hat sich diese Debatte stark auf den überstaatlichen Kontext konzentriert („transnationales Recht"); die Problematik stellt sich jedoch auch im rein nationalen Zusammenhang.[73] Die Suche nach Antworten wird dadurch erschwert, dass das entsprechende Handeln Privater ganz unterschiedliche Erscheinungsformen annehmen kann und von der Standardsetzung durch technische Experten über komplexe Vertragsnetzwerke und Musterverträge bis hin zu normativen Deklarationen reicht.[74] Unabhängig von der rechtstheoretischen Frage, ob solche (rein) privaten Abreden als „Recht" verstanden werden können oder ob Normen nur dann *Rechts*normen sind, wenn sie durch hoheitliche Stellen in einem (mehr oder weniger) formal definierten Verfahren mit (unterschiedlich weit reichendem) Verbindlichkeitsanspruch erlassen oder zumindest durch solche hoheitlichen Normen in Bezug genommen worden sind,[75] sollen in die folgende

[71] Hierzu unten § 6 II. 4.

[72] Siehe *F. Kirchhof*, Private Rechtsetzung, 1987; *L. Michael*, Rechtsetzende Gewalt im kooperierenden Verfassungsstaat, 2002; *S. Augsberg*, Rechtsetzung zwischen Staat und Gesellschaft, 2003; *G. Bachmann*, Private Ordnung, 2006; *S. Meder*, Ius non scriptum, 2. Aufl. 2009; C. Bumke/A. Röthel (Hrsg.), Privates Recht, 2012 (insbes. *G. Bachmann*, Legitimation privaten Rechts, in: a. a. O., S. 207 ff.). Siehe auch F. Möslein (Hrsg.), Regelsetzung im Privatrecht, 2019.

[73] Begrifflicher Ankerpunkt der Debatte: *P. Jessup*, Transnational Law, 1956, S. 2. Die Deutungen dieses Konzepts differieren jedoch. Vgl. einerseits etwa die anspruchsvolle Definition bei *G.-P. Calliess*, Transnationales Verbrauchervertragsrecht, RabelsZ 68 (2004), S. 244 (255): „Transnationales Recht bezeichnet eine dritte Kategorie von autonomen Rechtssystemen jenseits der traditionellen Kategorien des staatlichen nationalen und internationalen Rechts." Andere wollen den Begriff des Transnationalen hingegen nicht auf zivilgesellschaftliche Akteure beschränken, vgl. repräsentativ *Möllers*, Transnationale Behördenkooperation, ZaöRV 65 (2005), S. 351 ff. Aus der weiteren Literatur siehe nur *M. Renner*, Zwingendes transnationales Recht, 2011; C. Scott/F. Cafaggi/L. Senden (Hrsg.), The Challenge of Transnational Private Regulation, 2011; F. Cafaggi (Hrsg.), Enforcement of Transnational Regulation, 2012; *G.-P. Calliess/P. Zumbansen*, Rough Consensus and Running Code, 2012; A. Marx/M. Maertens et al. (Hrsg.), Private Standards and Global Governance, 2012; P. Jurčys/P. Kjaer/R. Yatsunami (Hrsg.), Regulatory Hybridization in the Transnational Sphere, 2013; *L. Viellechner*, Transnationalisierung des Rechts, 2013; G.-P. Calliess (Hrsg.), Transnationales Recht, 2014; T. Halliday/G. Shaffer (Hrsg.), Transnational Legal Orders, 2015; *J. Horst*, Transnationale Rechtserzeugung, 2019. Siehe jetzt umfassend P. Zumbansen (Hrsg.), The Oxford Handbook of Transnational Law, 2021.

[74] Zu den unterschiedlichen Formen und Funktionen privaten Rechts *C. Bumke/A. Röthel*, Auf der Suche nach einem Recht des privaten Rechts, in: dies. (Hrsg.), Privates Recht, 2012, S. 1 (4).

[75] Ob ein derart formaler Rechtsbegriff – als Recht gilt, was nach den Regeln der jeweiligen Rechtsordnung als Recht gilt –, der im Kern vom Staat her gedacht ist – maßgeblich ist die interne Perspektive, d. h. die Überzeugungen der Angehörigen des (hoheitlichen) Rechtsstabs –, insgesamt adäquat ist, muss hier nicht entschieden werden.

Untersuchung unmittelbar nur Normen einbezogen werden, die in einem wenigstens mittelbaren Verhältnis zu Trägern hoheitlicher Gewalt bzw. mit der Ausübung von Hoheitsgewalt befassten Stellen stehen.[76] Dabei genügt es, wenn Private von Hoheitsträgern zur Normsetzung ermächtigt werden, wenn (staatliches) Recht private Normen rezipiert oder wenn Private und Hoheitsträger bei der Normgenese gemeinsam agieren.[77] Mit dieser Weichenstellung soll die Existenz *genuin* „privaten Rechts" nicht in Abrede gestellt werden. Auch wird keineswegs verkannt, dass nicht-hoheitliche Stellen in der Weltgesellschaft zu einer eigenständigen politischen und ökonomischen Größe geworden sind, die dort teils schon traditionell von Staaten ausgeübte Funktionen übernehmen.[78] Dies trifft gerade auch auf das Feld der Informationssicherheit zu. Das spezifische Erkenntnisinteresse der vorliegenden Untersuchung gilt jedoch der Frage, ob und inwieweit Träger hoheitlicher Gewalt ihrer Verantwortung für die Sicherheit der Informationsordnung gerecht werden. Aus diesem Grund beschränkt sich die folgende Rekonstruktion der *rechtlichen* Regelungen auf solche privaten Regelungen, die in nennenswerter Weise mit den Aktivitäten von Hoheitsträgern verwoben sind. Wenn Private den Ausfall oder das Versagen hoheitlicher Regulierung durch eigene normierende Aktivitäten kompensieren müssen, ist dies auch aus der hier eingenommenen Perspektive ein bemerkenswerter Befund.

Zusammenfassend lässt sich der hiesige Arbeitsbegriff des Rechts bzw. der *rechtlichen* Regulierung also so charakterisieren, dass er, was das geforderte Maß an Verbindlichkeit betrifft, offen und inklusiv, mit Blick auf die normierenden Akteure hingegen eher eng und kriteriell ist. Der Begriff der Informationssicherheits*regulierung* bzw. allgemeiner noch der Technikregulierung nimmt dann in diesem Zusammenhang eine Perspektive auf das Recht ein, die dessen hoheitlichen Gestaltungsauftrag gegenüber der Technik akzentuiert.[79]

---

[76] Unter diesen Rechtsbegriff können ohne Schwierigkeiten Aktivitäten supra- und internationaler Stellen gefasst werden, sei es, dass aus der Binnensicht des nationalen Rechtsstabes ausreichende Ermächtigungen vorliegen oder dass auf die interne Perspektive der Angehörigen des internationalen Rechtsstabs abgestellt wird, vgl. *Knauff*, Der Regelungsverbund, 2010, S. 24 f., 45 ff.

[77] Entsprechend *Bumke/Röthel*, Auf der Suche nach einem Recht des privaten Rechts, in: dies. (Hrsg.), Privates Recht, 2012, S. 1 (2 f. m. w. N.). Zu den Formen der Verschränkung detailliert *A. von Arnauld*, Einbindung und Autonomie Privaten Rechts in die staatliche Rechtsordnung, in: Bumke/Röthel (Hrsg.), Privates Recht, 2012, S. 246 (250 ff.).

[78] Siehe neben der oben in § 2 Fn. 72 angeführten Literatur grundlegend auch *G. Teubner*, Global Law without a State, 1997; *ders.*, Global Private Regimes, in: Ladeur (Hrsg.), Public Governance in the Age of Globalization, 2004, S. 71 ff.; *T. Büthe/W. Mattli*, New Global Rulers, 2011. Vgl. auch *Vesting*, Rechtstheorie, 2. Aufl. 2015, § 5 Rn. 149 ff., 184 f.

[79] Zur Perspektivierungsfunktion des Regulierungsbegriffs ebenfalls *Eifert*, Regulierungsstrategien, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 3. Aufl. 2022, § 19 Rn. 7 ff.; ähnlich auch die Charakterisierung als „Analyseinstrument" bei *W. Durner*, Schutz

Dabei sitzt er allerdings nicht der Täuschung auf, Staat und Gesellschaft bzw. Staat und Technik operierten im Modus eines Reiz-Reaktions-Schemas, in dem das Recht anordnet und die Gesellschaft bzw. die Technik folgen. Ebenso wie die Steuerungstheorie setzt die Regulierungstheorie zwar voraus, dass eine mehr oder weniger gezielte Einwirkung auf die Gesellschaft durch Recht möglich ist. Darin setzt sie sich von Teilen der Governance-Literatur ab.[80] Aus der rechtlichen Binnenperspektive ist solch ein steuerungsaffiner Ansatz alternativlos, würde sonst doch das Selbstverständnis des modernen Rechts als sozialgestaltender Ordnung verfehlt. Aber auch aus einer rechtsexternen Sicht erscheint es jedenfalls in westlichen Verfassungsstaaten wenig plausibel, rechtsförmige Hoheitsakte auf eine Art Hintergrundrauschen für mehr oder weniger autonom handelnde horizontale Netzwerke zu reduzieren. Auf dieser Grundlage betont die Regulierungstheorie dann jedoch die Ineffizienzen und Nebenfolgen, die jeder Versuch, komplexe Handlungsfelder aus fragmentierten politischen Entscheidungsräumen heraus zu gestalten, notwendig mit sich bringt. Dies beugt Erwartungsenttäuschungen vor. Es schärft und erweitert zugleich den Blick auf das Recht und lädt zu einer komplexeren Betrachtungsweise ein. So ist den Bedingungen, unter denen rechtliche Regelungen entstehen, verstärkt Aufmerksamkeit zuzuwenden (Ressourcen wie Finanzen, Personal und eben auch Technik). Zudem ist als Teil der *lex lata* die ganze Bandbreite möglicherweise einschlägiger Regulierungsakteure, -arenen und -instrumente in den Blick zu nehmen, selbst wenn diese aus traditioneller rechtswissenschaftlicher Sicht randständig erscheinen mögen.[81] Gleiches gilt für Überlegungen zur *lex ferenda*, die fester Bestandteil der regulatorischen Analyse sind.

2. Methodische Implikationen

Eine regulatorische Analyse der Herausforderungen, mit denen Staat und Recht im Falle der Informationssicherheit konfrontiert sind, kann sich nicht auf das vertraute Feld der Auslegung von Gesetzen, Urteilen und Verwaltungsentscheidungen beschränken. Sie verlangt vielmehr neben der Einbeziehung politik- und sozialwissenschaftlicher Erkenntnisse zur Genese und zur

---

der Verbraucher durch Regulierungsrecht, in: VVDStRL 70 (2011), S. 398 (403 f.). Zur Bedeutung der Perspektivenwahl für die Methode der Wissenschaft vom Öffentlichen Recht allgemein *Voßkuhle*, Neue Verwaltungsrechtswissenschaft, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 3. Aufl. 2022, § 1, Rn. 2 ff.

[80] Siehe dazu die Nachweise bei *G. F. Schuppert*, Verwaltungsrecht und Verwaltungsrechtswissenschaft im Wandel, AöR 133 (2008), S. 79 ff.; *Voßkuhle*, Neue Verwaltungsrechtswissenschaft, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 3. Aufl. 2022, § 1 Rn. 68 ff.

[81] Vgl. *Baldwin/Cave/Lodge*, Understanding Regulation, 2. Aufl. 2012, S. 37.

Wirkungsweise von Normen auch technisches Wissen, um den Umfang des Regulierungsproblems zu bestimmen und mögliche Lösungsansätze zu identifizieren. Konkret muss sie die für die Materie prägenden technischen Zusammenhänge verarbeiten, um diese mit dem punktuell schon bestehenden Rechtsstoff sowie möglichen Regulierungsalternativen in Beziehung zu setzen.

Die mit dem Hin- und Herwandern des Blicks zwischen Lebens- und Rechtswelt verbundenen methodischen Fragen werden in der verwaltungsrechtswissenschaftlichen Literatur seit langem unter dem Stichwort der „Aufgabe" diskutiert[82] und haben in der „Neuen Verwaltungsrechtswissenschaft" ihre aktuell maßgebliche Fassung gefunden.[83] Hieran lässt sich vorliegend anschließen, wenn es darum gehen soll, einen Zugang zum Problem Informationssicherheit zu entwickeln, der das Recht über Mittel und Wege informiert, mit deren Hilfe sich Informationssicherheit faktisch und rechtlich gewährleisten lässt.

Eine größere Herausforderung – größer jedenfalls als in anderen Bereichen des staatlichen Handelns – stellt im vorliegenden Fall jedoch die Bestimmung des Umfangs der Aufgabe dar. Üblicherweise kann die Verwaltungsrechtswis-

[82] Zum Begriff der „Aufgabe" aus methodischer Sicht grundlegend *Schmidt-Aßmann*, Das allgemeine Verwaltungsrecht als Ordnungsidee, 2. Aufl. 2006, 3/79; *S. Baer*, Verwaltungsaufgaben, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 3. Aufl. 2022, § 13 Rn. 13 ff. Zur Ausbildung der „aufgabenbezogenen" Perspektive auf das Verwaltungsrecht *W. Hoffmann-Riem*, Reform des Allgemeinen Verwaltungsrechts als Aufgabe, AöR 115 (1990), S. 400 ff.; *R. Wahl*, Die Aufgabenabhängigkeit von Verwaltung und Verwaltungsrecht, in: Hoffmann-Riem/Schmidt-Aßmann/Schuppert (Hrsg.), Reform des Allgemeinen Verwaltungsrechts, 1993, S. 177 ff.; *C. Bumke*, Die Entwicklung der verwaltungsrechtswissenschaftlichen Methodik in der Bundesrepublik Deutschland, in: Schmidt-Aßmann/Hoffmann-Riem (Hrsg.), Methoden der Verwaltungsrechtswissenschaft, 2004, S. 73 ff. Zu den Konsequenzen für die rechtswissenschaftliche Arbeit *W. Hoffmann-Riem*, Methoden einer anwendungsorientierten Verwaltungsrechtswissenschaft, in: Schmidt-Aßmann/Hoffmann-Riem (Hrsg.), Methoden der Verwaltungsrechtswissenschaft, 2004, S. 9 (36); *Voßkuhle*, Neue Verwaltungsrechtswissenschaft, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 3. Aufl. 2022, § 1 Rn. 29 ff. Vorsichtiger *C. Möllers*, Theorie, Praxis und Interdisziplinarität in der Verwaltungsrechtswissenschaft, Verwaltungsarchiv 93 (2002), S. 22 ff.; *M. Jestaedt*, Perspektiven der Rechtswissenschaftstheorie, in: Jestaedt/Lepsius (Hrsg.), Rechtswissenschaftstheorie, 2008, S. 185 (202 ff.).

[83] Zum Stand der gegenwärtigen Debatte *Voßkuhle*, Neue Verwaltungsrechtswissenschaft, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 3. Aufl. 2022, § 1 Rn. 9. Der Zugriff der Neuen Verwaltungsrechtswissenschaft ist international weithin anschlussfähig, vgl. *Voßkuhle/Wischmeyer*, The 'Neue Verwaltungsrechtswissenschaft' against the backdrop of traditional administrative law scholarship in Germany, in: Lindseth/Rose-Ackerman (Hrsg.), Comparative Administrative Law, 2. Aufl. 2017, S. 85 ff.; vgl. weiter unten § 2 Fn. 93. Die Neue Verwaltungsrechtswissenschaft weist unter anderem eine enge Verwandtschaft zum „New Governance"-Paradigma auf, das im europäischen und im transnationalen Verwaltungsrecht prominent ist, vgl. dazu nur G. de Búrca/J. Scott (Hrsg.), Law and New Governance, 2006; *G. de Búrca/R. Keohane/C. Sabel*, New Modes of Pluralist Global Governance, N.Y.U. J. Int'l L. & Pol. 45 (2012–2013), S. 723 ff.; *dies.*, Global Experimentalist Governance, British Journal of Political Science 44 (2014), S. 477 ff.

senschaft insoweit an tradierte Kategorien (etwa: Gewährleistung der öffentlichen Sicherheit und Ordnung) oder an entsprechende politische Entscheidungen anknüpfen, die ausgewählten Verwaltungsträgern die Wahrnehmung einer Gruppe von Tätigkeiten mit definiertem Gemeinwohlbezug in einem abgrenzbaren Sachbereich zuweisen.[84] Im Fall der Informationssicherheit besteht über den Umfang der Aufgabe jedoch kein entsprechender Konsens; auch hat der Gesetzgeber bisher nur fragmentiert und lückenhaft gehandelt und ist, wie zu zeigen sein wird, zu zahlreichen relevanten Problemen noch gar nicht vorgedrungen. Schon aus Kompetenzgründen ist nicht zu erwarten, dass sich jene mit dem Problemfeld Informationssicherheit befassten politischen Diskurse in absehbarer Zeit zu einer einheitlichen Aufgabendefinition und zu einem im nationalen oder unionalen Rahmen konzentrierten Handlungsprogramm verdichten werden.[85] Die Rechtswissenschaft muss sich daher selbst auf die Suche nach Umfang und Grenzen des sachlichen Problemzusammenhangs machen. Nur durch eine Analyse der technischen Zusammenhänge und der daraus resultierenden Gefährdungslagen lässt sich ein zumindest plausibler Untersuchungsrahmen festlegen. Diesem Thema wird daher größere Aufmerksamkeit als üblich zu widmen sein.[86]

Schon bei der Bestimmung des Umfangs der Aufgabe, vor allem aber bei der Analyse der Instrumente stellt sich zudem die Frage, auf welche interdisziplinären Wissensbestände die Rechtsetzung zurückgreifen kann – mit direkten Implikationen für die dieser Regulierung gewidmete (verwaltungs-)rechtswissenschaftliche Forschung. Offensichtlich kommt hierbei dem informati-

[84] Zur Unmöglichkeit einer geschlossenen Staatsaufgabenlehre und zum politischen Charakter der Aufgabenzuweisung siehe nur *Schmidt-Aßmann*, Das allgemeine Verwaltungsrecht als Ordnungsidee, 2. Aufl. 2006, 3/79. Ebd. auch zur etablierten Unterscheidung von öffentlicher Aufgabe (Sachbereich mit Gemeinwohlbezug), Staatsaufgabe (dem Staat oder einer sonstigen hoheitlichen Einrichtung zugewiesene öffentliche Aufgabe) und Verwaltungsaufgabe (der Verwaltung zur Wahrnehmung zugewiesene Staatsaufgaben).

Jüngere Forschungen zeigen deutlich, dass sich Entscheidungen über die Aufgabenzuweisung oft weniger an sachlichen Kriterien als an politischen Präferenzen, Aufmerksamkeitsökonomien und institutionellen Vorentscheidungen orientieren. Vgl. dazu die Beiträge in Heft 1 dms 8 (2015) zum Themenschwerpunkt „Entstehung und Wandel von Politikfeldern", insbes. *K. Loer/R. Reiter/A. Töller*, Was ist ein Politikfeld und warum entsteht es?, dms 8:1 (2015), S. 7 ff. Allgemein zur Politikfeldentstehung *V. Schneider/F. Janning*, Politikfeldanalyse, 2006, S. 48 ff.; sowie die entsprechenden Beiträge in G. Wenzelburger/R. Zohlnhöfer (Hrsg.), Handbuch Policy-Forschung, 2015. Siehe auch *J. Kingdon*, Agendas, Alternatives, and Public Policies, 2. Aufl. 1995; *A. Töller*, Regieren als Problemlösung oder als eigendynamischer Prozess?, in: Egner/Haus/Terizakis (Hrsg.), Regieren, 2012, S. 171 ff. Die Pathologien dieses Prozesses zeigt gerade die „Digitalpolitik", vgl. *S. Haunss/J. Hofmann*, Entstehung von Politikfeldern – Bedingungen einer Anomalie, dms 8:1 (2015), S. 29 ff.; dazu bereits oben § 1 Fn. 20. Dass aus einer neuen Herausforderung klar definierte politische und rechtliche Materien entstehen können, zeigen etwa die Sozial- und Umweltpolitik bzw. das Sozial- und Umweltrecht.

[85] Hierzu unten § 5 III. 1.

[86] Hierzu unten § 6.

onstechnischen Schrifttum und den einschlägigen technischen Normen, die das technische Wissen zur Informationssicherheit aggregieren, zentrale Bedeutung zu. Beispielhaft nennen lassen sich die ISO/IEC 2700x-Reihe, die mehr als 20 Standards zur Informationssicherheit umfasst und die von der International Organization for Standardization (ISO) und der International Electrotechnical Commission (IEC) verwaltet wird, die Publikationen des BSI und die Requests for Comments (RFC) der Internet Engineering Task Force (IETF).[87] Allerdings kann gerade das in den technischen Normen oder in der sonstigen Fachliteratur präsentierte Wissen nicht schlicht übernommen werden. Zu sehr unterscheiden sich Erkenntnisinteresse der Ingenieure und juristischer Zugriff. Vielmehr ist aus regulatorischer Sicht der Sachbereich in einer Weise zu rekonstruieren, der für juristische Fragestellungen anschlussfähig ist. Soweit es damit bereits für die Rekonstruktion der Aufgabe Informationssicherheit erforderlich ist, den sozialen und technischen Grundlagen der vernetzten Informationsordnung, ihrem Aufbau, potenziellen Gefährdungslagen und möglichen Schutzmechanismen, Aufmerksamkeit zu widmen, gilt also, dass das Ziel der „Realbereichsanalyse" nicht schlicht die Beschreibung der „Sachlage" ist.[88] Vielmehr verfolgt die Rechtswissenschaft auch dann, wenn ihr Fokus auf der Aufgabe liegt, in ihrer Annäherung an Problemzusammenhänge, wie jede Disziplin, ein eigenständiges Erkenntnisinteresse, das ihre Wahrnehmung des Realbereichs prägt. Der juristische Blick ist nie deckungsgleich mit der Perspektive anderer Disziplinen oder der internen Sicht der Dinge. Das juristische Interesse gilt vielmehr stets primär jenen den Realbereich konstituierenden Handlungen, Routinen und Kommunikationen, deren Kenntnis nötig ist, um den Problemzusammenhang als rechtliches Pflichtenprogramm zu rekonstruieren. Weil die genuin (verwaltungs-)rechtliche Arbeit akteurs-, regime- und regelorientiert ist, ist die Rechtswissenschaft eben besonders an den darauf bezogenen Informationen aus dem untersuchten Sachbereich interessiert – unabhängig davon, ob diese Informationen innerhalb der unmittelbar zuständigen Fachdisziplin als besonders bedeutsam eingestuft werden. Dieser Punkt ist zu gegebener Zeit zu präzisieren.

[87] Vgl. weiter zu den maßgeblichen technischen Normungsinstanzen und Normen unten § 6 II. 6. b).

[88] Der Begriff „Realbereich" darf also nicht dahin missverstanden werden, dass Norm- und Realbereich zwei getrennte Sphären wären, vgl. dazu weiter *Voßkuhle*, Neue Verwaltungsrechtswissenschaft, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 3. Aufl. 2022, § 1 Rn. 29 ff. Vgl. zum konstruktiven Aspekt der Realbereichsanalyse auch *M. Eifert*, Innovationen in und durch Netzwerkorganisationen, in: ders./Hoffmann-Riem (Hrsg.), Innovation und rechtliche Regulierung, 2002, 88 (101).

3. Alter Wein in neuen Schläuchen?!

Stattdessen ist an dieser Stelle noch zu betonen, dass das hier entworfene methodische Programm dem Projekt einer „dogmatischen" Rechtswissenschaft in keiner Weise entgegengesetzt ist.[89] Die Gegenüberstellung einer rechtsdogmatisch purifizierten und einer entformalisierenden, interdisziplinär offenen Verwaltungsrechtswissenschaft ist seit langem als unproduktiv erkannt.[90] Dementsprechend lassen sich auch „aufgabenbezogene" und „dogmatische" Verwaltungsrechtswissenschaft nicht gegeneinander ausspielen, sondern verweisen aufeinander, schon weil das geltende Recht als – jedenfalls ein – maßgeblicher Bezugspunkt der dogmatischen Arbeit vielfältig mit dem Aufgabenbegriff

[89] Dass sich Regulierungsgedanke und juristische Methode und Dogmatik nicht gegeneinander ausspielen lassen, sondern einander ergänzen, betonen bereits *A. Voßkuhle*, Methode und Pragmatik im Öffentlichen Recht, in: Bauer/Czybulka et al. (Hrsg.), Umwelt, Wirtschaft und Recht, 2002, S. 171 (188 f.); *Schmidt-Aßmann*, Das allgemeine Verwaltungsrecht als Ordnungsidee, 2. Aufl. 2006, 2/20 ff.; *I. Appel*, Das Verwaltungsrecht zwischen klassischem dogmatischen Verständnis und steuerungswissenschaftlichem Anspruch, in: VVDStRL 67 (2008), S. 226 ff.; *M. Eifert*, Das Verwaltungsrecht zwischen klassischem dogmatischen Verständnis und steuerungswissenschaftlichem Anspruch, in: VVDStRL 67 (2008), S. 286 ff.

[90] Sie wird freilich immer wieder aufgewärmt, so etwa bei *K. Gärditz*, Die „Neue Verwaltungsrechtswissenschaft" – Alter Wein in neuen Schläuchen?, in: Burgi (Hrsg.), Zur Lage der Verwaltungsrechtswissenschaft, 2017, S. 105 (125). Dessen gegen die Neue Verwaltungsrechtswissenschaft gerichtete Polemik lässt allerdings in methodischer Hinsicht alle Fragen offen, etwa wenn einerseits gegen interdisziplinäre Öffnung ins Feld geführt wird, das Verwaltungsrecht „sollte Diskurse mit rechtlichen Argumenten führen" (a. a. O., S. 141), andererseits aber durchgängig eine „theorie- und kontextsensible" Dogmatik angemahnt wird (a. a. O., Fn. 182 und 184). Denn was ist die Neue Verwaltungsrechtswissenschaft, wenn nicht der Versuch, ein Programm für eine theorie- und kontextsensible Dogmatik vorzulegen? Die von *Gärditz* der Neuen Verwaltungsrechtswissenschaft unterstellte Frontstellung zur Dogmatik bzw. zur juristischen Methode hat sich diese so nie zu eigen gemacht, sondern stets das Komplementaritäts- und Ergänzungsverhältnis betont, vgl. nur zusammenfassend *Voßkuhle/Wischmeyer*, The 'Neue Verwaltungsrechtswissenschaft' against the backdrop of traditional administrative law scholarship in Germany, in: Lindseth/Rose-Ackerman (Hrsg.), Comparative Administrative Law, 2. Aufl. 2017, S. 85 (91 ff.).

Darüber, ob die Neue Verwaltungsrechtswissenschaft ihrem Anspruch auf eine theorie- und kontextsensible Dogmatik gerecht wird, lässt sich natürlich streiten. Der springende Punkt ist jedoch ein anderer. Wie jüngst *Alexander Somek* herausgearbeitet hat, harrt die rechtstheoretische Grundsatzfrage, an der sich eine nicht nur polemische Kritik der Neuen Verwaltungsrechtswissenschaft abarbeiten müsste, ob es ein spezifisch rechtliches, gewissermaßen „autonomes" Wissen gibt, durch das sich das Recht von seinen Nachbardisziplinen unterscheiden lässt, weiter der Klärung, vgl. *A. Somek*, Rechtstheorie zur Einführung, 2017, S. 10 ff. Die Leistung der Neuen Verwaltungsrechtswissenschaft besteht aus meiner Sicht darin, für das Verwaltungsrecht gezeigt zu haben, wie anspruchsvoll und prekär eine starke Autonomie-These ist – ohne sie damit jedoch preiszugeben. Einen Anspruch auf Lösung der rechtstheoretischen Grundsatzfrage erhebt sie nicht. Zur Notwendigkeit kontextsensibler Rechtswissenschaft allgemein jüngst *A.-B. Kaiser*, Ausnahmeverfassungsrecht, 2020, S. 17 ff.

operiert.[91] Zudem bündelt eine präzise Rekonstruktion der regulatorischen Aufgabe die durch rechtliche Regulierung verfolgten Ziele und gibt damit einen auch rechtsintern relevanten Maßstab für die Bewertung der zur Zielerreichung eingesetzten regulatorischen Mittel vor. Ignorieren lässt sich dies allenfalls unter stabilen gesellschaftlichen Bedingungen und in einer weitgehend konstanten regulatorischen Umgebung. Hier mag der Eindruck entstehen, Rechtsdogmatik sei inhärent statisch und rechtsdogmatisches Wissen und Arbeiten könne auf Anregungen durch außerfachliche Perspektiven und Weltwahrnehmungen verzichten.[92] Ob eine solche Situation je wirklich existiert hat oder stets nur eine Projektion auf die Vergangenheit war, sei hier dahingestellt – jedenfalls ist das öffentliche Recht der Gegenwart von einer solchen

[91] Die internen Ausdifferenzierungen der Debatte um die als Rechtsdogmatik bezeichnete Denk- und Argumentationsweise sind zu komplex, um hier weiter ausgelotet zu werden. Vgl. dazu nur grundlegend *W. Brohm*, Die Dogmatik des Verwaltungsrechts vor den Gegenwartsaufgaben in der Verwaltung, in: VVDStRL 30 (1972), S. 245 ff.; *R. Alexy*, Theorie der juristischen Argumentation, 1978, S. 307 ff.; *Schmidt-Aßmann*, Das allgemeine Verwaltungsrecht als Ordnungsidee, 2. Aufl. 2006, 1/4 ff.; *M. Eifert*, Zum Verhältnis von Dogmatik und pluralisierter Rechtswissenschaft, in: Kirchhof/Magen/Schneider (Hrsg.), Was weiß Dogmatik?, 2012, S. 79 ff.; *C. Bumke*, Rechtsdogmatik, JZ 69 (2014), S. 641 ff.; *ders.*, Rechtsdogmatik, 2017; *A. Stark*, Interdisziplinarität der Rechtsdogmatik, 2020, S. 21 ff. (a. a. O., S. 233 ff., auch instruktive Ausführungen zur Interdisziplinarität der Rechtsdogmatik). Zur internationalen Perspektive siehe nur *A. von Bogdandy*, Doctrinal Constructivism, I•CON 7 (2009), S. 364 ff.; *P. Chrétien*, Frankreich, in: von Bogdandy/Cassese/Huber (Hrsg.), IPE, Bd. IV, 2011, § 58 Rn. 42 ff.; *S. Cassese*, New Paths for Administrative Law, I•CON 10 (2012), S. 603 ff.

Im Übrigen ist die Beobachtung, dass in jedem Rechtsakt empirische Annahmen und normative Setzungen zusammenkommen in dem – dem Informationssicherheitsrecht nahestehenden – Technik- und Umweltrecht seit langem selbstverständlich, vgl. *Hoffmann-Riem*, Methoden einer anwendungsorientierten Verwaltungsrechtswissenschaft, in: Schmidt-Aßmann/Hoffmann-Riem (Hrsg.), Methoden der Verwaltungsrechtswissenschaft, 2004, S. 9 (36 ff.). Sie gilt jedoch auch für das vermeintlich formale Verwaltungsverfahrensrecht, vgl. *A. Voßkuhle*, Strukturen und Bauformen neuer Verwaltungsverfahren, in: Hoffmann-Riem/Schmidt-Aßmann (Hrsg.), Verwaltungsverfahren und Verwaltungsverfahrensgesetz, 2002, S. 277 ff.

[92] So kann in Zeiten relativer dogmatischer Stabilität die Analyse der Ziele und Aufgaben an praktischer Relevanz verlieren, sodass ihnen nur noch eine heuristische Funktion zugeschrieben wird, vgl. etwa *O. Bachof*, Die Dogmatik des Verwaltungsrechts vor den Gegenwartsaufgaben in der Verwaltung, in: VVDStRL 30 (1972), S. 194 (223 ff.). Jede größere Reform stört jedoch diese Stabilität und wirft die Frage nach den Aufgaben neu auf. Als historische Beispiele dafür, dass sich verwaltungsrechtswissenschaftliche Reformprojekte über den Aufgabenbegriff konstituieren, siehe nur *E. Forsthoff*, Verwaltungsrecht, 10. Aufl. 1973, S. 368; *P. Badura*, Verwaltungsrecht im liberalen und im sozialen Rechtsstaat, 1966, S. 20; *Wahl*, Die Aufgabenabhängigkeit von Verwaltung und Verwaltungsrecht, in: Hoffmann-Riem/Schmidt-Aßmann/Schuppert (Hrsg.), Reform des Allgemeinen Verwaltungsrechts, 1993, S. 177 ff. Zur Responsivität der Dogmatik Otto Mayers gegenüber dem seinerzeitigen sozialen und politischen Kontext vgl. nur *Bumke*, Die Entwicklung der verwaltungsrechtswissenschaftlichen Methodik in der Bundesrepublik Deutschland, in: Schmidt-Aßmann/Hoffmann-Riem (Hrsg.), Methoden der Verwaltungsrechtswissenschaft, 2004, S. 73 (85); *Wischmeyer*, Zwecke im Recht, 2015, S. 110 ff., 217 ff.

Stabilität weit entfernt.[93] Dies zeigt bereits seine Selbstwahrnehmung, die von anhaltender methodischer Unruhe geprägt ist.[94] Da das Recht die ihm im Zuge des Wandels neu zugewiesenen Aufgaben oft nicht mit den hergebrachten Routinen bearbeiten kann, kommt der Reflexion über Aufgaben und Kontexte der Regulierung in solchen Situationen besondere Bedeutung zu. Gleiches gilt für die verstärkte Auseinandersetzung mit den Voraussetzungen und Wirkungen der neuen rechtlichen Regeln.[95] Eben eine solche Situation, die es

[93] Auslöser der letzten methodischen Welle sind komplexe Veränderungen im politischen System seit Beginn der 1980er-Jahre, die sich – versetzt und mit unterschiedlichen Akzentuierungen – in einem Großteil der westlichen Verfassungsstaaten ereignet haben. Zu diesen Entwicklungen und den entsprechenden Diskussionen in transnationaler Perspektive siehe u. a. *W. Eskridge*, The New Public Law Movement, Mich. L. Rev. 89 (1991), S. 707 ff.; *J. Bourgon*, New Public Administration Theory, International Review of Administrative Sciences 73 (2007), S. 7 ff.; *M. Ruffert*, Transformation of Administrative Law, in: Ruffert (Hrsg.), The Transformation of Administrative Law in Europe, 2007, S. 3 ff.; *J.-P. Schneider*, Regulation and Europeanisation, in: Ruffert (Hrsg.), The Transformation of Administrative Law in Europe, 2007, S. 309 ff.; *J.-B. Auby*, Die Transformation der Verwaltung und des Verwaltungsrechts, in: von Bogdandy/Cassese/Huber (Hrsg.), IPE, Bd. III, 2010, § 56; *Chrétien*, Frankreich, in: von Bogdandy/Cassese/Huber (Hrsg.), IPE, Bd. IV, 2011, § 58; *Cassese*, New Paths for Administrative Law, I•CON 10 (2012), S. 603 ff.; *K.-P. Sommermann*, Objectives and Methods, in: Blanke/Cruz Villalón et al. (Hrsg.), Common European Legal Thinking, 2015, S. 543 ff.

Die Ursachen für diese Veränderungen – hierzu zählen die sogenannte „Krise des regulativen Rechts" (vgl. *K. Günther*, Der Wandel der Staatsaufgaben und die Krise des regulativen Rechts, in: Grimm [Hrsg.], Wachsende Staatsaufgaben – sinkende Steuerungsfähigkeit des Rechts, 1990, S. 50 ff.; *Voßkuhle*, Neue Verwaltungsrechtswissenschaft, in: Voßkuhle/Eifert/Möllers [Hrsg.], GVwR, Bd. 1, 3. Aufl. 2022, § 1, Rn. 10 ff.), der Aufstieg des Gewährleistungsparadigmas (dazu *M. Eifert*, Grundversorgung mit Telekommunikationsleistungen im Gewährleistungsstaat, 1998; *A. Voßkuhle*, Beteiligung Privater an der Wahrnehmung öffentlicher Aufgaben und staatliche Verantwortung, in: VVDStRL 62 [2003], S. 266 ff.; G. F. Schuppert [Hrsg.], Der Gewährleistungsstaat, 2004; *Franzius*, Gewährleistung im Recht, 2009), die Europäisierung (dazu nur *R. Wahl*, Die zweite Phase des Öffentlichen Rechts, Der Staat 38 [1999], S. 495 ff.) und die Genese der Informationsgesellschaft (dazu nur *W. Hoffmann-Riem*, Einleitende Problemskizze, in: ders./Schmidt-Aßmann [Hrsg.], Verwaltungsrecht in der Informationsgesellschaft, 2000, S. 9 ff.; vgl. weiter die Nachweise oben bei § 2 Fn. 46) – sind vielfach ausführlich beschrieben worden und müssen hier nicht rekapituliert werden.

[94] Seismographisch *C. Möllers*, Braucht das öffentliche Recht einen neuen Methoden- und Richtungsstreit?, Verwaltungsarchiv 90 (1999), S. 187 ff.; *A. Voßkuhle*, Die Reform des Verwaltungsrechts als Projekt der Wissenschaft, DV 32 (1999), S. 545 ff. Weniger erfolgsversprechend ist es hingegen offenbar, wenn Methodendiskussionen gezielt initiiert werden, um dogmatischen Wandel zu befördern; vgl. etwa den in den 1970er-Jahren unternommenen und weitgehend gescheiterten Versuch, Sozialwissenschaften in die juristische Forschung zu integrieren: D. Grimm (Hrsg.), Rechtswissenschaften und Nachbarwissenschaften, Bd. 1 und 2, 1973; *H. Rottleuthner*, Rechtswissenschaft als Sozialwissenschaft, 1973; W. Hoffmann-Riem (Hrsg.), Sozialwissenschaften im öffentlichen Recht, 1981.

[95] Vgl. dazu allgemein etwa *A. Voßkuhle*, Rechtstatsachenforschung und Verwaltungsdogmatik, VerwArch 85 (1994), S. 567 ff.; *ders.*, Neue Verwaltungsrechtswissenschaft, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 3. Aufl. 2022, § 1, Rn. 29 ff., sowie – je mit unterschiedlichen Schwerpunkten – die mittlerweile klassischen Darstellungen zur Proble-

nötig macht, eine neue Kategorie von Zielen und Aufgaben ins Medium des Rechts zu übersetzen, liegt nun vor, wenn es darum geht, die Sicherheit der Informationsinfrastrukturen in Staat und Gesellschaft mit den Mitteln des Rechts zu beeinflussen.

Anzuerkennen ist bei alldem jedoch, dass den Rechtswissenschaften vielfach das methodische Rüstzeug fehlt, um selbst in unmittelbar benachbarten Fächern wie der Soziologie oder der Politikwissenschaft Debatten bewerten und das dort reflektierte Wissen einordnen zu können.[96] Noch größere Rezeptionsbarrieren bestehen wohl im Umgang mit technischem Wissen.[97] Der methodisch kontrollierte Transfer entsprechender Erkenntnisse bleibt daher ein in hohem Maße selektives und konstruktives Unterfangen.[98] Allerdings können für die Berücksichtigung nachbarwissenschaftlicher Erkenntnisse gewissermaßen meta-methodologische Mindeststandards entwickelt werden, die zumindest einen naiven oder strategisch-verzerrten Zugriff verhindern. Erforderlich sind stets (a) eine spezifische Rechtfertigung für den Rückgriff, (b) Transparenz bei der Einbeziehung derartiger Erkenntnisse, (c) gegebenenfalls eine Erklärung für den Zugriff auf einen spezifischen Erkenntnisstand im Fach und (d) Schutzmechanismen gegen Überkomplexität.[99] Diese Standards geben keine Blaupause für erfolgreiche Interdisziplinarität, sondern dienen als Erinnerungsmarker bei der Aufbereitung und Integration fachfremder Begriffe und Wissensbestände. Sie werden bei der nachfolgenden Analyse zu beachten sein.

---

matik: *A. Roßnagel*, Technikfolgenforschung, 1993; *C. Böhret*, Gesetzesfolgenabschätzung, 2. Aufl. 1997; H. Hof/G. Lübbe-Wolff (Hrsg.), Wirkungsforschung zum Recht I, 1999; H. Hill/H. Hof (Hrsg.), Wirkungsforschung zum Recht II, 2000; H. Hof/M. Schulte (Hrsg.), Wirkungsforschung zum Recht III, 2001; U. Karpen/H. Hof (Hrsg.), Wirkungsforschung zum Recht IV, 2003.

[96] Siehe dazu u. a. die Beiträge in I. Augsberg (Hrsg.), Extrajuridisches Wissen, 2013 (darin insbes. *A.-B. Kaiser*, Multidisziplinäre Begriffsverwendungen, S. 99 ff.); L. Münkler (Hrsg.), Dimensionen des Wissens im Recht, 2019.

[97] Deutlich wird dies, wenn man die Technik primär als eigenständige epistemische Gemeinschaft versteht, dazu unten § 3 I.

[98] Unverändert gültig: *W. Hoffmann-Riem*, Sozialwissenschaften im Verwaltungsrecht, in: Die Wissenschaft vom Verwaltungsrecht, DV Beiheft 2 (1999), S. 83 (85); *Voßkuhle*, Methode und Pragmatik im Öffentlichen Recht, in: Bauer/Czybulka et al. (Hrsg.), Umwelt, Wirtschaft und Recht, 2002, S. 171 (182 ff.).

[99] Ausführlich hierzu bereits *C. Möllers/A. Voßkuhle*, Die Deutsche Staatsrechtswissenschaft im Zusammenhang der internationalisierten Wissenschaften, DV 26 (2003), S. 321 ff.; *T. Vesting*, Nachbarwissenschaftlich informierte und reflektierte Verwaltungsrechtswissenschaft, in: Schmidt-Aßmann/Hoffmann-Riem (Hrsg.), Methoden der Verwaltungsrechtswissenschaft, 2004, S. 253 ff.; *Hoffmann-Riem*, Methoden einer anwendungsorientierten Verwaltungsrechtswissenschaft, in: Schmidt-Aßmann/Hoffmann-Riem (Hrsg.), Methoden der Verwaltungsrechtswissenschaft, 2004, S. 9 (60 ff.). Gerade die Bedeutung des letztgenannten Punktes darf nicht unterschätzt werden. Vielmehr gilt es stets, die institutionellen und prozeduralen Grenzen von Rechtswissenschaft und -praxis im Auge zu behalten. Siehe im Übrigen auch *C. Engel*, Rationale Rechtspolitik und ihre Grenzen, JZ 60 (2005), S. 581 ff.

Erster Teil

Grundlagen des Informationssicherheitsrechts

§ 3 Informationssicherheitsrecht als Technikregulierung

> „*Die Technik* tut nichts, sondern wir tun uns mit ihr etwas an, was keineswegs heißt, dass wir die Folgen unseres Handelns überblicken."[1]

Die Digitalisierung fordert Staat und Gesellschaft in vielfältiger Form heraus. Dass dies aus rechtlicher Sicht nicht nur neue Fragen aufwirft, wird insbesondere dann deutlich, wenn man einen Aspekt der Digitalisierung in den Vordergrund stellt, der – obschon offensichtlich – selten betont wird: ihre technische Dimension. Soweit das Recht Impulse für die digitale Technik setzen möchte, ist dies letztlich Teil jener Bemühungen des Staates um die Technik, die bis in die Zeiten der (ersten) Industriellen Revolution zurückreichen. Unter dem Gesichtspunkt der Informationssicherheit liegt die Betonung der technischen Dimension der Digitalisierung sogar besonders nahe, beruht die Verwundbarkeit doch gerade auf Schwächen technischer Systeme wie Netzen und IT-Systemen. Vor allem aber ist die Gewährleistung der Sicherheit von Produkten seit jeher das Zentrum des Technikrechts.

Dennoch ist das Recht der Informationssicherheit bisher nur sehr punktuell als genuin technikrechtliche Materie analysiert worden.[2] Hierfür dürfte verantwortlich sein, dass Fragen der Informationssicherheit meist als Annex anderer Rechtsmaterien erörtert werden, etwa des Datenschutzrechts.[3] Welche Instrumente die gesetzlichen Regelungen zur Informationssicherheit mit anderen dem Technikrecht[4] zugeordneten Materien verbinden, wird detailliert im zweiten Teil dieser Untersuchung zu würdigen sein.[5] In diesem Kapitel soll zunächst die grundlegendere Frage adressiert werden, was es für das Recht im

---

[1] *U. Wengeroth*, Technik der Moderne, 2015, S. 2.

[2] Siehe allerdings *H. Federrath/A. Pfitzmann*, Datensicherheit, in: Schulte/Schröder (Hrsg.), Handbuch des Technikrechts, 2011, S. 857 ff. Vgl. weiter allgemein zur technikrechtlichen Erörterung von Fragen des Informations- und Kommunikationsrechts: *M. Kloepfer/C. Franzius/T. Weber*, Technik und Recht im wechselseitigen Werden, 2002, S. 108 ff.; *P.-T. Stoll*, Sicherheit als Aufgabe, 2003, S. 284 ff.; *I. Spiecker gen. Döhmann*, Rechtliche Begleitung der Technikentwicklung, in: Hill/Schliesky (Hrsg.), Die Vermessung des virtuellen Raums, 2012, S. 137 ff.

[3] Hierzu oben § 2 I.

[4] Zu diesem Begriff gleich unter § 3 II. 3.

[5] Dazu unten § 7.

Allgemeinen und das Informationssicherheitsrecht im Besonderen bedeutet, wenn es sich in ein regulatives Verhältnis zur Technik setzt. Dabei muss zunächst dem Begriff der Technik, der in der rechtswissenschaftlichen Literatur immer noch weitgehend unausgearbeitet ist, Aufmerksamkeit geschenkt werden. Denn ohne ein angemessenes Verständnis des Phänomens Technik lässt sich der Beitrag des Rechts zur Technikgestaltung nicht adäquat bestimmen. Plausibel gemacht werden soll hier ein Begriff der Technik, der diese (auch) als soziales System erfasst (I.). Auf dieser Grundlage werden dann unterschiedliche Ansätze, das Verhältnis von Recht und Technik zu fassen, vorgestellt, die zu einem Konzept der Technikregulierung als Modus der Strukturierung des Kommunikationsprozesses zwischen Recht und Technik zusammengeführt werden (II.). Dieses Modell wird im späteren Verlauf der Arbeit mit Leben zu füllen sein. Zuvor soll jedoch noch zu klären sein, weshalb die Annäherung des Rechts an die *Informations*technik die Frage nach der Technik wenigstens zeitweise aus dem Blick verloren hatte (III.).

I. Zur Gestaltbarkeit der Technik

1. Technik als Schicksal?

Gesellschaftliche, (staats-)rechtliche und technische Entwicklung stehen, wie die historische Forschung vielfach gezeigt hat, in einem engen Zusammenhang. So wandelt sich die Organisation staatlicher Herrschaft im Zuge der technologischen Entwicklung.[6] Politische Gemeinschaften verändern mit dem Fortschritt der Informations- und Kommunikationstechnologien ihre Rhyth-

[6] Vgl. nur die einflussreichen Überblicksdarstellungen von *D. Headrick*, Tools of Empire, 1981; *W. McNeill*, The Pursuit of Power, 1982; *R. Jervis*, The Meaning of the Nuclear Revolution, 1989 (speziell zur Nukleartechnologie); *G. Herrera*, Technology and International Transformation, 2006 (aus Sicht der internationalen Beziehungen); *D. Headrick*, Power over Peoples, 2010. Zur besonders strittigen Frage nach der Bedeutung der typischerweise staatlich geförderten Militärtechnologie für die allgemeine technologische Entwicklung vgl. pars pro toto die instruktive Diskussion zwischen *F. Kittler*, Auto Bahnen, in: Emmerich/Wege (Hrsg.), Der Technikdiskurs in der Hitler-Stalin-Ära, 1995, S. 114 ff., und *E. Schütz*, Faszination der blaßgrauen Bänder, in: a. a. O., S. 123 ff. Zusammenfassend auch *R. Mayntz*, Triebkräfte der Technikentwicklung und die Rolle des Staates, in: Simonis/Martinsen/Saretzki (Hrsg.), Politik und Technik, 2001, S. 3 ff. Vgl. im Übrigen bereits die differenzierten Überlegungen zur Rolle der Technik im Kapitel „Maschinerie und grosse Industrie" bei *Karl Marx*, Das Kapital, Bd. 1 (1867), in: MEW Bd. 23, Berlin 1959, S. 391 ff.; zur Weiterentwicklung *K. Bayertz/M. Quante*, Marxistische Technikphilosophie, in: Grunwald (Hrsg.), Handbuch Technikethik, 2013, S. 89 ff. In der rechtswissenschaftlichen Literatur spricht *A. Roßnagel*, Rechtswissenschaftliche Technikfolgenforschung, 1993, S. 67, treffend von „gegenseitigen Anpassungsprozessen"; *V. Boehme-Neßler*, BilderRecht, 2010, S. 1 ff., hält die „Entweder-Oder-Kontroverse" für heute weitgehend überwunden. Speziell zur Rolle staatlicher Akteure in der Frühzeit der *digitalen* Technologien siehe unten § 4 II. 1. c).

men.[7] Neue Technologien erschließen zuvor unzugängliche Territorien und erweitern damit die Räume politischer Gestaltbarkeit.[8] Moderne Staatlichkeit mit ihrem Dreiklang aus Staatsgewalt, Staatsvolk und Staatsgebiet ist somit auch eine spezifische technische Konstellation – mit Rückwirkungen auf das jeweilige (Verfassungs-)Recht.

Die hier wirkenden Mechanismen lassen sich nicht auf ein technikdeterministisches Basis-Überbau-Modell reduzieren. Technik ist keine naturwüchsige Kraft, die sich die Gesellschaft nach ihrem Bilde formt.[9] Umgekehrt implementiert die Technik auch nicht schlicht die herrschenden gesellschaftlichen Ideale. Stattdessen besteht ein komplexes Mit-, Neben- und Gegeneinander von gesellschaftlichen Ordnungsbestrebungen und technischer Entwicklung. Dieses auf einen Begriff zu bringen, hat sich als schwierig erwiesen.

Jener berühmten Debatte der Nachkriegszeit, in der die Frage nach der Technik kurzzeitig zum beherrschenden Thema der Geistes- und Gesellschaftswissenschaften wurde, ist dies jedenfalls nicht gelungen. So wurde es der Sache nicht gerecht, wenn Staat und Gesellschaft von den Vertretern der technischen Kybernetik als mit technischen Mitteln zu lösende Problemzusammenhänge konstruiert wurden.[10] Umgekehrt überzeugte es nicht, wenn die Technik bzw. der Technizismus als eine die menschlichen Beziehungen auf Zweck-Mittel-Relationen reduzierende und die Welt umfassend verfügbar

[7] Aus der unüberschaubaren Literatur beispielhaft für unterschiedliche Medienarten *L. Febvre/H.-J. Martin*, L'Apparition du livre, 1958; *J. Habermas*, Strukturwandel der Öffentlichkeit (1962), 1990; *R. Deibert*, Parchment, Printing, and Hypermedia, 1997. Vgl. auch die einschlägigen Beiträge in U. Dolata/R. Werle (Hrsg.), Gesellschaft und die Macht der Technik, 2007; *T. Vesting*, Die Medien des Rechts: Buchdruck, 2013; *ders.*, Die Medien des Rechts: Computernetzwerke, 2015; *M. Hildebrandt*, Smart Technologies and the End(s) of Law, 2016, S. 47 ff.

[8] Zu den hier bestehenden Wechselbeziehungen insbes. *T. Hughes*, Networks of Power, 1983. Siehe auch *A. Fickers/P. Griset*, Communicating Europe, 2019, S. 239 ff.

[9] Vgl. neben der gerade zitierten historischen Literatur auch *W. Bijker*, Of Bicycles, Bakelites, and Bulbs, 1995; *L. Bennett Moses*, How to Think about Law, Regulation and Technology, Law, Innovation and Technology 5:1 (2013), S. 1 (2).

[10] Siehe dazu nur *B. Seibel*, Berechnendes Regieren, Zeithistorische Forschungen/Studies in Contemporary History 9 (2012), S. 334 ff.; *ders.*, Cybernetic Government, 2016; *ders.*, Staat am Draht, Zeitschrift für Ideengeschichte 11:1 (2017), S. 5 ff. Siehe auch *P. Hurni*, Cybernetics, German Public Administration and the Reframing of the Public Servant in the Neo-Verwaltungswissenschaft, in: Sager/Overeem (Hrsg.), The European Public Servant, 2015, S. 175 ff., sowie philosophisch kontextualisierend *V. August*, Technologisches Regieren, 2021. Die Vorstellung, dass „in etwa zwanzig Jahren" staatliches Handeln weitgehend durch Maschinen erledigt würde, war dabei weit verbreitet, vgl. etwa die Prognosen bei *H. Simon*, The Shape of Automation for Men and Management, 1965, S. 96; *M. Minsky*, Computation, 1967. Zu Vorläuferbewegungen – darunter insbes. die positive Technikphilosophie von *F. Dessauer*, Philosophie der Technik, 1926 – näher H.-L. Dienel (Hrsg.), Der Optimismus der Ingenieure, 1998.

machende Verirrung kritisiert wurde.[11] Differenziertere Bestandsaufnahmen, die die technische Entwicklung nicht resignativ als Verhängnis begriffen oder aber utopistischen Vorstellungen einer Regierung der Technik oder einer nicht-entfremdeten „nachtechnologischen" Technik nachhingen,[12] sondern die in der Technik einen positiven Gestaltungsauftrag für Staat und Gesellschaft erkannten, ohne die damit verbundenen Schwierigkeiten zu leugnen, hatten es demgegenüber schwer, sich auf dem Markt der Ideen zu behaupten.[13] Ursache hierfür war auch, dass die Debattenteilnehmer ein verhältnismäßig geringes Interesse daran hatten, die Technik „in ihren realen Wirkungszusammenhängen" zu erfassen.[14] Stattdessen dominierten globale Positionsbestimmungen gegenüber „der" Technik als „geschichtsmächtiger Potenz"[15] die Debatte.[16] Diese Form der Distanznahme gegenüber dem untersuchten

[11] Zu der für den Technikdiskurs dieser Zeit prägenden Gegenwartsdiagnose siehe die Schriften des Soziologen und Gründers der neuen Leipziger Schule*: H. Freyer*, Theorie des gegenwärtigen Zeitalters, 1955, S. 79 ff.; *ders.*, Über das Dominantwerden technischer Kategorien (1960), in: ders.: Herrschaft, Planung und Technik, 1987, S. 117 ff. Ähnliche Diagnosen bei *A. Gehlen*, Die Seele im technischen Zeitalter, 1957; *H. Schelsky*, Der Mensch in der wissenschaftlichen Zivilisation, 1961. Einflussreich insbes. auch das nach 1945 mehrfach neu aufgelegte Werk von *F. G. Jünger*, Die Perfektion der Technik, 1939. Zu den Vorläufern der konservativen Technikkritik der Nachkriegszeit siehe *R. Sieferle*, Fortschrittsfeinde?, 1984, S. 155 ff.

Ähnliche Kritik kam jedoch auch von links. Weitgehend analog zu Freyer argumentierte etwa *H. Marcuse*, Some Social Implications of Modern Technology, Studies in Philosophy and Social Science 9 (1941), S. 414 ff.; *ders.*, Industrialisierung und Kapitalismus, in: Stammer (Hrsg.), Max Weber und die Soziologie heute, 1964, S. 161 (179). Kritisch dazu *C. Offe*, Technik und Eindimensionalität, in: Habermas (Hrsg.), Antworten auf Herbert Marcuse, 1968, S. 73 ff., der Marcuse „eine erstaunliche und beunruhigende Verwandtschaft zu konservativ-institutionalistischen Analysen von Autoren wie Hans Freyer, Helmut Schelsky und Arnold Gehlen" attestiert (a. a. O., S. 81). Zu den gleichwohl bestehenden Bruchlinien zwischen linker und rechter Technikkritik *G. Ropohl*, Allgemeine Technologie, 3. Aufl. 2009, S. 24; *F. Meinel*, Der Jurist in der industriellen Gesellschaft, 2011, S. 460 f.

Zu weiteren technikskeptischen Bewegungen in der Geschichte instruktiv insbesondere *L. Marx*, The Machine in the Garden, 1964; *W. Klems*, Die unbewältigte Moderne, 1988; *C. Müller/B. Nievergelt*, Technikkritik in der Moderne, 1996; *M. Spehr*, Maschinensturm, 2000; *S. Jones*, Against Technology, 2006. Elemente dieser Skepsis leben heute in Teilen der digitalisierungskritischen Literatur fort, vgl. unten § 4 II. 1. c).

[12] *H. Marcuse*, Der eindimensionale Mensch, 1967, S. 249.

[13] Siehe neben den sogleich sowie in § 3 I. 2. und § 3 I. 3. zitierten Werken insbes. auch *J. Habermas*, Technischer Fortschritt und soziale Lebenswelt (1965), in: ders., Technik und Wissenschaft als „Ideologie", 1968, S. 104 ff.

[14] So aber dann *Ropohl*, Allgemeine Technologie, 3. Aufl. 2009, S. 17; *A. Grunwald*, Technik, in: ders. (Hrsg.), Handbuch Technikethik, 2013, S. 13 (14).

[15] *E. Forsthoff*, Technische Realisation und politische Ordnung, in: Schatz (Hrsg.), Auf dem Weg zur hörigen Gesellschaft?, 1973, S. 183 (198).

[16] Hierfür steht paradigmatisch die von *Martin Heidegger* seit den 1930er-Jahren entwickelte Philosophie der Technik, vgl. insbes. *M. Heidegger*, Die Frage nach der Technik (1953), in: ders., Vorträge und Aufsätze, 1954, S. 13 ff.; *ders.*, Die Technik und die Kehre, 1962; plakativ auch *ders.*, Nur noch ein Gott kann uns retten, in: Der Spiegel 30 H. 23 (1976), S. 193 (206): „Die Technik in ihrem Wesen ist etwas, was der Mensch von sich aus nicht bewältigt". Dieser Ansatz lässt sich hier nicht näher entfalten.

Phänomen erwies sich letztlich für Theoriebildung und Praxis gleichermaßen als unfruchtbar.[17]

2. Technik jenseits von Mittel und Zweck

Dennoch dauerte es seine Zeit, bis sich in der philosophischen und soziologischen Literatur alternative Ansätze etablieren konnten. Erst in den 1970er-Jahren begannen Analysen, die sich mit den Entstehensbedingungen und dem Kontext technischer Systeme befassten, die ontologischen oder metaphysischen Deutungen der Technik abzulösen. Dem Zug der Zeit entsprechend zeichnete sich diese neue Literatur durch einen großen Methoden- und Themenpluralismus aus.[18] Auf einen einfachen Begriff lassen sich die hier verhandelten Fragen nicht bringen, schon gar nicht auf einen Begriff, den die Rechtswissenschaft ihrer Befassung mit der Technik zu Grunde legen könnte.[19] Nachvollziehbar war daher die seinerzeit von *Dietrich Murswiek* formulierte Anfrage, „ob der Jurist das versuchen sollte, was den Technikern selbst nicht gelingt, und was diejenigen, die berufsmäßig über Technik nachdenken, die Technik-Philosophen, für unmöglich halten, nämlich einen allgemeinen Begriff von Technik zu formulieren".[20]

Tatsächlich wäre ein solch allgemeiner Begriff auch heute für die Rechtswissenschaft weder hilfreich noch erforderlich: Nicht erforderlich, weil zur praktischen Arbeit an technikrechtlichen Normen regelmäßig ein Alltagsverständnis davon ausreicht, was Technik und technische Risiken sind. Dieses genügt für den Gesetzgeber und die Verwaltung, die Einfluss auf die Entwicklung und den Gebrauch von Technik nehmen möchten, ebenso wie für die Rechts-

[17] Vgl. resümierend *N. Luhmann*, Die Gesellschaft der Gesellschaft, 1997, S. 522: „Inzwischen mehren sich jedoch Anzeichen dafür, daß auch diese Kontrastierung von Technik und Natur oder Technik und Humanität (Technik und Vernunft, Technik und ‚Lebenswelt' usw.) verbraucht ist."

[18] Vgl. die Überblicksdarstellungen bei *H. Lenk*, Zu neueren Ansätzen der Technikphilosophie, in: Lenk/Moser (Hrsg.), Techne, Technik, Technologie, 1973, S. 198 ff.; *F. Rapp*, Analytische Technikphilosophie, 1978; C. Hanks (Hrsg.), Technology and Values, 2010; C. Hubig/A. Huning/G. Ropohl (Hrsg.), Nachdenken über Technik, 3. Aufl. 2013, daraus insbes. instruktiv *F. Rapp/G. Ropohl*, Historische und systematische Übersicht, in: a.a.O, S. 41 ff.; *C. Hubig*, Historische Wurzeln der Technikphilosophie, in: a. a. O., S. 19 ff.

[19] Vgl. die Einschätzung bei *Lenk*, Zu neueren Ansätzen der Technikphilosophie, in: Lenk/Moser (Hrsg.), Techne, Technik, Technologie, 1973, S. 198 (210), der die „Technik" beschreibt als „ein begriffliches Orientierungskonstrukt eigener Vieldeutigkeit, das nicht im Sinne eines Gattungsbegriffs Elemente umfasst, die durch einen gemeinsamen Wesenszug gekennzeichnet wären".

[20] *D. Murswiek*, Die staatliche Verantwortung für die Risiken der Technik, 1985, S. 73. Entsprechend *Grunwald*, Technik, in: ders. (Hrsg.), Handbuch Technikethik, 2013, S. 13: „Ein philosophisch und wissenschaftlich durchgehend anerkannter Technikbegriff liegt nicht vor."

wissenschaft, die diesen Versuch analytisch begleitet. Ein allgemeiner Technikbegriff wäre aber auch kaum hilfreich, müsste er mit Blick auf die naturwissenschaftliche Prägung und die soziale Einbettung der Technik doch so abstrakt sein, dass er für die normativ-pragmatische Grundgrammatik des Rechts kaum anschlussfähig und damit im regulatorischen Diskurs schwer zu verarbeiten wäre.[21]

Auch wenn die rechtswissenschaftliche Auseinandersetzung mit den Begriffs- und Theorieangeboten der techniksoziologischen und -philosophischen Literatur daher nicht mit letzter Konsequenz auf Begriffsbildung zielen sollte, kann diese Literatur durchaus ein präziseres Verständnis von dem Gegenstand vermitteln, mit dem das Recht zu tun hat, wenn es versucht, Technik zu fördern oder ihr Grenzen zu ziehen. Insbesondere lassen sich so mögliche Ansatzpunkte und Herausforderungen identifizieren, die beim Versuch rechtlicher Intervention in technische Zusammenhänge zu berücksichtigen sind. Vier Punkte sind insoweit zu bedenken.

Erstens gilt es, eine zentrale Unterscheidung im Blick zu behalten. Nach der klassischen Definition *Max Webers* bedeutet die „‚Technik' eines Handelns […] den Inbegriff der verwendeten *Mittel* desselben im *Gegensatz* zu jenem Sinn oder Zweck, an dem es letztlich orientiert ist, ‚rationale' Technik eine Verwendung von Mitteln, welche bewusst und planvoll orientiert ist an Erfahrungen und Nachdenken, im Höchstfall der Rationalität: an wissenschaftlichem Denken. Was in concreto als ‚Technik' gilt, ist also flüssig".[22] Weber und mit ihm zahlreiche weitere Autoren verstehen unter Technik also nicht nur verkörperte *Gegenstände* (Artefakte), sondern auch rationalen Standards folgende *Verfahren* wie die Kompositions-, Kalkulations-, Staatstechnik etc.[23] Diese Doppelung liegt in der Natur der Sache, denn Artefakt und

[21] Deutlich zeigen dies etwa die Bemühungen von *P. Marburger*, Die Regeln der Technik im Recht, 1979, S. 21 f., der – unter Bezugnahme auf *Lenk*, Zu neueren Ansätzen der Technikphilosophie, in: Lenk/Moser (Hrsg.), Techne, Technik, Technologie, 1973, S. 198 ff. – die Technik „ausgehend von ihren sinnlich wahrnehmbaren Manifestationen und deren Funktionen" definiert „als die Erzeugung (Produktion) und Verwendung (Konsumtion) materieller, energetischer und informationeller Umwandlungs-, Speicherungs- oder Transportsysteme". Diese anspruchsvolle Definition bleibt für die anschließende einsichtsreiche juristische Analyse der Regeln der Technik im Recht jedoch gänzlich folgenlos. Allgemein zur Problematik (unreflektierter) Theorie- und Begriffsimporte im Recht *A. Voßkuhle*, „Schlüsselbegriffe", VerwArch 93 (2002), S. 184 ff.

[22] *M. Weber*, Wirtschaft und Gesellschaft, 5. Aufl. 1980, S. 32.

[23] Zu dieser „Dualität" vieler Technikbegriffe näher *Grunwald*, Technik, in: ders. (Hrsg.), Handbuch Technikethik, 2013, S. 13. Komplexer noch die Aufgliederung bei *C. Hubig*, Technik als Medium, in: Grunwald (Hrsg.), Handbuch Technikethik, 2013, S. 118 (119): „Technik als ‚Inbegriff der Mittel' versammelt Mittel kategorial inhomogener Art wie (1) einschlägige Fähigkeiten und Fertigkeiten, (2) die in bestimmten Verfahrensschemata (Prozesstypes) bestimmten Weisen des Herstellens und Veränderns von Dingen, Zuständen und Verfahren selbst, (3) das Wissen um diese Schemata (auch ‚Technologie'), (4) das konkrete Agieren und Prozessieren (als *token*) des Bewirkens, (5) die bei diesem Bewirken ein-

Prozess lassen sich nicht strikt voneinander trennen, erfolgt die Herstellung von Artefakten doch stets in Verfahren (Berechnungen etc.), die sich wiederum typischerweise materialer Artefakte (Stift, Computer etc.) bedienen müssen. Dennoch ist gerade die materiale Verkörperung – und sei sie so ephemer wie die geschriebene Note oder das digitale Datum im Speicher-Chip – das Charakteristikum der Technik, das sie von anderen Formen geistigen Tätigwerdens abhebt und das sie zugleich zu etwas mehr und anderem als einem reinen Mittel-Zweck-Schema bzw. einer Erscheinungsform der (instrumentellen) Vernunft macht. Eben dies betont auch *Günter Ropohl* in seiner einflussreichen Bestimmung der Technik als „(a) die Menge der nutzenorientierten, künstlichen, gegenständlichen Gebilde (Artefakte oder Sachsysteme), (b) die Menge menschlicher Handlungen und Einrichtungen, in denen Sachsysteme entstehen und (c) die Menge menschlicher Handlungen, in denen Sachsysteme verwendet werden."[24]

Ropohls Ansatz verweist neben der Materialität auf das *zweite* für die Technik wesentliche Moment: die Verbindung gegenständlicher Gebilde mit menschlichen Handlungen bzw. die Einbindung der Technik in einen gesellschaftlichen Kontext. Technik ist keine naturwüchsige Kraft, die das Fundament weiterer geistiger und kultureller Entwicklungen bildet. Sondern sie ist anthropogen und damit stets Ausdruck und Produkt eines spezifischen kulturellen Kontextes. Diese Einsicht hat ab den 1980er-Jahren ein technikdeterministisches Verständnis abgelöst, wie es noch in der These von der Technik als „Geschick" der Menschheit in der Nachkriegszeit herrschend war.[25] Seither gilt das Interesse der technikspezifischen Forschung primär dem in die Gesellschaft eingebetteten „sozio-technischen System". Dieses umfasst das Artefakt ebenso wie den Prozess seiner Entstehung, die Praktiken seines Gebrauchs, die Folgen seines Einsatzes und die Formen seines Verschwindens. Ausführlich wird zudem der Einfluss normativer und kognitiver Leitbilder auf die Technikgenese thematisiert.[26] Nach dem Vorbild von Wissenschaftssoziologie und -theorie geraten zudem die Selektionsmechanismen, Organisationsfor-

gesetzten Artefakte als raumzeitliche Entitäten und schließlich (6) die Ergebnisse eines derartigen Bewirkens als realisierte Zwecke (im Unterschied zu natürlich gewordenen/‚gewachsenen'), die ihrerseits als Mittel einsetzbar sind".

[24] *Ropohl*, Allgemeine Technologie, 3. Aufl. 2009, S. 31. Zum Begriff des „Sachsystems", der bei Ropohl an die Stelle von Begriffen wie „Maschine", Gerät, Apparat etc. tritt und die Menge der technischen Hervorbringungen bezeichnet, siehe a. a. O., S. 117 ff.

[25] Programmatisch die auf dem 26. Deutschen Soziologentag 1986 erhobene Forderung, „technische Gegenstände als soziale Phänomene und technische Entwicklung als sozialen Prozeß" zu verstehen: *B. Lutz*, Das Ende des Technikdeterminismus und die Folgen, in: ders. (Hrsg.), Technik und sozialer Wandel, 1987, S. 34 (44).

[26] Zu diesem Ansatz im Überblick: W. Bijker/T. Hughes/T. Pinch (Hrsg.), The Social Construction of Technological Systems, 1987; *S. Beck/J. Niewöhner/E. Sörensen*, Science and Technology Studies, 2014.

men und Regelwerke der für die Technikentwicklung maßgeblichen epistemischen Gemeinschaften in den Blick. Das Gewicht, das die Literatur den sozialen Faktoren im Verhältnis zur Materialität der Technik zuschreibt, differiert. Bei einigen Autoren verschwindet das Artefakt weitgehend hinter dem sozialen Aushandlungsprozess, andere betonen stärker den Eigensinn des Objekts. Die Details dieser Diskussionen können hier außer Betracht bleiben.[27] Wesentlich ist, dass sich das Verhältnis von Recht und Technik nicht nur als Verhältnis von sozialer Ordnung und (bloßem) Objekt, sondern immer auch als Verhältnis zweier zueinander in Wechselbeziehung stehender sozialer Ordnungen darstellt. Mit dieser Einsicht eröffnen sich neue Spielräume für die Gestaltung und Regulierung der Technik. Insbesondere ist das Recht nicht mehr darauf beschränkt, das konkrete technische Objekt anzusprechen, etwa um dessen Nutzung zu untersagen; die soziale Genese und die Einbindung des Artefakts in soziale Netzwerke machen es vielmehr möglich und notwendig, Einfluss auf die in den Netzwerken organisierten Akteure und die für die Technikentwicklung maßgeblichen sozialen und materiellen Konstellationen zu nehmen. In der Rechtswissenschaft selbst sind solche Überlegungen rasch rezipiert und auf Formeln wie „Technik und Recht im wechselseitigen Werden" gebracht worden. Auf diesen Punkt wird gleich zurückzukommen sein.[28]

Die Einbettung technischer Artefakte in soziale Kontexte erteilt *drittens* der Vorstellung eine Absage, Technik sei ein neutrales Mittel für nicht-neutrale Zwecke.[29] Nicht nur der Einsatz technischer Mittel, sondern bereits der Entwurf technischer Leitbilder und die Genese von technischen Artefakten stellt eine soziale Praxis dar und lässt sich somit kritisch auf ihre (Vor-)Urteile befragen. Plastisch wird dies, wo sich „die Technik" institutionell als regelsetzende Gemeinschaft konstituiert, in der Ingenieure oder Programmierer nach eigenen Traditionen und Präferenzen (technische) Regeln festlegen und anwenden.[30] Diese Diskurse können und müssen mit der Rechtfertigungsfrage konfrontiert werden. Die spätere Verwendung der Systeme lässt sich dabei allenfalls künstlich ausblenden. Je nach Kontext haben diese Diskurse nicht nur

[27] Vgl. zur Vertiefung die Überblickswerke B. Joerges/H. Nowotny (Hrsg.), Social Studies of Science and Technology: Looking Back, Ahead, 2003; S. Bauer/T. Heinemann/T. Lemke (Hrsg.), Science and Technology Studies, 2017; U. Felt/R. Fouché et al. (Hrsg.), The Handbook of Science and Technology Studies, 4. Aufl. 2017.

[28] Unter § 3 II.

[29] Grundlegend *D. Ihde*, Technics and Praxis, 1979, S. 4: „relations with machines are non-neutral in the sense that they, by their very use, imply reflexive results for ourselves." Konzise dazu auch *Boehme-Neßler*, BilderRecht, 2010, S. 5 m. w. N. Siehe bereits – wenn auch noch mit einem anderen Einschlag – *C. Schmitt*, Das Zeitalter der Neutralisierungen und Entpolitisierungen (1929), in: ders., Positionen und Begriffe, 4. Aufl. 2014, S. 138 (147): „Die Technik ist immer nur Instrument und Waffe, und eben weil sie jedem dient, ist sie nicht neutral."

[30] *B. Joerges*, Soziologie und Maschinerie, in: Weingart (Hrsg.), Technik als sozialer Prozeß, 1989, S. 44 (46 f.).

eine ethische,[31] sondern auch eine politische[32] Dimension. Wenn Technik bzw. die mit ihr befassten Akteure aber auf diese Weise schon immer in ein Netz von Gründen und normativen Diskursen eingesponnen sind, dann wirft die Ansprache der Technik durch das Recht keine kategorial neuen Herausforderungen auf, sondern zieht lediglich eine weitere Reflexions- und Rechtfertigungsebene in den technikinternen Diskurs ein bzw. bindet diesen in eine weitere Kommunikationsbeziehung ein. Die Anschlussfähigkeit rechtlicher Argumente im technischen Diskurs darf daher, jedenfalls im Grundsatz, vorausgesetzt werden.

Vor diesem Hintergrund spricht *viertens* alles dafür, sich bei der Untersuchung sozio-technischer Systeme von einem allzu strikten Verständnis des Zweck-Mittel-Schemas zu lösen. Ohnehin hat dieses Schema in einer post-teleologischen Welt nur begrenzten Erklärungswert, ist dem einen doch oft Mittel, was dem anderen Zweck ist.[33] Vor allem aber lassen sich technische Systeme keineswegs so eindeutig, wie es dies etwa noch Max Weber erschien, der Seite der Mittel zuordnen.[34] Zwar mögen technische Systeme in einer konkreten Verwendungssituation aus der Sicht des jeweiligen Verwenders in erster Linie Mittel zu einem außerhalb ihrer selbst liegenden Zweck sein. Betrachtet man die Verwendungsrelation von außen, ist jedoch oft schon weit weniger klar, was Zweck und was Mittel ist. So stellt sich auf Seiten des Verwenders die

[31] Frühzeitig in diese Richtung *N. Wiener*, The Human Use of Human Things, 1950; *ders*., God and Golem, Inc., 1963. Einflussreich hierzu auch *H. Jonas*, Technology and Responsibility, Social Research 40 (1973), S. 31 ff.; ausgeführt in *ders.*, Das Prinzip Verantwortung, 1979. Hieran schließt heute eine ganze Disziplin, die Technikethik, an, vgl. dazu die Nachweise bei *T. Wischmeyer/E. Herzog*, Digitale Ethik in der Demokratie, JZ 74 (2019), S. 696 ff., darunter insbesondere zur Ethik der Digitaltechnik *S. Hansson*, The Ethics of Technology, 2017; W. Wallach/P. Asaro (Hrsg.), Machine Ethics and Robot Ethics, 2017; *S. Spiekermann*, Digitale Ethik, 2019.

[32] Vielzitiert das Robert-Moses-Beispiel bei *L. Winner*, Do Artifacts Have Politics?, Daedalus 109 (1980), S. 121; vgl. auch *ders.*, The Whale and the Reactor, 1986. Daran anknüpfend mit Blick auf den Datenschutz *H. Nissenbaum*, From Preemption to Circumvention, Berkeley Tech. L. J. 26 (2011), S. 1367 ff. Kritisch-differenzierend *B. Joerges*, Do Politics Have Artefacts?, Social Studies of Science 29 (1999), S. 411 ff. Vgl. umgekehrt die instruktive Kritik an politikfernen Spielarten der sozialkonstruktivistischen Technikforschung bei *L. Winner*, Upon Opening the Black Box and Finding It Empty, Science, Technology, & Human Values 18 (1993), S. 362 ff. Die Forderung bei *U. Beck*, Risikogesellschaft, 1986, S. 372, nach Reflexivität und „subpolitischer Kontrolle" der Technikentwicklung setzt ebenfalls hier an.

[33] Vgl. *Ropohl*, Allgemeine Technologie, 3. Aufl. 2009, S. 162: „Aus der soziotechnischen Arbeitsteilung erwachsen die normativen Probleme der Technisierung, und diese verlangen eine sorgfältige Analyse, die nicht dadurch ersetzt werden kann, dass man einem angeblich verselbständigten „Reich der technischen Mittel" eine dämonische Eigengesetzlichkeit andichtet. Wenn sich in der modernen Gesellschaft etwas verselbständigt hat, dann sind es nicht die technischen Mittel, sondern die ökonomischen Ziele." Siehe auch *Hubig*, Technik als Medium, in: Grunwald (Hrsg.), Handbuch Technikethik, 2013, S. 118 (121).

[34] Vgl. die Nachweise bei *S. Neuffer*, Zwecklose Technik, 2019, S. 57 f.

Frage, wie sehr dieser gegenüber den von ihm genutzten Dingen tatsächlich autonom ist.[35] Seitens der Technik gerät der ganze Vorgang der Technikgenese in den Blick, in dem das jetzt eingesetzte Produkt im Akt der Verwendung selbst seinen Zweck erfüllt. Zu Recht wird daher angemerkt, dass die „handlungstheoretische Struktur des Technikbegriffs […] viel reicher [ist] als es das einfache Zweck-Mittel-Bild suggeriert."[36] Damit soll nicht geleugnet werden, dass die Qualität als Mittel ein technisches System in vielen Konstellationen brauchbar charakterisieren kann. Doch eröffnet die Erkenntnis, dass sich ein sozio-technisches System immer auch selbst als Zweck betrachten lässt, neue Möglichkeiten der Kritik. Von einer höheren Warte aus ließe sich an dieser Stelle nun durchaus wieder in Frage stellen, ob es die Technik als abgrenzbaren Phänomenbereich überhaupt „gibt", oder ob Technik letztlich nicht doch eher eine Perspektive auf die Welt unter dem Gesichtspunkt ihrer Instrumentalisierbarkeit bezeichnet.[37] Mit dieser wieder an Weber anschließenden Frage – so interessant sie sein mag – verlässt man jedoch jene Theorieebene, die für die rechtswissenschaftliche Forschung noch anschlussfähige Erkenntnisse erwarten lässt.[38]

3. Technik als soziales System und als Möglichkeitsraum

Diese Überschau kann und soll nicht mehr als eine Grundorientierung vermitteln und verbreiteten Verkürzungen vorbeugen. Gezeigt wurde, dass das Recht in der Technik weder einem planetarischen Geschick noch einer bloßen Denkweise, Form oder Komplexitätsreduktionsstrategie begegnet.[39] Die Rede

[35] Harmlos mit Blick auf das hier in Frage stehende Autonomieverständnis ist der alltägliche Fall, dass das zuhandene „Mittel" seine Verwender erst neue „Zwecke" entdecken lässt, siehe bspw. die Analyse bei *S. Ramsay*, Reading Machines, 2011. Ähnlich bereits *Luhmann*, Die Gesellschaft der Gesellschaft, 1997, S. 523. In radikalisierter Form findet sich diese Beobachtung auch bei *Freyer*, Über das Dominantwerden technischer Kategorien, in: ders.: Herrschaft, Planung und Technik, 1987, S. 117 (124).

[36] *Grunwald*, Technik, in: ders. (Hrsg.), Handbuch Technikethik, 2013, S. 13. Vgl. auch ausführlich *C. Hubig*, Mittel, 2002.

[37] *A. Grunwald/Y. Julliard*, Technik als Reflexionsbegriff, Philosophie naturalis 2005, S. 127 ff., im Anschluss an *P. Janich*, Logisch-pragmatische Propädeutik, 2001, S. 151 f.

[38] Vgl. in diese Richtung die Bestimmung der Technik als „System der Dienlichkeit und Herbeiführbarkeit, als Ermöglichung des Gelingens instrumenteller Vollzüge" bei *Hubig*, Technik als Medium, in: Grunwald (Hrsg.), Handbuch Technikethik, 2013, S. 118 (121). Vgl. auch die Bestimmung bei *Heidegger*, Die Technik und die Kehre, 1962, S. 12: „Die Technik ist also nicht bloß ein Mittel. Die Technik ist eine Weise des Entbergens." Bei *E. Forsthoff*, Technisch bedingte Strukturwandlungen des modernen Staates, in: Freyer/Papalekas/Weippert (Hrsg.), Technik im technischen Zeitalter, 1965, S. 211 (212), findet sich die Formulierung von der Technik als „Prinzip der Verfügbarmachung der Mittel der Natur für menschliche Zwecke".

[39] Zu letzterem tendiert allerdings *Luhmann*, Die Gesellschaft der Gesellschaft, 1997, S. 525.

von einer „Eigendynamik“ der Technikentwicklung, von irreversiblen „Sachzwängen“ oder von einer „Verselbstständigung“ der Mittel verfehlt daher, jedenfalls wenn sie unreflektiert gebraucht wird, was Technik ausmacht.[40] Vielmehr trifft das Recht in sozio-technischen Systemen auf eine soziale Konstellation, ein Netzwerk, und auf einen „Möglichkeitsraum“ (*Christoph Hubig*), der seinerseits die Möglichkeiten unseres Handelns prägt.[41] Die Aufgabe und Herausforderung des Rechts im Umgang mit der Technik liegt darin, diesen Möglichkeitsraum zu erschließen und zu gestalten.

II. „Recht und Technik“ revisited

Die Rechtswissenschaft war weder schneller noch langsamer als andere Geistes- und Sozialwissenschaften in ihrer Annäherung an die Technik. Lange bevor es hier zu produktiven Ansätzen kam, hatte die Rechtspraxis jedoch bereits auf die Regulierungsnotwendigkeit der Technik reagiert und – weitgehend ohne wissenschaftliche Unterstützung – Regelungen geschaffen, in denen die Technik als „Möglichkeitsraum“ anerkannt wurde. So zerfällt bis weit in die zweite Hälfte des 20. Jahrhunderts hinein die Befassung des Rechts mit der Technik in eine pragmatische, sachangemessene, im einfachen Recht vorangetriebene Regulierung einerseits und einen der Technik zunächst mit Ignoranz, dann immer offener mit Skepsis begegnenden Wissenschaftsdiskurs andererseits (1.). Erst mit der Einsicht in die verfassungsrechtliche Dimension der Thematik verändert sich ab den 1970er-Jahren die Debattenlage (2.). Der konkreten Struktur der Kommunikation zwischen Recht und Technik wird seither ebenso wie der technikermöglichenden Funktion des Rechts deutlich größere Aufmerksamkeit geschenkt (3.).

---

[40] *C. Hubig*, Die Kunst des Möglichen II, 2007, S. 29; *Ropohl*, Allgemeine Technologie, 3. Aufl. 2009, S. 17.

[41] *Hubig*, Die Kunst des Möglichen II, 2007, S. 16 f. Das ist etwas anderes als die Idee, dass sich in der Technik eine autonome Kraft manifestiert. Vgl. *Ropohl*, Allgemeine Technologie, 3. Aufl. 2009, S. 17: „Da wird mit der Technokratie-These die Behauptung aufgestellt, die Technik gehorche einer inneren Eigengesetzlichkeit, die dem Menschen jede Möglichkeit bewusster Planung und Gestaltung verstelle und ihn zum willenlosen Spielball seiner eigenen Konstrukte mache. Auch die Experten in Wissenschaft und Technik, in denen man zunächst die Agenten der Technokratie gesehen hatte, seien nichts Anderes als die Erfüllungsgehilfen einer sich von selbst durchsetzenden Sachgewalt technischer Perfektion. Wenn hier die Technik zu einer autonomen Macht hypostasiert und wenn sie zum geheimnisvollen Dämon stilisiert wird, dann zeugt solche Mystifikation davon, wie wenig die Technik in ihren realen Wirkungszusammenhängen begriffen wird.“ In diesen „Kräften“ manifestieren sich regelmäßig die nicht-intendierte Nebenfolgen unseres Umgangs mit der Technik.

1. Von der Technikignoranz der Rechtswissenschaft …

Ende des 19. Jahrhunderts waren Staat und (Industrie-)Gesellschaft umfassend von den „empirischen Vorgegebenheiten einer zunehmend sich technifizierenden Welt" geprägt.[42] Auch der Gesetzgeber hatte sich die neue Welt erschlossen. Als „paradigmatischer Einschnitt" für die Rechtsentwicklung in Deutschland gilt allgemein die in den 1830er-Jahren einsetzende „Dampfkesselgesetzgebung", in der die für das Technikrecht typische Form ineinander greifender hoheitlicher und privater Regulierung etabliert wurde, organisatorisch umgesetzt im parallelen Aufbau staatlicher Fachbehörden und privater Standardisierungsvereine.[43] Die Annäherung des Rechts an die Welt der technischen Artefakte und Verfahren fiel dem Gesetzgeber zwar nicht leicht. So musste für den neuen Gegenstand zunächst einmal eine „sprachliche Fassung und [eine] kulturelle Deutung" gefunden werden.[44] Dies nahm geraume Zeit in Anspruch. Um 1900 war jedoch eine Konsolidierung der wesentlichen regulatorischen Prinzipien und Instrumente gelungen.[45] Auch die internationale Koordinierung war weit vorangeschritten.[46] Während die explodierenden Dampfkessel die Risiken privater Technik vor Augen führten, die durch Gesetz einzuhegen waren, standen zeitgleich Telegraph, Elektrizität und Eisenbahn für die Erfolge staatlicher Technikförderung. Letztere vollzog sich allerdings weitgehend unterhalb der Ebene des Gesetzes.[47] Der auf den Schutz von

[42] *R. Koselleck*, Geschichte, Geschichten und formale Zeitstrukturen, in: ders. (Hrsg.), Geschichte, Ereignis und Erzählung, 1973, S. 211 (221).

[43] Die Forschungsgruppe zum „Recht in der Industriellen Revolution" am Max-Planck-Institut für Europäische Rechtsgeschichte hat diese Geschichte umfassend aufgearbeitet, vgl. *M. Vec*, Recht und Normierung in der Industriellen Revolution, 2006; *M. Seckelmann*, Industrialisierung, Internationalisierung und Patentrecht, 2006; *L. Jellinghaus*, Zwischen Daseinsvorsorge und Infrastruktur, 2006; *I. vom Feld*, Kontrollierte Staatsentlastung im Technikrecht, 2007 (speziell zur Dampfkesselgesetzgebung); sowie als Gesamtüberblick *M. Vec*, Kurze Geschichte des Technikrechts, in: Schulte/Schröder (Hrsg.), Handbuch des Technikrechts, 2. Aufl. 2011, S. 3 ff. (a. a. O., S. 24, die oben zitierte Formulierung). Vgl. weiter noch *P. Lundgreen*, Standardization – Testing – Regulation, 1986; E. V. Heyen (Hrsg.), Technikentwicklung zwischen Wirtschaft und Verwaltung in Großbritannien und Deutschland, 2008.

[44] *M. Dommann*, Rechtsinstrumente, Schweizerische Zeitschrift für Geschichte 55 (2005), S. 17 (19).

[45] So der Befund bei *Vec*, Kurze Geschichte des Technikrechts, in: Schulte/Schröder (Hrsg.), Handbuch des Technikrechts, 2. Aufl. 2011, S. 3 (4 f.) m. w. N. (mit dem Hinweis, dass der Begriff des „Technikrechts" erst ab den 1970er-Jahren gebräuchlich wurde); eine frühere Datierung bei *Kloepfer/Franzius/Weber*, Technik und Recht im wechselseitigen Werden, 2002, S. 13.

[46] *J. Yates/C. Murphy*, Engineering Rules, 2019.

[47] Zu den stattdessen genutzten Instrumenten staatlicher Technologie- und Wirtschaftsförderung *L. Pahlow*, Industrialisierung als Staatsaufgabe, Rechtsgeschichte 15 (2009), S. 109 (121 ff.); *P. Collin*, Staatliche Kapitalhilfe für Unternehmen, Rechtsgeschichte 15 (2009), S. 126 (138 ff.); zusammenfassend *J. Radkau*, Technik in Deutschland, 2. Aufl. 2008, S. 113 ff.; *Boehme-Neßler*, BilderRecht, 2010, S. 3; *Vec*, Kurze Geschichte des Technikrechts, in: Schulte/Schröder (Hrsg.), Handbuch des Technikrechts, 2. Aufl. 2011, S. 3 (23).

Freiheit und Eigentum fokussierte Gesetzesbegriff des Konstitutionalismus führte zu einer bis heute bestehenden Unwucht, wonach Recht und Gesetz in erster Linie als Schranke für die Technikgestaltung und -nutzung wahrgenommen werden. Die (auch) innovationsermöglichende Funktion des Rechts rückte erst viel später in den Fokus.

Trotz alldem war in der rechtswissenschaftlichen Literatur von der Technik kaum die Rede. Auch die Tatsache, dass das staatliche Handeln selbst immer umfassender auf technische Artefakte angewiesen war, blieb ausgeblendet oder wurde allenfalls metaphorisch aufgenommen, etwa wenn *Max Weber* in der Tradition der Theoretiker des absolutistischen Fürstenstaates vom Staat und seinem Rechtsstab als „technisch rationale[r] Maschine" sprach.[48] Hierbei hatte es auch in der Folgezeit sein Bewenden.[49]

Erst nach 1945 ließ sich die Frage nach der Technik in der Rechtswissenschaft nicht länger ignorieren. Statt die Gegebenheiten nüchtern zu analysieren und das bereits eingespielte Wechselverhältnis von Recht und Technik zur Kenntnis zu nehmen, rezipierte man die Großtheorien *Freyers*, *Heideggers* und anderer. So charakterisierten *Hans Huber* und andere den „Einbruch der Technik in das Recht" als Abbruch einer langen Tradition und sahen die „dem Rechte innewohnenden Maßstäbe entkräftet".[50] *Ernst Forsthoff* deutete den Befund staatsrechtlich und beschrieb die Technik als strukturell antiliberale

[48] *Weber*, Wirtschaft und Gesellschaft, 5. Aufl. 1980, S. 469. Ebenso *ders.*, Parlament und Regierung im neugeordneten Deutschland, in: Gesammelte politische Schriften, 5. Aufl. 1988, S. 306 (322). Zur Geschichte der Metapher, die im Absolutismus zunächst als politische Strategie zur Einhegung der Fürstengewalt genutzt wurde, *B. Stollberg-Rilinger*, Staat als Maschine, 1986, S. 23 ff.

[49] Die rechtswissenschaftliche Literatur des Nationalsozialismus verwendet die Maschinenmetapher uneinheitlich. So kritisiert *E. Forsthoff*, Der totale Staat, 1. Aufl. 1933, S. 11, den liberalen Rechtsstaat als „bürokratische[n] Apparaturstaat". Demgegenüber den nationalsozialistischen Staat als „Apparat" der Bewegung beschreibend *R. Höhn*, Die Wandlung im staatsrechtlichen Denken, 1934, S. 36. Wieder anders dann etwa *H. Frank*, Technik des Staates, 1942, S. 27. Zur Technik-Affinität des Nationalsozialismus, die sich jedoch nicht in einer intensiveren Befassung der Rechtswissenschaft mit den Realitäten der Technik niederschlug, siehe nur *M. Stolleis*, Geschichte des öffentlichen Rechts in Deutschland, Bd. 3, 1999, S. 355 m. w. N.; *J. Herf*, Der nationalsozialistische Technikdiskurs, in: Emmerich/Wege (Hrsg.), Der Technikdiskurs in der Hitler-Stalin-Ära, 1995, S. 72 ff.

[50] *H. Huber*, Das Recht im technischen Zeitalter, 1960, S. 9 f. Ähnlich auch *K. Oftinger*, Punktationen für eine Konfrontation der Technik mit dem Recht, in: FS Zürich, 1961, S. 1 ff.; *ders.*, Konfrontation der Technik mit dem Recht, in: Freyer/Papalekas/Weippert (Hrsg.), Technik im technischen Zeitalter, 1965, S. 248 (262): „Wir stehen vor einer *partiellen Überwältigung des Rechts durch die Technik*. Die vom Recht geschützten Werte werden technischen Zwecken und Idealen geopfert. Maßstäbe des Technikers ersetzen die Maßstäbe des Juristen. *Juristisches Denken weicht technischem Denken*." Ein Überblick über die zeitgenössische Debatte bei *R. Herzog*, Der Mensch des technischen Zeitalters, in: Kunst (Hrsg.), Evangelisches Staatslexikon, 1966, S. XXI ff.

und antidemokratische Macht,[51] die zur Verdrängung des Juristen durch den Fachmann führe.[52] Geboten sei daher in der Tradition der Staatslehre des 19. Jahrhunderts die „Nichtidentifikation" des Staates mit der Technik, weil die Technik für den Staat „etwas Fremdes ist und bleiben muß".[53] Angesichts der „geschichtsmächtigen Potenz" der Technik (*Forsthoff*),[54] müsse dies jedoch ein nostalgischer Traum bleiben.[55] Die „Entfremdung" des Rechts schien unausweichlich.[56]

Ungeachtet dessen wuchsen unter dem Grundgesetz die gesetzlichen und untergesetzlichen Vorgaben für die Technik weiter an und dehnten sich bald auf die supra- und internationale Ebene aus. In der Rechtswissenschaft wirkte demgegenüber noch lange Forsthoffs These nach, wonach „die Technik Formen und Verfahren der Selbsterledigung impliziert, die sich in die Methodik des überkommenen und geltenden Verwaltungsrechts nicht einfügen lassen und für deren rechtliche Bewältigung eine rechtsstaatliche Formel nicht, jedenfalls noch nicht, gefunden werden kann."[57] Eine produktive Auseinander-

[51] So immer wieder *Forsthoff*, Technisch bedingte Strukturwandlungen des modernen Staates, in: Freyer/Papalekas/Weippert (Hrsg.), Technik im technischen Zeitalter, 1965, S. 211 (222); *ders.*, Technischer Prozess und politische Ordnung, Studium Generale 22 (1969), S. 849 ff.; *ders.*, Von der sozialen zur technischen Realisation, Der Staat 9 (1970), S. 145 ff.; *ders.*, Der Staat der Industriegesellschaft, 1971, S. 42 ff., 84, 105, 158 ff. Zu Forsthoffs im zeithistorischen Kontext wenig origineller, für die Rechtswissenschaft aber dennoch prägender Technikkritik kritisch-einordnend *V. Neumann*, Der harte Weg zum sanften Ziel, in: Roßnagel (Hrsg.), Recht und Technik, 1984, S. 88 ff.; *I. Staff*, Die Wahrung staatlicher Ordnung, Leviathan 15 (1987), S. 141 ff.

[52] Zur „Mythologie des Juristen" bei Forsthoff – vgl. *E. Forsthoff*, Der lästige Jurist, DÖV 1955, S. 648 ff.; *ders.*, Der Jurist in der industriellen Gesellschaft, NJW 1960, S. 1273 ff. – ausführlich *Meinel*, Der Jurist in der industriellen Gesellschaft, 2011, S. 470 ff. Forsthoff nimmt hier eine Diskussion auf, die von technischer Seite als Juristenkritik bereits in den 1880er-Jahren geführt worden ist, damals jedoch ohne größere Resonanz auf juristischer Seite blieb. Dazu näher *Vec*, Kurze Geschichte des Technikrechts, in: Schulte/Schröder (Hrsg.), Handbuch des Technikrechts, 2. Aufl. 2011, S. 3 (56 f.). Zur Rolle der bereits in preußischer Zeit bestehenden technischen Verwaltungsbeamten (insbesondere Bau- und Bergbeamten) vgl. *Lundgreen*, Standardization – Testing – Regulation, 1986, S. 8 ff., sowie zeitgenössisch *L. v. Rönne*, Das Staatsrecht der preußischen Monarchie, Bd. 2, 1863, S. 89 ff.

[53] *Forsthoff*, Technisch bedingte Strukturwandlungen des modernen Staates, in: Freyer/Papalekas/Weippert (Hrsg.), Technik im technischen Zeitalter, 1965, S. 211 (212).

[54] *Forsthoff*, Technische Realisation und politische Ordnung, in: Schatz (Hrsg.), Auf dem Weg zur hörigen Gesellschaft?, 1973, S. 183 (198).

[55] Auch bei *E. Forsthoff*, Lehrbuch des Verwaltungsrechts, Bd. 1, 1. Aufl. 1950, § 1 Ziff. 1 (S. 3) (= 10. Aufl. 1973 S. 4), findet sich die These, dass Technik in der Gegenwart die soziale Wirklichkeit forme.

[56] *E. Forsthoff*, Rechtsstaat im Wandel, 1964, S. 116. Zum Entfremdungs-Begriff bei Forsthoff siehe *Meinel*, Der Jurist in der industriellen Gesellschaft, 2011, S. 466 ff.

[57] *Forsthoff*, Verwaltungsrecht, 10. Aufl. 1973, § 4 Ziff. 3 (S. 74).

setzung der mit der Technisierung verbundenen Herausforderungen für Recht und Verfassung ließ daher auf sich warten.[58]

2. … über die Anerkennung der staatlichen Verantwortung für die Risiken der Technik …

Ein auf praktische Wirksamkeit im Hier und Jetzt zielendes Recht – also das Recht des demokratischen Verfassungsstaates[59] – konnte der Frage nach der Technik jedoch nicht auf Dauer nur mit derart abstrakten Gedanken begegnen. Dabei war auch dem Grundgesetz die Technik als Thema von Haus aus fremd. Der Parlamentarische Rat hatte ihr keine nähere Beachtung geschenkt und im Text des Grundgesetzes hatten technische Zusammenhänge keinen großen Niederschlag gefunden.[60] Zwar speicherten verschiedene Grundrechte Einsichten, die sich für die Bewältigung der mit einer Technisierung der Staatsgewalt verbundenen Freiheitsgefährdungen als relevant erwiesen oder die jedenfalls für entsprechende Fortschreibungen des Verfassungsrechts offen waren. Einzelne Technologien wie die „Berichterstattung durch Rundfunk und Film" (Art. 5 Abs. 1 S. 2 GG) genossen sogar eine spezielle Schutzstellung. Dennoch enthielt das Grundgesetz kein Konzept, dem sich übergreifende Vorgaben für das Verhältnis der Verfassung zur Technik hätten entnehmen lassen. Geschützt von den grundrechtlichen Freiheitsgarantien ermög-

[58] Im *Verwaltungs*recht hatte die Technik*kritik* der Nachkriegszeit demgegenüber bereits früher einen Nachhall gefunden, die auch auf konkrete Fragestellungen einging, vgl. insbes. *K. Zeidler*, Technisierung der Verwaltung, 1959; *H. P. Bull*, Verwaltung durch Maschinen, 1963; *S. Simitis*, Automation in der Rechtsordnung, 1967; siehe auch *Forsthoff*, Rechtsstaat im Wandel, 1964, S. 128, zu „Elektronenhirnen", die den Verwaltungsbeamten ersetzen würden. Hier wurde die Grundlage für jene Sonderstellung gelegt, die die Informationstechnik bald im verfassungsrechtlichen Koordinatensystem einnehmen sollte. Dazu gleich unter § 3 III. Die Technikignoranz war im Übrigen kein rein deutsches Phänomen. Auch in den USA blieb ein Werk wie das von *L. Tribe*, Channeling Technology Through Law, 1973, lange Zeit isoliert.

[59] Für das Verfassungsdenken der Nachkriegszeit prägend *K. Hesse*, Die normative Kraft der Verfassung, 1959, S. 15.

[60] *Murswiek*, Die staatliche Verantwortung für die Risiken der Technik, 1985, S. 22, spricht von „konstitutioneller Ignoranz". Das gilt in dieser Schärfe jedoch nur für das GG in der Fassung von 1949. Grundgesetzliche Normen, die heute explizit Aussagen zur Technik enthalten, sind neben dem oben erwähnten Art. 5 Abs. 1 S. 2 GG (Rundfunk und Film) noch Art. 13 Abs. 3–6 GG (Überwachungstechnologien) und Art. 26 Abs. 2 GG (Kriegswaffen). Bezieht man die Kompetenzbestimmungen mit ein, verbreitert sich das Spektrum: Art. 73 Abs. 1 Nr. 6 GG (Luftverkehr), Art. 73 Abs. 1 Nr. 6a GG (Eisenbahnen und Schienenwege), Art. 73 Abs. 1 Nr. 7 GG (Telekommunikation), Art. 73 Abs. 1 Nr. 12 GG (Waffen und Sprengstoffe), Art. 73 Abs. 1 Nr. 14 GG (Kernenergie), Art. 74 Abs. 1 Nr. 11 GG (Bergbau, Industrie etc.), Art. 74 Abs. 1 Nr. 26 GG (Gentechnik etc.), Art. 87d GG (Luftverkehr), Art. 87e GG (Eisenbahnen), Art. 87f GG (Telekommunikation) und Art. 91c GG (informationstechnische Systeme).

lichte dies der Technik zunächst, in Staat und Gesellschaft weiter Raum zu gewinnen.

Dies änderte sich ab den 1970er-Jahren. Seither wurde die Technik zum Gegenstand gründlicher (verfassungs-)rechtlicher Analysen. Inwieweit diese Entwicklung durch die kritischen Arbeiten Forsthoffs und anderer intellektuell vorbereitet war, kann kaum geklärt werden. Allerdings stellte sich die *verfassungs*rechtliche Antwort auf die Herausforderungen der Technik deutlich differenzierter als jene Kulturkritik dar.

Auslöser des verstärkten Interesses war die Debatte zur Nutzung der Kernenergie. Hier wurde erstmals intensiv erörtert, welche Grenzen der privaten Technikgestaltung und dem privaten Technikgebrauch gezogen werden müssten; geklärt wurde auch, dass die staatliche Verantwortung für die Technik nicht dort endet, wo Private handeln, und dass die (Neben-)Folgen des Technikgebrauchs in die Entscheidung über mögliche Grenzen nicht ignoriert werden dürfen.[61] Der Gesetzgeber konnte daher bei der Entscheidung über das Ob und Wie der Regulierung der Technik nicht mehr nur Opportunitätserwägungen folgen, sondern musste den betroffenen grundrechtlichen Interessen Dritter Rechnung tragen.

Indem sich das Verfassungsrecht so als Maßstab für die Beurteilung der Technik gesetzt hatte, stellte sich zwangsläufig die Frage nach der Implementierung der grundrechtlichen Wertungen. Von Verfassungs wegen musste die Rechtswissenschaft also Interesse für die mit der Technik verbundenen Sozialstrukturen entwickeln, galt es doch die einzelnen technischen Systeme in ihrem „jeweiligen Sach- oder Verwendungszusammenhang" und je im Lichte der bestehenden und durch ihren Einsatz gefährdeten Verfassungsrechtsgüter zu beurteilen.[62]

---

[61] Umfassend *Murswiek*, Die staatliche Verantwortung für die Risiken der Technik, 1985. Vgl. zum frühen Diskussionsstand ferner nur *R. Grawert*, Technischer Fortschritt in staatlicher Verantwortung, in: Listl/Schambeck (Hrsg.), FS Broermann, 1982, S. 457 ff.; *A. Roßnagel*, Bedroht die Kernenergie unsere Freiheit?, 2. Aufl. 1983; *ders.*, Radioaktiver Zerfall der Grundrechte?, 1984; *P. Kirchhof*, Kontrolle der Technik, NVwZ 1988, S. 97 ff.; *J. Ipsen*, Die Bewältigung der wissenschaftlichen und technischen Entwicklungen durch das Verwaltungsrecht, in: VVDStRL 48 (1990), S. 187 ff.; *D. Murswiek*, Die Bewältigung der wissenschaftlichen und technischen Entwicklungen durch das Verwaltungsrecht, in: VVDStRL 48 (1990), S. 207 ff.; *Schlink*, Die Bewältigung der wissenschaftlichen und technischen Entwicklungen durch das Verwaltungsrecht, in: VVDStRL 48 (1990), S. 235 ff.; *R. Wahl*, Forschungs- und Anwendungskontrolle, UTR 14 (1991), S. 7 ff.; *U. K. Preuß*, Risikovorsorge, in: Grimm (Hrsg.), Staatsaufgaben, 1994, S. 523 ff.; *F. Ossenbühl*, Die Not des Gesetzgebers im naturwissenschaftlich-technischen Zeitalter, 2000; *P. Tettinger*, Verfassungsrecht und Techniksteuerung, in: Vieweg (Hrsg.), Technikssteuerung und Recht, 2000, S. 287 ff. Das Themenspektrum erweiternd: *A. Roßnagel/P. Wedde et al.*, Digitalisierung der Grundrechte?, 1990.

[62] So die Formulierung bei *H. Schulze-Fielitz*, Technik und Umweltrecht, in: Schulte/Schröder (Hrsg.), Handbuch des Technikrechts, 2011, S. 455 (457), unter Verweis auf *Tettinger*, Verfassungsrecht und Technikssteuerung, in: Vieweg (Hrsg.), Technikssteuerung und Recht, 2000, S. 287 (288 ff.).

3. … zur Technikregulierung als Strukturierung des Kommunikationsprozesses zwischen Recht und Technik

Dennoch dauerte es, bis die Frage nach der Technik über Spezialistenkreise hinaus Beachtung fand.[63] Ließ sich Anfang der 1990er-Jahre noch eine „Technikignoranz der Juristen" diagnostizieren,[64] kann davon heute allerdings keine Rede mehr sein. Technik ist mittlerweile ein bestimmendes Thema des Rechts und der Rechtswissenschaft. Gerade „neue" technische Innovation wie die Nanotechnologie oder das maschinelle Lernen werden zeitnah und breit aufgegriffen. Auch das Verfassungsrecht reagiert darauf.[65] Hinzu kommt eine intensive Befassung mit technikrelevanten Querschnittsthemen wie „Risiko" oder „Innovation" sowie eine nicht kleine Zahl von Gesamtbetrachtungen zum Verhältnis von Recht und Technik.[66] Anerkannt ist, dass sich die Rolle des Rechts im Verhältnis zur Technik nicht auf Einhegung und Kontrolle beschränkt, sondern auch die Technik- bzw. Innovationsermöglichung umfasst.[67] Das ist gerade mit Blick auf Informationssicherheit ein wesentlicher

[63] Aus dem frühen Schrifttum, das sich v. a. auf die Rezeption technischer Regeln („Stand der Technik") konzentrierte, siehe nur *H. Krüger*, Rechtsetzung und technische Entwicklung, NJW 1966, S. 617 ff.; *H. Plischka*, Technisches Sicherheitsrecht, 1969, S. 32 ff., 80 ff.; *R. Breuer*, Direkte und indirekte Rezeption technischer Regeln durch die Rechtsordnung, AöR 101 (1976), S. 46 ff.; *Marburger*, Die Regeln der Technik im Recht, 1979; *R. Wolf*, Der Stand der Technik, 1986; *U. Battis/C. Gusy*, Technische Normen im Baurecht, 1988. Vgl. auch zur frühen Reaktion des Rechts auf die Computertechnik unter § 3 III. Zur Problematik vertiefend unten § 5 III. 2. b).

[64] *M. Mai*, Technikblindheit des Rechts – Technikignoranz der Juristen?, Zeitschrift für Rechtssoziologie 13 (1992), S. 257 ff. Ein Indiz für die Zugehörigkeit zu der seinerzeit noch kleinen Gruppe von Fachvertretern, die als Experten für das Verhältnis von Recht und Technik galten, kann die Teilnahme am Kolloquium der TFA-Enquete-Kommission des Bundestages zu den „Rechtlichen Aspekten der Technikfolgen-Abschätzung" dienen, in dem *Hans Peter Bull*, *Rudolf Lukes*, *Spiros Simitis*, *Peter Marburger*, *Alexander Roßnagel* und *Michael Kloepfer* gehört wurden (Materialien zur Drs. 10/6801, Bd. II, 1987).

[65] Zur Semantik des „Neuen" in diesem Zusammenhang und den damit verbundenen Schwierigkeiten ausführlich *T. Wihl*, Die Entwicklung „neuer" Grundrechte, in: Grimm (Hrsg.), Vorbereiter – Nachbereiter?, 2019, S. 307 ff. Allgemein zur Hebung und Aktualisierung (grund-)rechtlicher Innovationsressourcen *G. Hornung*, Grundrechtsinnovationen, 2015, S. 414 ff. und passim; speziell zur Digitalisierung *Peuker*, Verfassungswandel durch Digitalisierung, 2020.

[66] Zum Risikobegriff vgl. die Nachweise unten § 4 Fn. 22. Zum Stand der rechtswissenschaftlichen Innovationsforschung gleich in § 3 Fn. 67. Neben den in den folgenden Fußnoten zitierten Beiträgen siehe auch grundlegend *Roßnagel*, Technikfolgenforschung, 1993; *Kloepfer/Franzius/Weber*, Technik und Recht im wechselseitigen Werden, 2002. Aus der internationalen Literatur vgl. insbesondere die Beiträge in R. Brownsword/K. Yeung (Hrsg.), Regulating Technologies, 2008; M. Goodwin/B.-J. Koops/R. Leenes (Hrsg.), Dimensions of Technology Regulation, 2010; R. Brownsword/E. Scotford/K. Yeung (Hrsg.), The Oxford Handbook of Law, Regulation, and Technology, 2017.

[67] Siehe *W. Hoffmann-Riem*, Innovationen durch Recht und im Recht, in: Schulte (Hrsg.), Technische Innovation und Recht, 1997, S. 3 ff.; *M. Kloepfer*, Recht ermöglicht Technik, NuR 1997, S. 417 ff.; W. Hoffmann-Riem/J.-P. Schneider (Hrsg.), Rechtswissenschaftliche

Aspekt. Denn das Verbot „unsicherer" Informationstechnik allein würde wohl kaum zur notwendigen Ertüchtigung jener Institutionen und Verfahren, die zur Sicherheit der Informationstechnik beitragen, führen.

Gegenstand dieser Literatur ist ein immer dichteres Geflecht von Rechtsnormen unterschiedlicher Provenienz und Ranges, die auf eine gesellschaftsverträgliche Gestaltung der Technik hinzuwirken suchen. Unabhängig von der Frage, ob es sich dabei nun um ein eigenständiges „Rechtsgebiet" handelt oder um eine Querschnittsmaterie, die sachgebietsübergreifend – vom Immissionsschutz-, Chemikalien- und Gentechnikrecht über das Produkt-, Geräte- und Anlagensicherheitsrecht bis hin zum Datenschutz[68] – typische mit dem Einsatz technischer Systeme verbundene Problemlagen adressiert,[69] ist zu konstatieren, dass sich hier ein Kanon von schematisierten Strategien etabliert hat, mit dessen Hilfe der Staat seiner Verantwortung für die Technik nachzukommen versucht.[70] Über die gemeinsame Problemstellung und die analogen „Regelungsstrukturen" lässt sich die Materie in der Summe als „Technikrecht" begreifen.[71]

Innovationsforschung, 1998; *M. Schulte*, Techniksteuerung durch Technikrecht – rechtsrealistisch betrachtet, in: Vieweg (Hrsg.), Technikssteuerung und Recht, 2000, S. 23 ff.; *R. Pitschas*, Technikentwicklung und -implementierung als rechtliches Steuerungsproblem, in: Kloepfer (Hrsg.), Technikentwicklung und Technikrechtsentwicklung, 2000, S. 73 ff.; *C. Franzius*, Technikermöglichungsrecht, DV 34 (2001), S. 487 ff.; *M. Schmidt-Preuß*, Technikermöglichung durch Recht, in: Kloepfer (Hrsg.), Kommunikation – Technik – Recht, 2002, S. 175 ff.; *W. Hoffmann-Riem*, Innovationsoffenheit und Innovationsverantwortung durch Recht, AöR 131 (2006), S. 255 ff.; *H.-H. Trute*, Wirtschaft und Technik, in: Isensee/Kirchhof (Hrsg.), HStR, Bd. IV, 2006, § 88 Rn. 18 ff.; *M. Eifert*, Innovationsfördernde Regulierung, in: ders./Hoffmann-Riem (Hrsg.), Innovationsfördernde Regulierung, 2008, S. 9 ff.; *A. Scherzberg*, Innovationen und Recht, in: W. Hoffmann-Riem, Offene Rechtswissenschaft, 2010, S. 273 ff.; *Spiecker gen. Döhmann*, Rechtliche Begleitung der Technikentwicklung, in: Hill/Schliesky (Hrsg.), Die Vermessung des virtuellen Raums, 2012, S. 137 ff.; *W. Hoffmann-Riem*, Innovation und Recht – Recht und Innovation, 2016, S. 389 ff.

[68] Vgl. die Beiträge in M. Schulte/R. Schröder (Hrsg.), Handbuch des Technikrechts, 2. Aufl. 2011.

[69] Zur begrenzt ertragreichen Diskussion, ob das Technikrecht ein „Rechtsgebiet" bildet, *U. Di Fabio*, Technikrecht, in: Vieweg (Hrsg.), Technikssteuerung und Recht, 2000, S. 9; *Vec*, Kurze Geschichte des Technikrechts, in: Schulte/Schröder (Hrsg.), Handbuch des Technikrechts, 2. Aufl. 2011, S. 3 (4 f.) m. w. N. Zur parallelen Frage, ob das Sicherheitsrecht bzw. sogar das Informationssicherheitsrecht jeweils „Rechtsgebiete" sind, vgl. unten § 4 Fn. 4 und § 6 Fn. 18.

[70] Zu den Instrumenten des Technikrechts im Überblick *M. Kloepfer*, Instrumente des Technikrechts, in: Schulte/Schröder (Hrsg.), Handbuch des Technikrechts, 2. Aufl. 2011, S. 151 ff.; aus unionsrechtlicher Sicht *A. Röthel*, Europarechtliche Vorgaben für das Technikrecht, in: a. a. O., S. 201 (214 ff.). Ein wichtiger institutionalisierter Mechanismus, der breit erforscht ist, ist die Technikfolgenabschätzung. Siehe dazu die Beiträge in *G. Aichholzer/A. Bora et al.*, Technology Governance, 2010; M. Decker/A. Grunwald/M. Knapp (Hrsg.), Der Systemblick auf Innovation, 2012; *G. Simonis*, Konzepte und Verfahren der Technikfolgenabschätzung, 2013.

[71] Zum Begriff der „Regelungsstruktur": *H.-H. Trute/W. Denkhaus/D. Kühlers*, Governance in der Verwaltungsrechtswissenschaft, DV 37 (2004), S. 451 (468).

Diese Regeln, deren informationssicherheitsrechtliche Ausprägung hier noch detailliert aufzuschlüsseln sein wird,[72] beruhen auf einem Verständnis des Verhältnisses von Recht und Technik, das nicht unpassend mit der Formel von „Technik und Recht im wechselseitigen Werden" bezeichnet worden ist.[73] Präziser lässt sich unter Rückgriff auf den obigen Befund, dass „die Technik" nicht als Reich der Objekte oder als Summe der Artefakte verstanden werden darf, sondern auch bzw. sogar in erster Linie ein soziales System und ein Netzwerk von Akteuren darstellt, zu denen sich das Recht in eine kommunikative Beziehung setzen kann, die rechtliche Regulierung der Technik als Strukturierung eines komplexen Kommunikationsprozesses verstehen. Die Technik als soziales System ist gegenüber derartigen kommunikativen Interventionen grundsätzlich offen. Simplistische Formeln à la „code is law" verkennen die hier wirkenden wechselseitigen Mechanismen grundlegend.[74] In wenigen Fällen wird die Kommunikation allerdings direkt und linear erfolgen, etwa indem das Recht ganz konkrete Vorgaben zur Gestaltung eines technischen Artefakts macht oder gar die Herstellung oder den Gebrauch bestimmter Systeme (etwa bestimmter Waffenarten) untersagt. Üblicherweise wird eine indirekte und reziproke Kommunikationsarchitektur etabliert, in der das Recht Einfluss auf die Bedingungen der Technikgestaltung nimmt, aber auch den Eigensinn der Technik anerkennt und auf das Recht zurückwirken lässt, etwa in Form einer Privilegierung bestimmter Zertifizierungssysteme oder durch die Verpflichtung auf ein spezifisch rechtsgutsschützendes technisches „Design".[75]

Wenn also von der rechtlichen Regulierung der Technik die Rede ist, dann schwingen alle diese Assoziationen mit. Hieran wird in terminologischer und konzeptioneller Hinsicht anzuschließen sein, wenn es darum gehen wird, die rechtliche Regulierung der Informationssicherheit zu bewerten. Auch dort besteht die Aufgabe rechtlicher Regulierung im Kern darin, durch Vorgaben zur Organisation und zum Verfahren einen kommunikativen Austausch mit der Technik aufzubauen und zu institutionalisieren. Flankiert werden muss

---

[72] Hierzu unten § 7.

[73] Prägend: *Kloepfer/Franzius/Weber*, Technik und Recht im wechselseitigen Werden, 2002. Ähnlich zuletzt – in Anlehnung an P. Weingart (Hrsg.), Technik als sozialer Prozeß, 1989 – *Haake*, Technik – Recht – Raum, 2022, S. 1 f. und passim (speziell zum Verhältnis von Völkerrecht und Technikentwicklung); sowie – in Anlehnung an die Ansätze Alexander Roßnagels – *S. Jandt*, Technikadäquate Grundrechtsentwicklung, 2022, S. 25 ff. und passim.

[74] Das Anliegen von *L. Lessig*, Code and other Laws of Cyberspace, 1999, war differenzierter und zielte in Richtung der Argumentation von *Langdon Winner* (dazu § 3 Fn. 32). Siehe dazu nur *J. Kesan/R. Shah*, Shaping Code, Harv. J. L. & Tech. 18 (2005), S. 319 ff.; *E. Dommering*, Regulating Technology: Code is not Law, in: Dommering/Asscher (Hrsg.), Coding Regulation, 2006, S. 1 ff.; *C. Raab/P. De Hert*, Tools for Technology Regulation, in: Brownsword/Yeung (Hrsg.), Regulating Technologies, 2008, S. 263 ff.

[75] Zu diesen Instrumenten näher unter § 6 II. 6.

dies von Maßnahmen, die zur Generierung hoheitlichen Regulierungswissens beitragen und Anreize zur Implementierung sicherer Informationstechnik setzen.

III. Exkurs: Der Sonderweg des Datenschutzrechts

Wie einleitend erwähnt, wurde das Problem Informationssicherheit besonders früh im Kontext des Datenschutzrechts erkannt.[76] Diese Rechtsmaterie hatte zwar durch ihren Gegenstand, die datenverarbeitende Informationstechnik, einen offensichtlichen Technikbezug. Ein eigentlich kommunikatives Verhältnis zur (Informations-)Technik hat das Datenschutzrecht jedoch erst spät gesucht. Für das Informationssicherheitsrecht dient das Datenschutzrecht somit gewissermaßen als Warnung, die Technik nicht aus dem Blick zu verlieren. Im Folgenden sollen weder die Geschichte noch die Grundprinzipien des Datenschutzrechts umfassend rekonstruiert werden.[77] Stattdessen sind einzelne Momente der Genese des Datenschutzrechts zu beleuchten, die für das Verhältnis des Datenschutzrechts zur Technik charakteristisch sind.

Bekanntlich erzielte die Computertechnik ab den 1960er-Jahren erhebliche Raumgewinne und eröffnete der automatisierten Datenverarbeitung zuvor ungeahnte Anwendungsbereiche. Der rechtswissenschaftliche Diskurs reagierte bemerkenswert schnell auf diese Entwicklung. Verbreitet wurde angenommen, dass die neue Informationstechnik Staat und Gesellschaft grundlegend verändern würde.[78] Getragen war die Bewegung vom Widerstand gegen ein kybernetisch-technokratisches Denken; als solche fügte sie sich in die seinerzeit im progressiven wie im konservativen Milieu herrschende technikkri-

[76] Siehe oben § 2 I. 2.

[77] Zur intensiv erforschten Genese des Datenschutzrechts siehe nur (aus deutscher Sicht) *H. P. Bull*, Informationelle Selbstbestimmung – Vision oder Illusion?, 2. Aufl. 2011, S. 22 ff.; *Wihl*, Die Entwicklung „neuer" Grundrechte, in: Grimm (Hrsg.), Vorbereiter – Nachbereiter?, 2019, S. 307 ff.; *J. Pohle*, Datenschutz und Technikgestaltung, 2018; *Simitis/Hornung/Spiecker gen. Döhmann*, in: dies. (Hrsg.), Datenschutzrecht, 2019, Einl. Rn. 1 ff. Zu Vorformen auch *K. von Lewinski*, Geschichte des Datenschutzrechts von 1600 bis 1977, in: Arndt/Betz et al. (Hrsg.), Freiheit – Sicherheit – Öffentlichkeit, 2009, S. 196 ff. *Kaiser*, Die Kommunikation der Verwaltung, 2009, S. 168, weist darauf hin, dass schon die datenschutzrechtliche Literatur *vor* dem Volkszählungsurteil unüberschaubar ist; die Nachweise im Folgenden beschränken sich daher auf einzelne prägende Beiträge.

[78] Repräsentativ *A. Miller*, Personal Privacy in the Computer Age, Mich. L. Rev. 67 (1969), S. 1089 (1093): „The assumption throughout is that the computer is not simply a sophisticated indexing machine, a miniaturized library, or an electronic abacus; it is the keystone of a new communications medium that eventually will have global dimensions." Auch in der oben § 3 Fn. 58 erwähnten frühen Literatur zur Verwaltungsautomatisierung finden sich entsprechende Motive. Schon summierend *E. Benda*, Privatsphäre und „Persönlichkeitsprofil", in: Leibholz/Faller et al. (Hrsg.), FS Geiger, 1974, S. 23 (25).

tische Grundstimmung ein.[79] Die heute oft mit dem Recht auf informationelle Selbstbestimmung assoziierten historischen Totalitarismuserfahrungen waren demgegenüber für die seinerzeitige Diskussion weit weniger bedeutsam.[80]

Dass sich die entsprechenden Pläne für den Ausbau staatlicher Datenbanken und Informationssysteme bald als überambitioniert erwiesen, tat der Dynamik der juristischen Debatte keinen Abbruch.[81] Vielmehr setzte sich die Vorstellung durch, dass vernetzte Computer – insbesondere solche in der Hand des seinerzeit als Innovationstreiber agierenden Staates – nicht einfach ein weiteres Mittel staatlichen Handelns, sondern eine neue und eigene Machttechnologie bildeten.[82] Die durch sie ermöglichte Intensivierung der Überwachungs- und Kontrollmöglichkeiten des Staates gegenüber der Gesellschaft verschärfe zum einen die Gefährdungslage für das anerkannte Rechtsgut Privatheit.[83] Zum anderen führten derartige zentrale Datensammlungen zu strukturellen Verschiebungen im Verhältnis von Staat und Bürger. Gegenüber einem technisch überlegenen Staat, dessen Praktiken für die Bürger zunehmend undurchschaubar würden, drohe ein vollständiger Kontrollverlust.[84] Hierauf müsse mit Gegenmaßnahmen reagiert werden.

---

[79] Hierzu oben § 3 I. 1. Vgl. weiter *Kaiser*, Die Kommunikation der Verwaltung, 2009, S. 168 ff.

[80] Instruktiv zu den sich im Recht auf informationelle Selbstbestimmung bündelnden rechtspolitischen Strömungen *Wihl*, Die Entwicklung „neuer" Grundrechte, in: Grimm (Hrsg.), Vorbereiter – Nachbereiter?, 2019, S. 307 (315).

[81] In den USA wurde die Diskussion durch die Planungen für ein – gescheitertes – „National Data Center" ausgelöst, die von Anhörungen im Repräsentantenhaus 1965 und 1966 zu den Themen „Special Inquiry on Invasion of Privacy" und „The Computer and the Invasion of Privacy" sowie zwischen 1965 und 1967 zu „Invasion of Privacy", „Right of Privacy Act of 1967" und „Computer Privacy" begleitet waren. Siehe dazu aus der zeitgenössischen Literatur *E. Dunn*, The Idea of a National Data Center and the Issue of Personal Privacy, The American Statistician 21 (1967), S. 21 ff.; *A. Miller*, The National Data Center and Personal Privacy, The Atlantic 220:5 (1967), S. 53 ff.; vgl. die für die deutsche Debatte einflussreiche Aufbereitung bei *R. Kamlah*, Right of Privacy, 1969. In der deutschen Diskussion sind es die im ersten EDV-Bericht erwähnten Zentraldateien (BT-Drs. V/3355, S. 6), allen voran das durch Gesetz vom 18.3.1971 (BGBl. I S. 243) errichtete Bundeszentralregister und das im Entwurf des Bundesmeldegesetzes von 1973 erwähnte integrierte Einwohnermeldesystem (BT-Drs. VI/2654) mit dem geplanten „Personenkennzeichen", an denen sich die Debatte entzündet. Dazu insbes. *A. Podlech*, Verfassungsrechtliche Probleme öffentlicher Informationssysteme, Datenverarbeitung im Recht 1 (1972), S. 149 ff.

[82] Einprägsam *M. Stone/M. Warner*, Politics, Privacy, and Computers, The Political Quarterly 40 (1969), S. 256 (260): „The computer has given bureaucracy the gift of omniscience, if not omnipotence, by putting into its hands the power to know. No fact unrecorded, nothing forgotten nor lost, nothing forgiven."

[83] Ausbuchstabiert wird dies in den Arbeiten von Alan Westin, vgl. insbes. *A. Westin*, Science, Privacy, and Freedom Part I, Colum. L. Rev. 66 (1966), S. 1003 ff.; *ders.*, Privacy and Freedom, 1967.

[84] Ausführlich dazu *Miller*, Personal Privacy in the Computer Age, Mich. L. Rev. 67 (1969), S. 1089 ff. Aus der deutschen Debatte zur besonderen Gefährdung der elektronischen Informationsverarbeitung dann *W. Steinmüller/H. Wolter*, Besonderheiten elektronischer

Dabei geriet kurzzeitig auch die Technikgestaltung in den Blick. Vorgeschlagen wurde, zur Verhinderung des Missbrauchs entsprechende „Design"-Vorgaben zu entwickeln.[85] Und auch die allerersten gesetzlichen Regelungen zur Datenverarbeitung konzentrierten sich nach dem Vorbild des Technikrechts darauf, die technische Sicherheit der datenverarbeitenden Systeme zu gewährleisten.[86] Doch galt dies rasch als unzureichend. So formulierte *Ulrich Seidel* im Einklang mit den Reformern aus der Rechtswissenschaft: „Technische Sicherungen können […] nur die Frage beantworten, wie ein vermeintlich berechtigter Benutzer mit Gewißheit erkannt und die Ausübung seiner Rechte kontrolliert werden kann. Sie lassen das Problem offen, nach welchen Kriterien der Benutzer berechtigt sein soll, auf die gespeicherten Daten zuzugreifen."[87]

Damit war der Anschluss an die gleichfalls noch junge technikrechtliche Debatte gekappt. Verantwortlich für den Sonderweg des Datenschutzrechts dürfte zum einen sein, dass die Risiken der neuen Technik nicht von Privaten ausgingen, sondern dass der Staat selbst die Systeme entwickelt hatte und betrieb. Zum anderen war an den neuen Automaten weniger ihre Materialität beängstigend als die durch sie ermöglichte Rationalitätssteigerung des (Verwaltungs-)Verfahrens. Regulierungsbedürftig erschienen daher nicht die in zentralen Rechenzentren verborgen operierenden Maschinen, sondern die mit ihrer Hilfe ermöglichte hochrationalisierte Vorgangsbearbeitung. Der Zugriff auf die Technik war daher ab den 1970er-Jahren kein technik- sondern ein grundrechtlicher. In der Rechtsprechung des BVerfG zum allgemeinen Persönlichkeitsrecht fand sich hierfür zwar nur begrenzt Material.[88] Die vorhan-

---

Datenverarbeitung, in: Dammann/Karhausen et al. (Hrsg.), Datenbanken und Datenschutz, 1974, S. 51 ff. Klar unterschieden werden die beiden Stränge des datenschutzrechtlichen Diskurses – die individuelle Gefährdung von Privatheit und die kollektiven Verschiebungen im gesellschaftlichen Gefüge – bei *H. Fiedler*, Datenschutz und Gesellschaft, in: Siefkes (Hrsg.), Gesellschaft für Informatik – 4. Jahrestagung, 1975, S. 68 ff. Dass sich die Debatte zum Datenschutz natürlich nicht in diesen zwei Begründungssträngen erschöpft, sei hier dahingestellt; vgl. die umfangreiche Aufbereitung des Diskurses bei *D. Solove*, A Taxonomy of Privacy, U. Penn L. Rev. 154 (2006), S. 477 ff.; *S. Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014; *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 85 ff.

[85] Vgl. dazu frühzeitig *P. Baran*, Communications, computers and people, in: American Federation of Processing Societies (Hrsg.), Proceedings, 1965, S. 45 ff.; ausführlich dargestellt bei *Pohle*, Datenschutz und Technikgestaltung, 2018, S. 19. Auch bei *Westin*, Privacy and Freedom, 1967, finden sich bereits Überlegungen zur technischen Seite des Datenschutzes.

[86] Vgl. § 2 des Hessischen Datenschutzgesetzes vom 7.10.1970, GVBl. S. 625.

[87] *U. Seidel*, Persönlichkeitsrechtliche Probleme der elektronischen Speicherung privater Daten, NJW 1970, S. 1581 (1583).

[88] In dem in der frühen datenschutzrechtlichen Debatte immer wieder herangezogenen sog. Mikrozensus-Beschluss des BVerfG (E 27, 1) hatten die technischen Modalitäten der staatlichen Datenerhebung schon deswegen keine Rolle gespielt, weil diese ausweislich § 4 Abs. 1 des streitgegenständlichen Gesetzes über die Durchführung einer Repräsentativsta-

denen Bruchstücke[89] nutzte die Literatur jedoch effektiv für eine verfassungsrechtliche Fundierung ihrer Kritik an der staatlichen Datenverarbeitungstechnik.[90] Durchschlagskraft entwickelte vor allem das von *Steinmüller et al.* gefertigte Datenschutz-Gutachten, das vorschlug, den staatlichen Technikeinsatz überall dort, wo personenbezogene Daten[91] verarbeitet werden, am Maßstab der „freien Entfaltung der Persönlichkeit", also Art. 2 Abs. 1 GG, zu messen.[92] Die damit verbundenen Weichenstellungen – einerseits die aus der Orientierung an Art. 2 Abs. 1 GG resultierende ausschließliche Fokussierung auf die Verarbeitung *personenbezogener* Daten, andererseits die Hintansetzung der spezielleren Grundrechte zugunsten eines Zugriffs über Art. 2 Abs. 1 GG, der alle Konstellationen staatlichen Handelns gleichermaßen erfasste und auf den Nachweis einer konkreteren Gefährdung spezieller Freiheitsgarantien verzichtete[93] – prägten die anschließende Diskussion.[94]

Die Technik und ihre Entwicklung waren ab dann nur noch Auslöser und Rechtfertigungsgrund, nicht aber Gegenstand der Regulierung. So auch im Volkszählungsurteil. In dieser Entscheidung weist das Gericht gleich zu Beginn auf die Bedeutung der technischen Entwicklung für die Genese des „neuen" Grundrechts hin und begründet die Notwendigkeit der Gewährung eines eigenständigen Schutzanspruchs mit den „Bedingungen der modernen

tistik der Bevölkerung und des Erwerbslebens (Mikrozensus) vom 16.3.1957 (BGBl. I S. 213) i.d.F. v. 5.12.1960 (BGBl. I S. 873) noch durch persönliche oder schriftliche Befragung durchgeführt wurde und eine automatisierte Verarbeitung nicht stattfand. Auch dem sog. Scheidungsakten-Beschluss (BVerfGE 27, 344) liegt ein „analoger" Sachverhalt zu Grunde.

[89] Auch diese Bausteine stellen teilweise schon Reaktionen auf den technischen Wandel dar. So lässt sich etwa der prägende Beitrag von *S. Warren/L. Brandeis*, The Right to Privacy, Harv. L. Rev. 4 (1890), S. 193 ff., als Reaktion auf die Verbesserungen von Fotografie und Telegrafie lesen; zu Kontext und Wirkung dieses Beitrags vgl. nur *D. Solove*, Understanding Privacy, 2010, S. 15 ff.

[90] Vgl. beispielhaft *Seidel*, Persönlichkeitsrechtliche Probleme der elektronischen Speicherung privater Daten, NJW 1970, S. 1581 ff.; *R. Kamlah*, Datenüberwachung und Bundesverfassungsgericht, DÖV 1970, S. 361 ff.; *A. Podlech*, Verfassungsrechtliche Probleme öffentlicher Datenbanken, DÖV 1970, S. 473 ff.

[91] Während das Gutachten den Informationsbegriff verwendet, wird hier im Folgenden in Übereinstimmung mit dem heute etablierten Sprachgebrauch stets von personenbezogenen Daten gesprochen.

[92] *W. Steinmüller/B. Lutterbeck et al.*, Grundfragen des Datenschutzes, BT-Drs. VI/3826, Anlage 1, Juli 1971.

[93] Vgl. die kursorischen Ausführungen zu weiteren Grundrechten bei *Steinmüller/Lutterbeck/Mallmann/Harbort/Kolb/Jochen*, Grundfragen des Datenschutzes, BT-Drs. VI/3826, Anlage 1, Juli 1971, S. 60. Anders akzentuiert *H.-U. Gallwas*, Verfassungsrechtliche Grundlagen des Datenschutzes, Der Staat 18 (1979), S. 507 ff. Vgl. später auch *M. Albers*, Informationelle Selbstbestimmung, 2005, S. 357 ff. und passim; *Bull*, Informationelle Selbstbestimmung – Vision oder Illusion?, 2. Aufl. 2011, S. 57 ff.

[94] Siehe aus der seinerzeitigen Debatte insbesondere noch *A. Podlech*, Datenschutz im Bereich der öffentlichen Verwaltung, 1973; U. Dammann/M. Karhausen et al. (Hrsg.), Datenbanken und Datenschutz, 1974; *C. Mallmann*, Datenschutz in Verwaltungs-Informationssystemen, 1976.

Datenverarbeitung".[95] Der ausführlich referierte Vortrag der Beschwerdeführer skizziert die technischen Entwicklungen präzise:

„Seit der Mikrozensus-Entscheidung hätten sich die technischen Voraussetzungen der Datenerhebung und Datenverarbeitung grundlegend verändert. Die Statistischen Landesämter hätten sich zu Landesdatenzentralen entwickelt, zahlreiche Sonderverwaltungen hätten eigene Datenbanken mit eigenen Personenkennzeichen eingeführt; auf Gemeindeebene entwickelten sich die Melderegister zunehmend zu einer umfassenden Einwohnerdatenbank, deren Daten im Prinzip für jede staatliche Stelle abrufbar seien. Dies habe zur Folge, daß die Volkszählungsdaten auf den gleichen Rechnern mit denselben Programmen durch dieselben Personen verarbeitet würden, wie die Daten für andere staatliche Funktionen. Deshalb reichten die herkömmlichen Sicherungen für einen wirksamen Datenschutz nicht aus. Es sei möglich, einen riesigen Datenbestand für eine beliebige Vielzahl von abrufenden Stellen ständig verfügbar zu halten. Außerdem verfügten die unbestimmt vielen möglichen Empfänger der Volkszählungsdaten in der Regel über eigene Datenbanken. Diese lieferten Zusatzwissen, das mit den Volkszählungsdaten verknüpft werden könne. Dadurch werde die Schwelle der Reidentifikation weiter herabgesetzt. Aufgrund dieser gewandelten technologischen Bedingungen sei die Erstellung eines umfassenden und detaillierten Bildes der jeweiligen Person – ein Persönlichkeitsprofil – möglich, und zwar auch im Intimbereich".[96]

Diese Analyse der sozio-technischen Entwicklung macht sich der Senat bei der Bildung der Entscheidungsmaßstäbe zu eigen,[97] verdichtet sie dann zur Diagnose, dass es „unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses' Datum mehr" gibt.[98] Hierin liegt eine entscheidende Wendung: Wenn nunmehr alle (personenbezogenen) Daten von Belang sind, kommt es auf die technischen Systeme, die sie verarbeiten, dem Grunde nach gar nicht mehr an. Der Fokus verschiebt sich von der Regulierung der Technik auf den Schutz der Daten – er greift unabhängig von der Technik, mit deren Hilfe diese verarbeitet werden. Konsequenterweise unterstellte das Gericht in den auf das Volkszählungsurteil folgenden Entscheidungen daher auch nichtautomatisierte Datenverarbeitungsprozesse dem Schutz des neuen Grundrechts.[99] Zwar muss dieser Schritt, den der Datenschutzgesetzgeber nachvollzog, auch als pragmatische Übergangslösung verstanden werden, damit der grundrechtliche Schutz in einer lange Zeit nur partiell automatisierten Verwaltung nicht durch einen Medienbruch unterlaufen werden konnte – zumal nie ausgeschlossen werden kann, dass „analog" erhobene Informationen später

[95] BVerfGE 65, 1 (LS 1).
[96] BVerfGE 65, 1 (17).
[97] BVerfGE 65, 1 (42).
[98] BVerfGE 65, 1 (45).
[99] Besonders deutlich BVerfGE 78, 77 (84): „Die Möglichkeiten und Gefahren der automatischen Datenverarbeitung haben zwar die Notwendigkeit eines Schutzes persönlicher Daten deutlicher hervortreten lassen, sind aber nicht Grund und Ursache ihrer Schutzbedürftigkeit."

„digital" verarbeitet werden. Er trug zudem der Tatsache Rechnung, dass der informationelle Kontrollverlust, den es zu verhindern galt, nicht denknotwendig an das technische Medium Computer gebunden ist. Dennoch trat dadurch in den Hintergrund, dass die Entwicklungslogik des Datenschutzrechts von Beginn an auf die Automatisierung der staatlichen Datenverarbeitung ausgerichtet war, wie sie heute – von Randerscheinungen abgesehen[100] – Realität ist.

Vor diesem Hintergrund erstaunt es nicht, dass sich das Gericht im Volkszählungsurteil nicht darum bemüht hat, die Wechselbezüglichkeit des Verhältnisses von Recht und Technik herauszustellen oder auf die Entfaltung entsprechender Kommunikationsarenen zu dringen. Stattdessen wohnt den Gehalten des neuen Rechts, die als spezifischer Beitrag des Datenschutzrechts zum Recht der (Informations-)Technik zählen können, eine rein abwehrende Haltung gegenüber der Technik inne.[101] Die anschließende Entwicklung hielt sich weitgehend auf diesen Bahnen. Die vielfältige und vielstimmige Kritik an der Entscheidung wurde vom BVerfG punktuell verarbeitet, führte aber nicht zu einem Spurwechsel des Gerichts.[102]

Hier ist nicht der Ort für eine umfassende Rekonstruktion dieser Kritik an der Verfassungsjudikatur oder für Alternativentwürfe.[103] Stattdessen gilt es festzuhalten, dass das Volkszählungsurteil in Reaktion auf den technischen Wandel eine verfassungsrechtlich radizierte Regulierungs- und Rahmenverantwortung des Gesetzgebers für die Informationstechnik anerkannt hat. Die intensive Beobachtung der technischen Entwicklung, die Anlass für die Fortentwicklung der Grundrechtsdogmatik war, charakterisiert auch spätere Entscheidungen des Gerichts zur informationellen Selbstbestimmung.[104] Recht verstanden stellt das Recht auf informationelle Selbstbestimmung damit ein

[100] Aus dem nicht-öffentlichen Bereich: EuGH, C-25/17 v. 10.7.2018 – Zeugen Jehovas. Soweit heute noch in der Verwaltung rein analog gearbeitet wird, ist dies allerdings andernorts regelmäßig Anlass für Krisendiagnosen.

[101] Vgl. BVerfGE 65, 1 (LS 2 bis 4 und S. 41 ff.). Vgl. auch die Selbstauslegung des Gerichts durch *E. Benda*, Das Recht auf informationelle Selbstbestimmung, DuD 8 (1984), S. 86 ff. Dazu im Detail unten § 5 I. 2. c) aa).

[102] Für die relative Statik der Rechtsprechung dürfte auch verantwortlich sein, dass das Recht auf informationelle Selbstbestimmung keine alleinige Erfindung des Gerichts war, sondern sich auf jahrzehntelange Vorarbeiten der Rechtswissenschaft stützen konnte, in der fast alle später kritisierten Punkte bereits erwogen worden waren. Siehe insbes. *Wihl*, Die Entwicklung „neuer" Grundrechte, in: Grimm (Hrsg.), Vorbereiter – Nachbereiter?, 2019, S. 307 (310 ff.), sowie *Pohle*, Datenschutz und Technikgestaltung, 2018, S. 144 f. und passim.

[103] Instruktiv insbes. *G. Britz*, Informationelle Selbstbestimmung, in: Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, 2010, S. 561 ff.; *Albers*, Umgang mit personenbezogenen Informationen und Daten, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 3. Aufl. 2022, § 22 Rn. 56 ff. (in der 3. Aufl. gegenüber den Vorauflagen stark gekürzt). Vgl. auch unten § 5 I. 2. c) aa).

[104] Beispielhaft: BVerfGE 120, 378 (398); 133, 277 (316 ff., Rn. 93 ff.); 141, 220 (264 ff., Rn. 90 ff.); 150, 244 (263 ff., Rn. 35 ff.); 150, 309 (330 ff., Rn. 54 ff.); 155, 119 (166 ff., Rn. 90 ff.).

Automatisierungsfolgenbewältigungsrecht dar.[105] Die Entwicklung einer kommunikativen Beziehung zwischen Recht und Technik unterblieb jedoch und musste auf der Ebene des einfachen Rechts nachgeholt werden. Dort hat sie heute unter anderem im Gebot, für die Verarbeitung personenbezogener Daten geeignete technische und organisatorische Maßnahmen zu treffen (vgl. Art. 25 und 32 DSGVO), und in den dem Technikrecht entlehnten Regelungen zur Datenschutz-Folgenabschätzung (Art. 35 DSGVO) und zur Zertifizierung (Art. 42 f. DSGVO) ihren Sitz gefunden. Diese und weitere Maßnahmen werden im Recht der Informationssicherheit wiederbegegnen, das sich stärker als das Datenschutzrecht im Kern als Technikrecht begreifen muss.[106]

[105] Vgl. auch *T. Barczak* in: Dreier, GG, Bd. I, 4. Aufl., i. E., Art. 2 Abs. 1 Rn. 89. Hierauf stellt auch nochmals sehr deutlich BVerfGE 120, 378 (398) ab: „Eine weitere Besonderheit des Eingriffspotentials von Maßnahmen der elektronischen Datenverarbeitung liegt in der Menge der verarbeitbaren Daten, die auf konventionellem Wege gar nicht bewältigt werden könnte. Der mit solchen technischen Möglichkeiten einhergehenden gesteigerten Gefährdungslage entspricht der hierauf bezogene Grundrechtsschutz (vgl. BVerfGE 65, 1 [42]; 113, 29 [45 f.]; 115, 320 [342])." Im gleichen Sinne jüngst zur Gefährdung durch „nicht nachvollziehbare Algorithmen" BVerfGE 152, 152 (190, Rn. 85).

[106] Dazu ausführlich unten § 6 II.

§ 4 Informationssicherheitsrecht in der Sicherheitsgesellschaft

> „Der Risikogegenbegriff der Sicherheit bleibt […] ein Leerbegriff, ähnlich wie der Begriff der Gesundheit in der Unterscheidung von krank/gesund. Er fungiert also nur als Reflexionsbegriff. Oder auch als Ventilbegriff für soziale Forderungen, die je nach variablen Anspruchsniveaus in die Risikokalkulation durchschlagen. Im Ergebnis hat man mit dem Risiko/Sicherheit-Paar also ein Beobachtungsschema, das es im Prinzip ermöglicht, *alle* Entscheidungen unter dem Gesichtspunkt ihres Risikos zu kalkulieren."[1]

Ungeachtet der gerade vorgenommenen Verortung des Rechts der Informationssicherheit in den ruhigen Gewässern des Technikrechts ist der mit der Materie befasste Regulierungsdiskurs in der Praxis von harten Gegensätzen geprägt.[2] Als Informations*sicherheits*recht ist die Materie in den Strudel jener intensiven Auseinandersetzungen um den Sicherheitsbegriff gezogen worden, die spätestens seit dem 11. September 2001 in der Rechtswissenschaft das Nachdenken über Sicherheitsgewährleistung durch Recht prägen.[3] Die Bestrebungen der einen richten sich hier auf die Integration des zersplitterten Rechtsstoffs zu einem von einheitlichen Prinzipien beherrschten Sicherheitsrecht[4] und auf die Konsolidierung und Effektivierung der staatlichen „Sicher-

---

[1] *N. Luhmann*, Soziologie des Risikos, 2003, S. 29.

[2] Dazu bereits oben § 1 III.

[3] Zur „klassischen" Begriffsgeschichte grundlegend *W. Conze*, Sicherheit, Schutz, in: Brunner/Conze/Koselleck (Hrsg.), Geschichtliche Grundbegriffe, Bd. 5, 1984, S. 831 ff.; *M. Makropoulos*, Sicherheit, in: Ritter/Gründer/Gabriel (Hrsg.), Historisches Wörterbuch der Philosophie, Bd. 9, 1995, S. 745 ff.; zum internationalen Diskurs nach 1945 *K. Krause/M. Williams*, Security and "Security Studies", in: Gheciu/Wohlforth (Hrsg.), The Oxford Handbook of International Security, 2018, S. 14 (15 ff.). Zu den Wandlungen des Sicherheitsdiskurses in der Bundesrepublik sensibel und umfassend *M. Kötter*, Pfade des Sicherheitsrechts, 2008. Zum Stellenwert des 11.9.2001 in diesem Kontext vgl. aus der uferlosen Literatur nur *A. Voßkuhle*, Das Verhältnis von Freiheit und Sicherheit, in: Heckmann/Schenke/Sydow (Hrsg.), FS T. Würtenberger, 2013, S. 1101 ff.

[4] Zu Umfang und Telos eines entsprechenden „Rechtsgebiets" ausführlich *Gusy*, Sicherheitsrecht als Rechtsgebiet?, in: Dietrich/Gärditz (Hrsg.), FS Graulich, 2019, S. 9 ff. Kritisch

heitsarchitektur".[5] Bei anderen stehen „neues" Sicherheitsrecht und „Sicherheitsstaat" hingegen im Verdacht, liberal-rechtstaatliche Standards zu relativieren. Befürchtet wird gar eine autoritäre Verschärfung: Der Staat der „Sicherheitsgesellschaft" sei, so heißt es, ein „nervöser Staat", in dem der Ausnahme- zum Normalzustand werden könne.[6] Verwiesen wird darauf, welche enormen politischen, sozialen und ökonomischen Ressourcen im Namen der Sicherheit mobilisiert werden.[7] Die Digitalisierung gilt als Treiber dieser Entwicklung, vor allem weil die hier anfallenden Datenmengen und die auf ihrer Grundlage entwickelten Technologien – beispielsweise in Form des Predictive Policing – einen bisher ungekannten Zugriff auf den Einzelnen ermöglichen.[8] Gerade die Debatte um Informations- bzw. Cybersicherheit wird schließlich als Paradefall einer Politik der „Versicherheitlichung" angeführt, weil die dortige Krisenrhetorik rechtlichen Grenzverschiebungen Vorschub leiste.[9] Schon deshalb muss hier reflektiert werden, wie sich das Recht der Informationssicherheit zum Sicherheitsdiskurs verhält.

Dazu muss zunächst die gerade skizzierte Kritik am Sicherheitsbegriff bzw. an dessen neuen Verwendungsformen präzisiert und eingeordnet werden (I.). Anschließend ist speziell der Cyber- bzw. Informationssicherheitsdiskurs daraufhin zu untersuchen, inwieweit diesem die ihm zugeschriebenen grenzverschiebenden Tendenzen tatsächlich innewohnen (II.). Dabei wird sich zeigen, dass effektive Informationssicherheitsgewährleistung zwar nicht in klassischer Gefahrenabwehr aufgehen kann, sondern einen flexibleren Regulierungsan-

---

M. Kniesel, Sicherheitsrecht. Anmerkungen zu einem Rechtsgebiet in der Findungsphase, Die Polizei 2018, S. 265 ff. Siehe auch *M. Baldus*, Entgrenzungen des Sicherheitsrechts, DV 47 (2014), S. 1 ff.; *K. F. Gärditz*, Sicherheitsrecht als Perspektive, GSZ 2017, S. 1 ff.; *H. A. Wolff*, Prävention durch Verwaltungsrecht: Sicherheit, in: VVDStRL 81 (2022), S. 437 ff. Zum verfassungsrechtlichen Pendant – dem „Sicherheitsverfassungsrecht" – siehe grundlegend *R. Poscher*, Sicherheitsverfassungsrecht im Wandel, in: Vesting/Korioth (Hrsg.), Der Eigenwert des Verfassungsrechts, 2011, S. 245 ff.; *S. Tanneberger*, Die Sicherheitsverfassung, 2014; *D. Kugelmann*, Entwicklungslinien eines grundrechtsgeprägten Sicherheitsverwaltungsrechts, DV 47 (2014), S. 25 ff.; *K. F. Gärditz*, Sicherheitsverfassungsrecht und technische Aufklärung durch Nachrichtendienste, EuGRZ 2018, S. 6 ff.; *M. Bäcker*, Sicherheitsverfassungsrecht, in: Herdegen/Masing et al. (Hrsg.), HVerfR, 2021, § 28.

[5] Zum Begriff *T. Würtenberger/S. Tanneberger*, Sicherheitsarchitektur als interdisziplinäres Forschungsfeld, in: Riescher (Hrsg.), Sicherheit und Freiheit statt Terror und Angst, 2010, S. 97 ff.; *B. Rusteberg*, Zivile Sicherheit in der Sicherheitsarchitektur des deutschen Bundesstaates, in: Gusy/Kugelmann/Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, 2017, S. 113 (114).

[6] Zum Begriff *Barczak*, Der nervöse Staat, 2. Aufl. 2021.

[7] *Krause/Williams*, Security and "Security Studies", in: Gheciu/Wohlforth (Hrsg.), The Oxford Handbook of International Security, 2018, S. 14 f.

[8] Zu Predictive Policing siehe nur *T. Rademacher*, Predictive Policing, AöR 142 (2017), S. 366 ff.; *T. Wischmeyer*, Predictive Policing, in: Kulick/Goldhammer (Hrsg.), Der Terrorist als Feind?, 2019, S. 189 ff.; *H. Hofmann*, Predictive Policing, 2020; *L. Sommerer*, Personenbezogenes Predictive Policing, 2020.

[9] Siehe hierzu die Nachweise unten bei § 4 II. 1. a).

satz verfolgen muss, wie er auch vom „neuen" Sicherheitsrecht propagiert wird. Dies zwingt aber nicht zu einem die unterschiedlichen Facetten des Problems harmonisierenden, normative Grenzen relativierenden oder gar den Sicherheitsimperativ verabsolutierenden Zugriff. Im Gegenteil muss hier semantisch abgerüstet und klar zwischen dem allgemeinen Bedürfnis nach (Informations-)Sicherheit und den speziellen Modalitäten seiner Verwirklichung unterschieden werden. Allerdings lassen sich mit Hilfe der Versicherheitlichungsthese Felder identifizieren, denen die juristische Aufarbeitung der Materie besondere Aufmerksamkeit widmen muss (III.).

I. Sicherheit: Auftrag, Perspektive oder Dispositiv?

1. Sicherheit als staatlicher Auftrag

Aus Sicht des Verfassungsrechts ist die Gewährleistung von Sicherheit Ziel und Aufgabe des Staates.[10] Verfassungsdogmatisch wird dies primär dadurch operationalisiert, dass Sicherheit als „Verfassungswert" gilt, der Einschränkungen der Grundrechte rechtfertigen kann.[11] Anerkannt ist, dass dieser Wert nicht absolut gesetzt werden darf; stattdessen ist stets eine „Balance zwischen Freiheit und Sicherheit" zu suchen.[12] Je nachdem, ob dem Schutz- bzw. Si-

[10] Vgl. aus der uferlosen Literatur nur die grundlegenden Beiträge von *J. Isensee*, Das Grundrecht auf Sicherheit, 1983; *M. Möstl*, Die staatliche Garantie für die öffentliche Sicherheit und Ordnung, 2002, S. 14 ff.; *Stoll*, Sicherheit als Aufgabe, 2003, S. 15 ff.; *W. Brugger*, Gewährleistung von Freiheit und Sicherheit, in: VVDStRL 63 (2004), S. 102 ff.; *C. Gusy*, Gewährleistung von Freiheit und Sicherheit, in: VVDStRL 63 (2004), S. 151 (174 ff.); *J. Isensee*, Staatsaufgaben, in: Isensee/Kirchhof (Hrsg.), HStR, Bd. IV, 3. Aufl. 2006, § 73 Rn. 26; *V. Götz*, Innere Sicherheit, in: Isensee/Kirchhof (Hrsg.), HStR, Bd. IV, 3. Aufl. 2006, § 85; *M. Thiel*, Die „Entgrenzung" der Gefahrenabwehr, 2011; *Leuschner*, Sicherheit als Grundsatz, 2018, S. 13 ff.; *Barczak*, Der nervöse Staat, 2. Aufl. 2021, S. 353 ff.; sowie die oben in § 4 Fn. 4 zitierten Titel. Spezifisch zur Informationssicherheit: *Heckmann*, Staatliche Schutz- und Förderpflichten zur Gewährleistung von IT-Sicherheit, in: Rüßmann (Hrsg.), FS Käfer, 2009, S. 129 ff.; *Möllers/Pflug*, Verfassungsrechtliche Rahmenbedingungen des Schutzes kritischer IT-Infrastrukturen, in: Kloepfer (Hrsg.), Schutz kritischer Infrastrukturen, 2010, S. 47 ff.; *Leisterer*, Internetsicherheit in Europa, 2018, S. 31 ff.; *Leuschner*, Sicherheit als Grundsatz, 2018, S. 207 ff.; *R. Poscher/P. Lassahn*, Verfassungsrechtliche Dimensionen der IT-Sicherheit, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 7; siehe dazu ausführlich unten § 5 II. 1.

[11] Emphatisch BVerfGE 49, 24 (56 f.).

[12] BVerfGE 115, 320 (358). Zu den prekären Eigenschaften dieser „Balance", die nicht als polar strukturiertes Spannungsfeld verstanden werden darf, über die oben in § 4 Fn. 10 zitierte Literatur hinaus instruktiv: *O. Lepsius*, Sicherheit und Freiheit, in: Schuppert/Merkel et al. (Hrsg.), Der Rechtsstaat unter Bewährungsdruck, 2010, S. 23 ff.; *J. Masing*, Die Ambivalenz von Freiheit und Sicherheit, JZ 66 (2011), S. 753 ff.; *Voßkuhle*, Das Verhältnis von Freiheit und Sicherheit, in: Heckmann/Schenke/Sydow (Hrsg.), FS T. Würtenberger, 2013, S. 1101 ff.; *J. Isensee*, Sicherheit als Voraussetzung und als Thema einer freiheitlichen Verfas-

cherheitsaspekt im Rahmen dieser Abwägung ein Eigenwert zugestanden oder ob Sicherheit als rein instrumentelles Gut oder aber als – nie ganz zu erreichender[13] – Zustand, in dem sich sonstige (Freiheits-)Rechtsgüter befinden können,[14] verstanden wird, verändert sich die Begründungslast und neigt sich die Waage tendenziell der einen oder anderen Richtung zu. Dogmatisch erschwert werden Abwägung und Grenzziehung zwischen Freiheit und Sicherheit durch die Existenz objektiver Grundrechtsgehalte. Denn insbesondere mit Hilfe der grundrechtlichen Schutzpflicht können Sicherheits- als Freiheitsinteressen reformuliert werden: Eingriffe in die Freiheit der einen lassen sich dann auch damit rechtfertigen, dass nur so der Schutz der Freiheit der anderen realisiert werden kann.[15] Aufgehoben scheint die kategoriale Differenz von Freiheit und Sicherheit schließlich dort, wo – wie im Konventions- und im Unionsrecht – ein eigenständiges Grundrecht „auf Sicherheit" existiert (Art. 5 Abs. 1 EMRK; Art. 6 GRCh); um hier eine Konfusion zu vermeiden, bedarf ein solches „Grundrecht", wenn man ihm denn überhaupt abwehrrechtliche Qualitäten zuerkennen möchte, einer engen tatbestandlichen Begrenzung.[16] Wird Sicherheitsgewährleistung als Voraussetzung des Freiheitsgenusses oder als eigenständiges Grundrecht gedacht, hat dies schließlich über die jeweiligen Abwägungslagen hinaus auch weitreichende institutionelle Konsequenzen.[17]

Die Konstruktion, Kalibrierung und Kritik dieser Maßgaben hat einen guten Teil der Kräfte der Verfassungsrechtsdogmatik unter dem Grundgesetz gebunden.[18] Keine der dabei aufgeworfenen Fragen kann als endgültig gelöst

---

sung, in: Anderheiden/Keil et al. (Hrsg.), GS Brugger, 2013, S. 499 (507 ff.); *W. Hoffmann-Riem*, Der Staat als Garant von Freiheit und Sicherheit, in: Papier/Münch/Kellermann (Hrsg.), Freiheit und Sicherheit, 2016, S. 19 ff.

[13] Zu dieser oft übersehenen Eigenschaft des Sicherheitsbegriffs *C. Gusy*, Ziele, Aufträge und Maßstäbe, in: Gusy/Kugelmann/Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, 2017, S. 55 (59).

[14] So insbes. die nichtjuristische Literatur, vgl. etwa die einflussreiche Definition bei *R. Fischer/E. Halibozek/D. Walters*, Introduction to Security, 10. Aufl. 2018, S. 3: „*Security* implies a stable, relatively predictable environment in which an individual or group may pursue its ends without disruption or harm and without fear of disturbance or injury."

[15] Dazu pointiert *R. Wahl/J. Masing*, Schutz durch Eingriff, JZ 45 (1990), S. 553 ff.

[16] Nach sehr allgemeinen Bezugnahmen auf das Grundrecht jetzt eher restriktiv zur Deutung des Art. 6 GRCh in Richtung eines Grundrechts auf Sicherheit *vor*, nicht *durch* den Staat: EuGH, C-511/18 u. a. v. 6.10.2020, Rn. 125 – La Quadrature du Net u.a: „[…] kann Art. 6 der Charta jedoch nicht dahin ausgelegt werden, dass er die staatlichen Stellen verpflichtet, spezifische Maßnahmen zur Ahndung bestimmter Straftaten zu erlassen". Umfassend zur Problematik *Leuschner*, Sicherheit als Grundsatz, 2018, S. 72 ff.

[17] Wegweisend insoweit *E.-W. Böckenförde*, Grundrechte als Grundsatznormen, Der Staat 29 (1990), S. 1 (25 ff.): „Jurisdiktionsstaat".

[18] Neben den gerade zitierten Schriften siehe nur exemplarisch *G. Robbers*, Sicherheit als Menschenrecht, 1987; *Murswiek*, Die staatliche Verantwortung für die Risiken der Technik, 1985, S. 88 ff.; *G. Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, 1987;

betrachtet werden; ihr Transfer auf die Ebene des Konventions- und Unionsrecht bringt neue Probleme mit sich. Konsentiert bleibt trotz aller Differenzen, dass die Gewährleistung von Sicherheit legitimes Ziel demokratischer Politik und, unter gewissen Bedingungen und in gewissen Grenzen, Auftrag eben dieser ist.

Die allgemeine Grundrechtsdogmatik thematisiert selbst allerdings kaum je näher, was sich inhaltlich hinter dem Begriff der Sicherheit verbirgt. Sie bildet damit auch nur Hintergrund und Maßstab für jene Auseinandersetzung um den Sicherheitsbegriff, auf die in der Einleitung zu diesem Kapitel Bezug genommen wurde. Gewiss geht es auch bei dieser Kontroverse um die Konstruktion und Auflösung grundrechtlicher Abwägungslagen. Doch stehen zunächst Begrifflichkeiten, Perspektiven und Inhalte des einfachen Rechts im Vordergrund, die zunächst als solche gewürdigt werden müssen.[19]

2. Vom „alten" zum „neuen" Sicherheitsrecht: Sicherheit als Perspektive

a) Transformationen des Sicherheitsrechts

Hier, im einfachen Recht, ist seit längerer Zeit ein intensiv diskutierter Transformationsprozess im Gange. Wenn die Funktion des auf die Gewährleistung von Sicherheit gerichteten Rechts ganz allgemein dadurch charakterisiert werden kann, dass dieses auf eine möglichst adäquate Abgrenzung der wechselseitigen privaten Freiheitssphären zielen soll,[20] dann galt dieser Ausgleich nach tradiertem Verständnis dann als gelungen, wenn staatliche Interventionen an konkrete Gefahrenlagen anknüpften, an einen Störer adressiert waren und dem Schutz der „öffentlichen Sicherheit" dienten, wobei letztere weitgehend

P. Szczekalla, Die sogenannten grundrechtlichen Schutzpflichten im deutschen und europäischen Recht, 2002; *R. Poscher*, Grundrechte als Abwehrrechte, 2003, S. 380 ff.; *Möstl*, Die staatliche Garantie für die öffentliche Sicherheit und Ordnung, 2002, S. 42 ff.; *J. Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, 2. Aufl. 2005; *J. Isensee*, Das Grundrecht als Abwehrrecht und als staatliche Schutzpflicht, in: Isensee/Kirchhof (Hrsg.), HStR, Bd. IX, 3. Aufl. 2011, § 191.

[19] Wiederum anders gelagert ist die völkerrechtliche Diskussion um „human security", die aus der Erfahrung mit staatlichem Unrecht und „failed states" heraus Sicherheitsgewährleistung nicht vom Staat her denkt, sondern im Zusammenspiel von Menschenrechten, nichtstaatlichen Akteuren und internationaler Gemeinschaft verorten will. Dazu nur *G. Oberleitner*, Human Security: Idea, Policy and Law, in: Martin/Owen (Hrsg.), Routledge Handbook on Human Security, 2013, S. 319 ff.; *T. Debiel*, Human Security und die Vereinten Nationen, in: Oberdorfer/Werkner (Hrsg.), Menschliche Sicherheit und gerechter Frieden, 2019, S. 13 ff.

[20] Zu dieser Charakterisierung des Sicherheitsrechts: *D. Grimm*, Zukunft der Verfassung, 1991, S. 197 ff.; *Wahl*, Die Aufgabenabhängigkeit von Verwaltung und Verwaltungsrecht, in: Hoffmann-Riem/Schmidt-Aßmann/Schuppert (Hrsg.), Reform des Allgemeinen Verwaltungsrechts, 1993, S. 177 (192).

als Blankettbegriff verstanden wurde („Wahrung der Rechtsordnung"). Dieser Ansatz, der staatliche Sicherheitsgewährleistung mehr oder weniger mit dem etablierten Maßnahmenkatalog der Polizei- und Ordnungsbehörden gleichsetzte, ignorierte schon immer weite Teile des Rechts und der Rechtswirklichkeit, denen ein Interesse an Sicherheitsfragen schwer abgesprochen werden konnte, etwa die Produktsicherheit; mittlerweile kann er auch seinen traditionellen Kernbereich, das Polizei- und Ordnungsrecht, kaum noch adäquat beschreiben. Stattdessen lassen sich dort umfangreiche Grenzverschiebungen beobachten, die sich auf Formeln bringen lassen wie: von der Gefahr zum Risiko – von der Gefahrenabwehr zur (Informations-)Vorsorge gegen drohende Schäden – von der staatlichen Aufgabe zur Verantwortungsteilung – und eben vom „alten" zum „neuen" Sicherheitsrecht.[21]

b) Sicherheitsrecht als Risikorecht

Unabhängig von einer Bewertung dieser Veränderungen im Polizei- und Ordnungsrecht selbst ist zunächst zu konstatieren, dass hier nachvollzogen wird, was in anderen Rechtsbereichen seit der Entdeckung des Risikorechts in den

[21] Aus der umfangreichen Literatur zur Entwicklung des Polizei- und Ordnungsrechts siehe neben den oben in § 4 Fn. 4 zitierten Schriften nur *J. Aulehner*, Polizeiliche Gefahren- und Informationsvorsorge, 1998, S. 47 ff.; *H.-H. Trute*, Die Erosion des klassischen Polizeirechts durch die polizeiliche Informationsvorsorge, in: Erbguth/Müller/Neumann (Hrsg.), GS Jeand'Heur, 1999, S. 403 ff.; *M. Albers*, Die Determination polizeilicher Tätigkeit, 2001; *Möstl*, Die staatliche Garantie für die öffentliche Sicherheit und Ordnung, 2002, S. 147 ff., 253 ff.; *R. Pitschas*, Polizeirecht im kooperativen Staat, in: Pitschas (Hrsg.), Kriminalprävention und „Neues Polizeirecht", 2002, S. 241 ff.; *H.-H. Trute*, Gefahr und Prävention, DV 36 (2003), S. 501 ff.; *F. Schoch*, Abschied vom Polizeirecht des liberalen Rechtsstaats?, Der Staat 43 (2004), S. 347 ff.; *Kötter*, Pfade des Sicherheitsrechts, 2008, S. 182 ff.; *R. Poscher*, Eingriffsschwellen im Recht der inneren Sicherheit, DV 41 (2008), S. 345 ff.; *H.-H. Trute*, Grenzen des präventionsorientierten Polizeirechts, DV 42 (2009), S. 85 ff.; *U. Volkmann*, Polizeirecht als Sozialtechnologie, NVwZ 2009, S. 216 ff.; *Gusy*, Neuer Sicherheitsbegriff, VerwArch 2010, S. 309 ff.; *Thiel*, Die „Entgrenzung" der Gefahrenabwehr, 2011, S. 12 ff.; *B. Park*, Wandel des klassischen Polizeirechts zum neuen Sicherheitsrecht, 2013; *Baldus*, Entgrenzungen des Sicherheitsrechts, DV 47 (2014), S. 1 ff.; *Bäcker*, Kriminalpräventionsrecht, 2015, S. 33 ff.; *A. Leisner-Egensperger*, Polizeirecht im Umbruch, DÖV 2018, S. 677 ff.; *M. Löffelmann*, Die Zukunft der deutschen Sicherheitsarchitektur, GSZ 2018, S. 85 ff.; *M. Möstl*, Staatsaufgabe Sicherheit in Zeiten des Terrorismus, in: Kulick/Goldhammer (Hrsg.), Der Terrorist als Feind?, 2020, S. 67 ff.; *M. Bäcker*, Von der Gefahr zum „Gefährder", in: Kulick/Goldhammer (Hrsg.), Der Terrorist als Feind?, 2020, S. 147 ff.; *Barczak*, Der nervöse Staat, 2. Aufl. 2021, S. 368 ff. Zu aktuellen Einzelproblemen siehe auch *A. Kulick*, Gefahr, „Gefährder" und Gefahrenabwehrmaßnahmen angesichts terroristischer Gefährdungslagen, AöR 143 (2018), S. 175 ff.; *M. Möstl*, Rechtsstaatlicher Rahmen der Terrorabwehr, DVBl. 2020, S. 160 ff.; *A. Kießling*, Die aktionelle Maßnahme im Vorfeld, in: Kulick/Goldhammer (Hrsg.), Der Terrorist als Feind?, 2020, S. 261 ff. Aus der strafprozessualen Paralleldiskussion siehe nur *T. Singelnstein*, Logik der Prävention, in: Brunhöber (Hrsg.), Strafrecht im Präventionsstaat, 2014, S. 41 ff.

späten 1970er-Jahren vorexerziert wurde.[22] Der Risikodiskurs, der sich disziplinübergreifend entwickelt hat und in Gestalt der soziologischen Thesen zur Risikogesellschaft wirkmächtig geworden ist,[23] reagierte ursprünglich auf die Überforderung der klassischen Gefahrendogmatik durch die Ungewissheit bezüglich der Wirkungsweisen und die Unkalkulierbarkeit des Schadenspotenzials beim Einsatz neuer Technologien. Mit der Zeit spielte als Motiv auch die zunehmende territoriale Entgrenzung der Gefährdungslagen eine wichtige Rolle.[24] Auslöser der Debatte waren die ab den 1980er-Jahren verstärkt ins Bewusstsein drängenden ökologischen Krisen und technischen Katastrophen. Rechtlich rezipiert wurden die Ansätze daher zunächst im Umwelt- und Technikrecht. Die Diskussion emanzipierte sich jedoch rasch von einem engen Technikbezug und erschloss sich weitere Bereiche wie das Gesundheits- und Finanzmarktrecht, um schließlich das Sicherheitsrecht im engeren Sinne zu erreichen.[25]

---

[22] Zur Dogmatisierung des Risikobegriffs maßstabsetzend BVerfGE 49, 89 (137 ff.). Aus der Literatur siehe insbes. *Murswiek*, Die staatliche Verantwortung für die Risiken der Technik, 1985; *U. Di Fabio*, Risikoentscheidungen im Rechtsstaat, 1994, S. 98 ff.; A. Bora (Hrsg.), Rechtliches Risikomanagement, 1999 (daraus insbes. *K.-H. Ladeur*, Risikobewältigung durch Flexibilisierung und Prozeduralisierung des Rechts, in: a. a. O., S. 41 ff.; *R. Wolf*, Die Risiken des Risikorechts, in: a. a. O., S. 65 ff.); *A. Scherzberg*, Risikosteuerung durch Verwaltungsrecht, in: VVDStRL 63 (2004), S. 214 (219 ff.); *O. Lepsius*, Risikosteuerung durch Verwaltungsrecht, in: VVDStRL 63 (2004), S. 264 (267 ff.); *Schmidt-Aßmann*, Das allgemeine Verwaltungsrecht als Ordnungsidee, 2. Aufl. 2006, 3/92 ff.; *L. Jaeckel*, Gefahrenabwehrrecht und Risikodogmatik, 2010, S. 57 ff. und passim (zum Gefahrenbegriff als Kontrast a. a. O., S. 90 ff.); *Thiel*, Die „Entgrenzung" der Gefahrenabwehr, 2011, S. 300 ff.; *A.-K. Kaufhold*, Systemaufsicht, 2016, S. 124 ff. (zu Systemrisiken); *A. Klafki*, Risiko und Recht, 2017.

[23] Insbes. in Gestalt der Arbeiten von *Ulrich Beck* – allen voran *Beck*, Risikogesellschaft, 1986. Ähnlich gelagert auch die (theoretisch allerdings stark von Foucault beeinflusste) Studie von *F. Ewald*, Der Vorsorgestaat, 1993. Zeitgenössische (rechts-)kritische Stellungnahmen zu dieser Entwicklung etwa bei *E. Denninger*, Der Präventions-Staat, Kritische Justiz 21 (1988), S. 1 ff.; *H. A. Hesse*, Der Schutzstaat, 1994. Anders dagegen die Perspektive bei Niklas Luhmann (insbes. *Luhmann*, Die Gesellschaft der Gesellschaft, 1997, S. 1088 ff.; *ders.*, Soziologie des Risikos, 2003; *ders.*, Ökologische Kommunikation, 2008), der im Unterschied zu *Beck* nicht neue (tatsächliche) Gefährdungslagen, sondern Veränderungen in der gesellschaftlichen Konstruktion von Zeit und Wirklichkeit für den Aufstieg des Risikoparadigmas verantwortlich macht. Siehe aus der systemtheoretischen Risikoforschung weiter auch *D. Baecker*, Womit handeln Banken?, 1991; *E. Esposito*, The future of futures, 2011.

[24] Vgl. *U. Beck*, Weltrisikogesellschaft, 2008, S. 61 f.: „Die Großgefahren heben die drei tragenden Säulen des Risikokalküls auf. Mit ihnen sind erstens nicht-eingrenzbare, globale, oft irreparable Schädigungen verbunden: Der Gedanke der (geldlichen) Kompensation versagt. Zweitens ist die vorsorgende Nachsorge für den schlimmstdenkbaren Unfall ausgeschlossen: Die antizipatorische Folgenkontrolle ist unmöglich. Drittens ist der ›Unfall‹ raum-zeitlich unbegrenzt."

[25] International verlief der Entwicklungspfad weitgehend analog, vgl. *J. Black*, Risk in Regulatory Processes, in: Baldwin/Cave/Lodge (Hrsg.), Oxford Handbook of Regulation, 2010, S. 302 (304 f.).

In der Rechtswissenschaft fungierte der Risikobegriff als Schlüssel zur Analyse der epistemischen Voraussetzungen von Rechtsetzung und -rechtsanwendung und als Mittel, um entsprechende regulatorische Vorgaben, etwa zur Beachtung des Vorsorgeprinzips, oder Regulierungstendenzen wie die immer stärkere Prozeduralisierung des Rechts zu begreifen und einzuordnen; darüber hinaus wies er einen Weg zu einer holistischen Betrachtung von Regulierungsfragen, die die tradierten Fächergrenzen transzendierten.[26] Dass die mit dem Risikobegriff verkoppelte Einsicht in die Ungewissheit der Entscheidungsbedingungen darüber hinaus genutzt werden konnte, um Exekutive und Legislative weitreichende Einschätzungsspielräume zuzuerkennen und um die Kontrolle der Gerichte auf Verstöße gegen Konsistenz- und Verfahrenspflichten zu beschränken, gehört zu den oft kritisierten Konsequenzen dieses Ansatzes.[27]

c) Ein „neuer" Sicherheitsbegriff

Diese Einsichten gingen nicht verloren, als mit der Zeit die Risiko- wieder von der Sicherheitssemantik überlagert wurde.[28] Der dabei entstehende „neue" Sicherheitsbegriff ist zwar ähnlich inhaltsarm wie der Risikobegriff; insbesondere belastet er sich nicht mit den Konnotationen des „alten" Begriffs der „öffentlichen Sicherheit", setzt Sicherheit also nicht mit jenem konkreten Maßnahmenbündel und jenen spezifischen Gefährdungskonstellationen gleich, die das hergebrachte Polizei- und Ordnungsrecht gekennzeichnet hatten.[29] Stattdessen steht er für eine „Perspektive" auf das Panorama aller staatlichen und gesellschaftlichen Aktivitäten, die an einem möglichst störungsfreien Funktionieren eben dieser Aktivitäten interessiert ist (Außenpolitik, soziale Sicherheit, Lebensmittelsicherheit, Informationssicherheit etc.).[30] Die Deutung des Konzepts Sicherheit als „Perspektive" entschärft zu einem gewissen Grade den Vorwurf der Beliebigkeit, der sich gegen jeden derart universal anwendba-

[26] Vgl. neben der oben in § 4 Fn. 22 zitierten Literatur insbes. auch *B. Wollenschläger*, Wissensgenerierung im Verfahren, 2009, S. 55 ff.

[27] Vgl. beispielhaft BVerfGE 128, 1 (39, Rn. 143); 143, 246 (355, Rn. 307); zu den Grenzen des Verhältnismäßigkeitsgrundsatzes im Risikorecht siehe *Scherzberg*, Risikosteuerung durch Verwaltungsrecht, in: VVDStRL 63 (2004), S. 214 (243); *Jaeckel*, Gefahrenabwehrrecht und Risikodogmatik, 2010, S. 301; *Klafki*, Risiko und Recht, 2017, S. 26 f.

[28] Die Transformation und Verbreiterung des Sicherheitsbegriffs begegnet nicht nur in der Rechtswissenschaft, vgl. den Überblick bei *B. Buzan/L. Hansen*, The Evolution of International Security Studies, 2009.

[29] Hierzu *Gusy*, Sicherheitsrecht als Rechtsgebiet?, in: Dietrich/Gärditz (Hrsg.), FS Graulich, 2019, S. 9 (10).

[30] Siehe stellvertretend für diese vielgebrauchte Formulierung *Gärditz*, Sicherheitsrecht als Perspektive, GSZ 2017, S. 1 ff.

ren Begriff aufdrängen muss.[31] Der Perspektivwechsel setzt dennoch durchaus ein anspruchsvolles und in weiten Strecken noch nicht bewältigtes Programm.

Der – im Detail keineswegs homogene[32] – Neuansatz bezog seine Legitimation aus unterschiedlichen Quellen, darunter auch aus solchen, die schon für den Risikodiskurs maßgeblich waren, etwa dem gesteigerten Vernetzungsgrad und der daraus resultierenden Schadensanfälligkeit moderner Industriegesellschaften[33] sowie dem sich durch den Fortschritt von Wissenschaft und Technik ständig verfeinerten Risikobewusstsein.[34] Weitere Gründe für die Transformation des Sicherheitsdenkens waren die veränderten (geo-)politischen Rahmenbedingungen nach dem Ende des Kalten Krieges, die an die Stelle der konzeptionell klar fassbaren Bipolarität neue, diffusere Bedrohungslagen setzten.[35] Schließlich trug auch die zunehmende digitale Vernetzung dazu bei, dass für das „alte" Sicherheitsrecht prägende Faktoren, insbesondere dessen Anknüpfung an örtlich und zeitlich klar als Gefährdungsquellen identifizierbare Orte und Personen, noch unbrauchbarer als zuvor erschienen. Statt eines differenzierten Regulierungsmodells, das für vorab definierte Bedrohungslagen jeweils konkrete Maßnahmenbündel vorhielt, galt es nun, ein Bedrohungskontinuum in den Blick zu nehmen. Und statt konkrete Schadensursachen (etwa Naturkatastrophen, kriminelle, terroristische oder militärische Bedrohungslagen) je mit einem separaten Rechts- und Maßnahmenregime zu bekämpfen, galt es, den Schutz „vitaler Systeme" umfassend zu gewährleisten.[36]

---

[31] Dieser Vorwurf gegenüber dem (neuen) Sicherheitsbegriff findet sich nicht nur in der Rechtswissenschaft, vgl. etwa *A. Wolfers*, "National" Security as an Ambiguous Symbol, Political Science Quarterly 67:5 (1952), S. 481 ff.; *D. Baldwin*, The Concept of Security, Review of International Studies 23:1 (1997), S. 5 ff.; *Krause/Williams*, Security and "Security Studies", in: Gheciu/Wohlforth (Hrsg.), The Oxford Handbook of International Security, 2018, S. 14 (15).

[32] Vgl. *U. Bröckling*, Dispositive der Vorbeugung, in: Daase/Offermann/Rauer (Hrsg.), Sicherheitskultur, 2012, S. 93 ff.

[33] Hierzu und zum Folgenden *Wiater*, Sicherheitspolitik zwischen Staat und Markt, 2013, S. 33 ff.; *S. Kaufmann*, Das Themenfeld „Zivile Sicherheit", in: Gusy/Kugelmann/Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, 2017, S. 3 ff.

[34] Vgl. *Gusy*, Ziele, Aufträge und Maßstäbe, in: Gusy/Kugelmann/Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, 2017, S. 55 (57), mit Verweis auf *S. Krasmann/B. Paul et al.*, Die gesellschaftliche Konstruktion von Sicherheit, 2014, S. 25.

[35] *K. Kristensen*, 'The Absolute Protection of our Citizens', in: Dunn Cavelty/Kristensen (Hrsg.), Securing 'the Homeland', 2008, S. 63 (67).

[36] Zum Fokus auf „vitale Systeme", zum Perspektivwechsel von den Schadensursachen auf die Schadenswirkungen und zum Paradigma von „low probability, high consequences"-Szenarien im Sicherheitsrecht vgl. *S. Collier/A. Lakoff*, The Vulnerability of Vital Systems, in: Dunn Cavelty/Kristensen (Hrsg.), Securing 'the Homeland', 2008, S. 17 (34); *R. Haverkamp/S. Kaufmann/P. Zoche*, Einführung, in: Zoche/Kaufmann/Haverkamp (Hrsg.), Zivile Sicherheit, 2011, S. 9 ff.; *Kaufmann*, Das Themenfeld „Zivile Sicherheit", in: Gusy/Kugelmann/Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, 2017, S. 3 (4); *Gusy*, Ziele, Aufträge und Maßstäbe, in: Gusy/Kugelmann/Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, 2017, S. 55 (65).

Durch Antizipation potenzieller Risiken und das Ergreifen entsprechende Vorsorgemaßnahmen sollte bereits das Entstehen konkreter Gefahrenlagen möglichst verhindert werden.[37]

Sicherheitspolitik in diesem Sinne muss auf regulatorischer Ebene nach einem integrierten Ansatz streben, der von Regelungen der Daseinsvorsorge („Versorgungssicherheit") über technische Sicherheitsvorgaben („Produktsicherheit"; „Informationssicherheit") bis hin zum klassischen Polizei- und Ordnungsrecht und zum Recht der Nachrichtendienste („innere Sicherheit") reicht. Sie adressiert ein weites Spektrum von Beeinträchtigungen für Güter und Infrastrukturen, das von technischen Ausfällen über Unglücksfälle, Naturkatastrophen und menschliches Versagen bis hin zu feindlichen Angriffen und Terrorismus reicht. In ihren Bereich fallen alle Maßnahmen, die sich der Verhinderung, Eindämmung oder dem Management derartiger Störungen zuordnen lassen. Institutionell-administrativ muss ihr an einer intensiven Vernetzung der einschlägig zuständigen Behörden gelegen sein („Sicherheitsarchitektur").[38]

Ein derart weit verstandener Sicherheitsbegriff ist nur noch als Rahmenkonzept charakterisierbar bzw. muss – wie dies in dem die hier beschriebene Wandlung zusammenfassenden Ansatz der „Zivilen Sicherheit" vorgeschlagen wird – negativ definiert werden als Abwesenheit von potenziellen Störungen, also von Unsicherheit,[39] bzw. als „Sicherheitsgewährleistung mit anderen als militärischen Mitteln".[40] Beides lässt die Frage offen, worin sich Sicherheitsgewährleistung noch von anderen Zielen demokratischer Politik und die zu diesem Zweck bemühten Mitteln von den allgemeinen regulatorischen Instrumenten unterscheiden. Insgesamt ist Sicherheit, ähnlich wie schon der Gegenbegriff, das Risiko, im „neuen" Recht weitgehend zur Chiffre für Regulierungsbedürftigkeit geworden.[41]

d) Erscheinungsformen des „neuen" Sicherheitsrechts

Trotz oder gerade wegen dieser definitorischen Offenheit hat sich dieser Perspektivwechsel in Rechtspolitik und Rechtswissenschaft als überaus anschluss-

---

[37] Zusammenfassend *Barczak*, Der nervöse Staat, 2. Aufl. 2021, S. 369.

[38] *S. Kaufmann*, Zivile Sicherheit, in: Hempel/Krasmann/Bröckling (Hrsg.), Sichtbarkeitsregime, 2011, S. 101 (102).

[39] Für einen alternativen, am Sorge-Konzept ansetzenden Sicherheitsbegriff siehe *Folkers*, Das Sicherheitsdispositiv der Resilienz, 2018, S. 40, 226 ff., 353 ff.

[40] So *Gusy*, Ziele, Aufträge und Maßstäbe, in: Gusy/Kugelmann/Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, 2017, S. 55 (66).

[41] Vgl. zum Sicherheitsbegriff das am Beginn dieses Kapitels abgedruckte Zitat von *Luhmann*, Soziologie des Risikos, 2003, S. 29. Analog zum Risikobegriff *Black*, Risk in Regulatory Processes, in: Baldwin/Cave/Lodge (Hrsg.), Oxford Handbook of Regulation, 2010, S. 302 ff. Die Differenzen zwischen Sicherheits- und Risikoansatz werden präzise herausgearbeitet durch *Folkers*, Das Sicherheitsdispositiv der Resilienz, 2018, S. 29 ff. und passim.

fähig erwiesen. Welche Transformationen dieser Neuansatz im Kernbereich des tradierten Polizei- und Ordnungsrecht mit sich gebracht hat, ist bereits Gegenstand intensiver Untersuchungen geworden. Diese sollen hier nicht noch einmal rekapituliert werden.[42] Stattdessen sind die praktischen Konsequenzen des Neuansatzes an zwei typischerweise nicht im Zentrum der rechtswissenschaftlichen Befassung stehenden, für das neue Sicherheitsdenken aber paradigmatischen Sachbereichen herauszuarbeiten, an denen sich zugleich für die Bewertung des Informationssicherheitsrechts wesentliche Weichenstellungen aufzeigen lassen.

So hat sich die Modernisierung des lange „verdrängten" Katastrophenrechts[43] und seine Fortentwicklung zu einem den Schutz vor Naturkatastrophen (klassisch: Katastrophenschutzrecht in Länderkompetenz) und im Verteidigungsfall (klassisch: Zivilschutzrecht in Bundeskompetenz, Art. 73 Abs. 1 Nr. 1 GG) integrierenden *Bevölkerungsschutzrecht* aus Effizienzgründen die Annahme zu eigen gemacht, dass eine übergreifende, nicht auf die Ursachen, sondern auf die Auswirkungen der Katastrophen ausgerichtete Planung geboten sei; begründet wurde dies damit, dass in Zeiten hybrider Bedrohungen nicht immer eindeutig ist, ob die Ursache eines Schadens in einer Naturkatastrophe oder einem zur Auslösung des Verteidigungsfalls nötigenden Geschehen liegt.[44] Umgesetzt wurde die Reform 2009 durch die Neufassung des einschlägigen Gesetzes über den Zivilschutz und die Katastrophenhilfe des Bundes (ZSKG) und die Einrichtung des BBK.[45] Dass die praktische Durchführung hinter den politischen und rechtlichen Vorgaben zurückbleibt,

---

[42] Vgl. die Nachweise oben in § 4 Fn. 21.

[43] So noch die Diagnose bei *H.-H. Trute*, Katastrophenschutzrecht, KritV 88 (2005), S. 342 ff.

[44] *M. Kloepfer/A. Walus/S. Deye/F. Schärdel*, Handbuch des Katastrophenrechts, 2015, S. 75 f. Zu weiteren – auch fiskalischen – Motiven siehe *K. Pohlmann*, Bundeskompetenzen im Bevölkerungsschutz, in: Lange/Endreß/Wendekamm (Hrsg.), Versicherheitlichung des Bevölkerungsschutzes, 2013, S. 249 (250 f., 254).

[45] Aus dem Schrifttum siehe insbes. *R. Stober/S. Eisenmenger*, Katastrophenverwaltungsrecht, NVwZ 2005, S. 121 ff.; M. Kloepfer (Hrsg.), Katastrophenrecht, 2008; *K. Meyer-Teschendorf*, Fortentwicklung der Rechtsgrundlagen für den Bevölkerungsschutz, DVBl. 2009, S. 1221 ff.; H.-J. Lange/C. Gusy (Hrsg.), Kooperation im Katastrophen- und Bevölkerungsschutz, 2015 (daraus insbes. *C. Gusy*, Katastrophenschutzrecht, in: a. a. O., S. 65 ff.); *Kloepfer/Walus/Deye/Schärdel*, Handbuch des Katastrophenrechts, 2015; *Gusy*, Ziele, Aufträge und Maßstäbe, in: ders./Kugelmann/Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, 2017, S. 55 ff.; *A. Thiele*, Zivile Sicherheit im Katastrophenrecht, in: Gusy/Kugelmann/Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, 2017, S. 539 ff.; *C. Gusy*, Katastrophenrecht, GSZ 2020, S. 101 ff.; *W. Köck*, Katastrophenschutzrecht, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht, Bd. 3, 4. Aufl. 2021, § 71. Monographische Darstellungen der Materie sind nach wie vor selten. Aus der einschlägigen Reihe im Nomos-Verlag „Schriften zum Katastrophenrecht" zuletzt *A.-M. Grüner*, Biologische Katastrophen, 2017.

steht auf einem anderen Blatt.[46] Unabhängig davon ist an der Materie vor allem der zeitlich umfassende Ansatz bemerkenswert: Dem Katastrophenrecht im weiteren Sinne werden bereits die Vorgaben zur Katastrophenvermeidung zugeordnet. Das Katastrophenrecht im engeren Sinne bilden dann die Katastrophenvorsorge- und die eigentlichen Katastrophenbekämpfungsmaßnahmen (umfassend geregelt in den Katastrophenschutzgesetzen und den Brandschutz- und Rettungsdienstgesetzen der Länder); abgerundet wird die Materie durch rechtliche Vorgaben zur Katastrophennachsorge, die sich wie das Katastrophenvermeidungsrecht überwiegend im Bundesrecht finden.[47] Auf die mit einem solchermaßen „teleologisch" gedachten Regulierungskonzept verbundenen kompetenzrechtlichen Probleme wird gleich noch einzugehen sein.

Zuvor ist jedoch auf den zweiten Anwendungsfall einzugehen: die sich mit dem Katastrophenrecht teilweise überlagernden, in ihrer Schutzrichtung aber distinkten Bemühungen zum Schutz „kritischer Infrastrukturen" (KRITIS).[48] Auch das ab Mitte der 1990er-Jahre entwickelte KRITIS-Konzept[49] zielt im

[46] Dazu gleich unter § 4 I. 3. b) cc). Siehe auch *BMI/BBK*, Stärkung des Bevölkerungsschutzes durch Neuausrichtung des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe, März 2021; *Bundesregierung*, Deutsche Strategie zur Stärkung der Resilienz gegenüber Katastrophen, Juli 2022.

[47] Zu diesen und alternativen Ordnungsmodellen *Trute*, Katastrophenschutzrecht, KritV 88 (2005), S. 342 (349); *Gusy*, Katastrophenschutzrecht, in: Lange/Gusy (Hrsg.), Kooperation im Katastrophen- und Bevölkerungsschutz, 2015, S. 65 (67).

[48] Näher zum Verhältnis des KRITIS-Diskurses zum Katastrophenrecht sowie zum allgemeinen Infrastrukturrecht: *T. Wischmeyer/O. Schumacher*, Schutz kritischer Infrastrukturen, in: Dietrich et al. (Hrsg.), Handbuch Sicherheits- und Staatsschutzrecht, 2022, § 14 Rn. 6 ff. Zu letzterem siehe nur *G. Hermes*, Staatliche Infrastrukturverantwortung, 1998; *O. Dörr*, Infrastrukturrecht, in: VVDStRL 73 (2014), S. 323 ff.; *H. Wißmann*, Infrastrukturrecht, in: VVDStRL 73 (2014), S. 369 ff.; *K. F. Gärditz*, Infrastruktursicherung, in: Kirchhof/Korte/Magen (Hrsg.), Öffentliches Wettbewerbsrecht, 2014, S. 363 ff.; *A. Voßkuhle*, Staatsaufgabe Infrastruktur, in: Habersack/Huber/Spindler (Hrsg.), FS Stilz, 2014, S. 675 ff.; im allgemeinen Infrastrukturrecht spielen Sicherheitsaspekte bisher kaum eine Rolle, vgl. bereits *F. Schoch*, Diskussionsbemerkung, in: VVDStRL 73 (2014), S. 431.

[49] Zu Vorläufern *A. Folkers*, Kritische Infrastruktur, Arch+ 2020, S. 102 ff. Ausgangspunkt der heutigen Debatte war der Abschlussbericht der *U.S. President's Commission on Critical Infrastructure Protection (PCCIP)*, Critical Foundations: Protecting America's Infrastructures, 1997. Deutschland reagierte hierauf 1997 mit der Einrichtung der Interministeriellen Arbeitsgruppe Kritische Infrastrukturen (AG KRITIS – nicht zu verwechseln mit der 2018 gegründeten gleichnamigen privaten Arbeitsgruppe), deren Abschlussbericht 2000 vorlag; zum Einfluss der U.S.-Vorarbeiten auf die deutsche Umsetzung *M. Kloepfer*, Einleitung, in: ders. (Hrsg.), Schutz kritischer Infrastrukturen, 2010, S. 9 (12). Der anschließende Diskurs war maßgeblich davon geprägt, dass sich seit der Jahrtausendwende terroristische Anschläge zunehmend gegen zivile Infrastrukturen richteten. Zu den Reaktionen in den USA vgl. *T. Schulze*, Bedingt abwehrbereit, 2006, S. 164 ff.; *Wiater*, Sicherheitspolitik zwischen Staat und Markt, 2013, S. 36. Für die deutsche Politikentwicklung wurde dann maßgeblich *BMI*, Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), 2009. Zu den Entwicklungen seither zusammenfassend *BBK*, 10 Jahre „KRITIS-Strategie", 2020. Fast zeitgleich zur deutschen KRITIS-Strategie begann sich auch die Europäische Union in Form der Richtlinie 2008/114/EG vom 8.12.2008 über die Ermittlung europäischer

Sinne des neuen Sicherheitsbegriffs auf eine ganzheitliche Regulierung.[50] Eine Schärfung erfährt es durch die Konzentration auf bestimmte Regulierungsobjekte, nämlich die als „kritisch" identifizierten Infrastrukturen.[51] Diese sollten vor möglichst allen Gefahren, unabhängig von der Art der Gefahrenquelle und der Form der Bedrohung, geschützt werden. Verhindert werden soll so jede Form des Ausfalls oder der Beeinträchtigung, unabhängig davon, ob diese durch äußere Angriffe, Terrorismus, kriminelles Handeln, technisches oder menschliches Versagen oder Naturereignisse verursacht worden ist.[52] Entsprechend ist auch von einem „All-Gefahren-Ansatz" die Rede, der dem Vorsorge-Grundsatz verpflichtet ist.[53]

Die zur Erreichung dieser Ziele gewählten Mittel müssen dementsprechend vielfältig sein.[54] In der Regulierungspraxis stehen dennoch bestimmte Gefahrenarten im Vordergrund: zunächst die physische Anlagensicherheit, jetzt die

kritischer Infrastrukturen (EKI-RL) der Thematik zu nähern. Zu deren beschränktem Anwendungsbereich und zu aktuellen Reformplänen siehe *Wischmeyer/Schumacher*, Schutz kritischer Infrastrukturen, in: Dietrich et al. (Hrsg.), Handbuch Sicherheits- und Staatsschutzrecht, 2022, § 14 Rn. 8, 106.

[50] Aus dem weiteren Schrifttum zur Thematik siehe zunächst *M. Sonntag*, IT-Sicherheit kritischer Infrastrukturen, 2005; *Schulze*, Bedingt abwehrbereit, 2006; M. Kloepfer (Hrsg.), Schutz kritischer Infrastrukturen, 2010; *Wiater*, Sicherheitspolitik zwischen Staat und Markt, 2013, S. 19 ff.; *S. Schulz/J. Tischer*, Internet als kritische Infrastruktur, ZG 2013, S. 339 ff.; *A. Guckelberger*, Energie als kritische Infrastruktur, DVBl. 2015, S. 1213 ff. Vor allem die Veröffentlichungen aus jüngerer Zeit stellen dann stark den Aspekt der Informationssicherheit in den Vordergrund. Zu der entsprechenden Literatur siehe unten § 6 II. 5.

[51] Freilich ist „Kritikalität" als relationaler Begriff selbst strukturell unbestimmt, vgl. *J. Engels*, Relevante Beziehungen, in: Engels/Nordmann (Hrsg.), Was heißt Kritikalität?, 2018, S. 17 (33); *A. Folkers*, Was ist kritisch an Kritischer Infrastruktur?, in: Engels/Nordmann (Hrsg.), Was heißt Kritikalität?, 2018, S. 123 (146); zur Operationalisierung im Recht bedarf es daher einer rechtsförmigen Konkretisierung des Anwendungsbereichs, vgl. *O. Schumacher*, Relevanzzuschreibungen im Recht der Pandemie, GSZ 2021, S. 155 (159 ff.).

[52] Hierzu und zum Folgenden bereits *Wischmeyer/Schumacher*, Schutz kritischer Infrastrukturen, in: Dietrich et al. (Hrsg.), Handbuch Sicherheits- und Staatsschutzrecht, 2022, § 14 Rn. 74.

[53] *BMI*, KRITIS-Strategie, 2009, S. 7. Analog für das Konzept der Zivilen Sicherheit insgesamt *Gusy*, Ziele, Aufträge und Maßstäbe, in: Gusy/Kugelmann/Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, 2017, S. 55 (61 ff.); *Rusteberg*, Zivile Sicherheit in der Sicherheitsarchitektur des deutschen Bundesstaates, in: Gusy/Kugelmann/Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, 2017, S. 113 (114).

[54] Zu den Instrumenten zählen Planungs- und Monitoring-Pflichten, Pflichten zur Personalauswahl und -steuerung, technische Sorgfalts- und Sicherungspflichten, sektorabhängige Bereitstellungs-, Vorhalte- und Leistungspflichten, Pflichten zur Einführung von Risikomanagementsystemen sowie – im Schadensfall – Informationspflichten, Pflichten zur angemessenen Verteilung noch vorhandener Ressourcen, Schadensminderungs- und Beseitigungspflichten sowie Betriebsaufrechterhaltungspflichten. Dazu umfassend *Wischmeyer/Schumacher*, Schutz kritischer Infrastrukturen, in: Dietrich et al. (Hrsg.), Handbuch Sicherheits- und Staatsschutzrecht, 2022, § 14 Rn. 81 ff.

Informationssicherheit.[55] Letztere gewann ab Mitte der 2000er-Jahre immer stärkeres Gewicht innerhalb des KRITIS-Diskurses und dominiert diesen heute. Folgerichtig findet sich die maßgebliche Definition kritischer Infrastrukturen im Informationssicherheitsrecht, konkret in § 2 Abs. 10 S. 1 BSIG. Danach gelten als KRITIS alle Einrichtungen, Anlagen oder Teile davon, die bestimmten Sektoren – namentlich Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen – zuzuordnen sind und die zugleich „von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden".[56] Die Auswahl der Sektoren im BSIG wird dabei stark durch die grundgesetzliche Kompetenzordnung vorgeprägt.[57]

Auf die spezifisch informationssicherheitsrechtlichen Regelungen, die auf dem KRITIS-Ansatz aufbauen und die sich nicht nur im BSIG, sondern auch in zahlreichen weiteren Normen wie dem EnWG finden, wird noch ausführlich einzugehen sein. An dieser Stelle ist nur darauf hinzuweisen, dass der KRITIS-Ansatz nicht in der Informationssicherheitsregulierung aufgeht; dort ist die (partielle) Konsolidierung durch den Gesetzgeber nur am weitesten fortgeschritten.

3. Kritik der „Versicherheitlichung": Sicherheit als Dispositiv

a) Diagnose der Diskursverschiebung

Ebenso wie die am Vorsorge- und Präventionsparadigma ausgerichteten Transformationen des zunehmend auf die „personenbezogene Sicherheitsgewährleistung"[58] gerichteten Sicherheitsrechts im engeren Sinne – also des Po-

[55] Zum physischen Anlagenschutz grundlegend *BMI*, Basisschutzkonzept, 2005. Zum Schutz von IT-Infrastrukturen zunächst *BMI*, Nationaler Plan zum Schutz der Informationsinfrastrukturen, 2005; zur Fortentwicklung in den aktuellen Cybersicherheitsstrategien für Deutschland und die EU siehe oben § 1 Fn. 22. Auf Seite der nachgeordneten Behörden bedeutete diese Schwerpunktverlagerung einen deutlichen Kompetenzgewinn des BSI zugunsten des BBK.

[56] Eine Konkretisierung erfolgt durch die BSI-Kritisverordnung (BSI-KritisV) vom 22.4.2016 (BGBl. I S. 958), zuletzt geändert durch Art. 1 der Verordnung vom 6.9.2021 (BGBl. I S. 4163). Dazu näher unten § 6 II. 4. b).

[57] Dazu gleich unter § 4 I. 3. b) cc). Zur Differenz zwischen dem allgemeinen Begriff der „Kritischen Infrastruktur" und dem Begriff „Kritische Infrastruktur im Sinne von BSIG/BSI-KritisV" näher *BBK*, Klärung und Erweiterung des KRITIS-Vokabulars, Januar 2021, S. 8.

[58] So – in Anlehnung an *Kloepfer/Walus/Deye/Schärdel*, Handbuch des Katastrophenrechts, 2015, § 17 Rn. 16 ff. – *Rusteberg*, Zivile Sicherheit in der Sicherheitsarchitektur des deutschen Bundesstaates, in: Gusy/Kugelmann/Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, 2017, S. 113 (117).

lizei- und Ordnungsrechts, des Rechts der Nachrichtendienste und des als „Kriminalpräventionsrecht" rekonfigurierten Straf- und Strafprozessrechts[59] – sind nun auch der Umbau des Katastrophen- zum Bevölkerungsschutzrecht sowie der Ausbau der Regelungen zum Schutz kritischer Infrastrukturen Einwänden ausgesetzt. Während sich die Kritik an den personenbezogenen Maßnahmen regelmäßig an bestimmten, als übermäßig qualifizierten Eingriffsmaßnahmen bzw. an als ungenügend bewerteten Eingriffsvoraussetzungen festmachen lässt, ist bei den eher technischen Vorgaben des Bevölkerungsschutzrechts und des Rechts der kritischen Infrastrukturen freilich nicht offensichtlich, ob und wie diese den Weg in eine illiberale „Sicherheitsgesellschaft" ebnen sollen.[60] Dennoch wird auch insoweit zur Vorsicht gemahnt: Wenn alles zur Frage der Sicherheit werde, setze dies eine politische und mediale Vorsorgelogik in Gang, in der die neuen Risiken jene Gefährdungslagen zu überschatten drohen, auf deren Verhinderung die Institutionen des freiheitlichen Rechtsstaates einst zugeschnitten wurden.[61] Mehr noch leiste die Proliferation von Krisenszenarien und das Primat der Risikominimierung der Rechtfertigung außergewöhnlicher, d. h. potenziell übermäßig freiheitseinschränkender Maßnahmen Vorschub.[62] Indem der Sicherheitsdiskurs ständig neue Bedrohungsszenarien konstruiere und das (Un-)Sicherheitsgefühl der Bevölkerung (über-)sensibilisiere, ermögliche er strukturell illiberale Politik.[63] Diese und ähnliche Punkte bilden den Kern der Kritik an einer Diskursverschiebung, die auch als „Versicherheitlichung" bezeichnet und als Korrelat und Vorbedingung des Rückbaus rechtsstaatlicher Standards wahrgenommen wird.

Eine entsprechende Diskurskritik, die gegenüber der älteren Risikoliteratur eine „Verschiebung des Analysegegenstands und der Analyseperspektive: von einer Soziologie des Risikos zu einer Analytik der Sicherheit" bzw. – sehr ver-

---

[59] Zu letzterem grundlegend *Bäcker*, Kriminalpräventionsrecht, 2015 (illustrativ etwa a. a. O., S. 319 ff., zur Vorverlagerung der Strafbarkeit durch die Schaffung von abstrakten Gefährdungsdelikten, wie sie u. a. für die Terrorismusbekämpfung genutzt werden). Zur Gesamtthematik siehe die Nachweise oben in § 4 Fn. 21.

[60] Ausführliche Ausarbeitungen der kritischen Positionen bei *P.-A. Albrecht*, Das Strafrecht auf dem Weg zur Sicherheitsgesellschaft, in: Schuppert/Merkel et al. (Hrsg.), Der Rechtsstaat unter Bewährungsdruck, 2010, S. 55 ff.; *T. Singelnstein/P. Stolle*, Sicherheitsgesellschaft, 3. Aufl. 2012. Vgl. auch die daran orientierte Beschreibung bei *Barczak*, Der nervöse Staat, 2. Aufl. 2021, S. 359 f.

[61] Dazu allgemein *Krasmann/Paul/Schlepper/Kühne/Kreissl*, Die gesellschaftliche Konstruktion von Sicherheit, 2014; siehe auch *Gusy*, Ziele, Aufträge und Maßstäbe, in: Gusy/Kugelmann/Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, 2017, S. 55 (56 f.).

[62] So etwa *Dunn Cavelty*, Gesellschaft im Daueralarm, in: Daase/Engert/Junk (Hrsg.), Verunsicherte Gesellschaft – überforderter Staat, 2013, S. 133 ff.

[63] *P. Stolle*, Das (Un-)Sicherheitsgefühl, Kritische Justiz 44 (2011), S. 16 ff.; *Gusy*, Ziele, Aufträge und Maßstäbe, in: Gusy/Kugelmann/Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, 2017, S. 55 (62).

einfacht – von *Ulrich Beck* zu *Michel Foucault* vornimmt und die dementsprechend die „Risiken der Sicherheit" in den Vordergrund stellen will,[64] hat – ausgehend von der Theorie internationaler Beziehungen – in der Soziologie und der Politikwissenschaft heute breite Gefolgschaft gefunden[65] und wird zunehmend auch in der Rechtswissenschaft rezipiert.[66] Sicherheit ist damit nicht mehr einfach ein Zustand oder gar ein Wert, sondern ein „Sprechakt": Indem etwas als Frage der Sicherheit markiert wird, wird das so Bezeichnete aus der „normalen" Ordnung der Dinge ausgeschieden, mit der Emotion Angst besetzt und als Ausnahme entsprechenden Sonderregelungen unterworfen. Hierauf müsse im Sinne einer „desecuritization" mit einer Kultur der Normalisierung, der Rationalisierung und des Kompromisses reagiert werden.[67]

---

[64] So die griffige Formulierung bei *Folkers*, Das Sicherheitsdispositiv der Resilienz, 2018, S. 39 f. *F. Lentzos/N. Rose*, Die Unsicherheit regieren, in: Purtschert/Meyer/Winter (Hrsg.), Gouvernementalität und Sicherheit, 2008, S. 75 (77), sprechen in diesem Sinne vom „Regieren der Unsicherheit". Grundlegend für diesen Literaturzweig sind dementsprechend *M. Foucault*, Überwachen und Strafen, 1976; *ders.*, Sicherheit, Territorium, Bevölkerung, 2004.

[65] Zu konstruktivistischen Ansätzen, unter denen vor allem die sog. Kopenhagener Schule der internationalen Beziehungen Prominenz erlangt hat, vgl. *O. Wæver*, Securitization and Desecuritization, in: Lipschutz (Hrsg.), On Security, 1995, S. 46 ff.; *B. Buzan/O. Wæver/J. Wilde*, Security, 1998; *T. Balzacq*, Securitization Theory, 2011; *H. Stritzel*, Security in Translation, 2014. Zur Einordnung dieser Richtung in die allgemeine Sicherheitsforschung *Krause/Williams*, Security and "Security Studies", in: Gheciu/Wohlforth (Hrsg.), The Oxford Handbook of International Security, 2018, S. 14 (21 ff.). Aus der Fülle an weiteren, mehr oder weniger eng an dieses Paradigma und/oder an Foucault anschließenden Texten siehe nur *S. Opitz*, Zwischen Sicherheitsdispositiv und Securitization, in: Purtschert/Mayer/Winter (Hrsg.), Gouvernementalität und Sicherheit, 2008, S. 201 ff.; *E. Conze*, Securitization, Geschichte und Gesellschaft 38 (2012), S. 453 ff. (zur Leistungsfähigkeit des Konzepts in historischer Hinsicht); *B. Godefroy*, Von der Krise zur Versicherheitlichung, in: Korte (Hrsg.), Politik in unsicheren Zeiten, 2016, S. 62 ff. (zur Verbindung mit älteren Krisen-Modellen); *U. Bröckling*, Gute Hirten führen sanft, 2017, S. 73 ff. Überblick über verschiedene Ansätze bei *C. Daase*, Sicherheitskultur als interdisziplinäres Forschungsprogramm, in: Daase/Offermann/Rauer (Hrsg.), Sicherheitskultur, 2012, S. 23 ff.

Zur Rezeption des Konzepts in der Forschung zur (deutschen) inneren Sicherheit siehe etwa *Kaufmann*, Das Themenfeld „Zivile Sicherheit", in: Gusy/Kugelmann/Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, 2017, S. 3 (9 f.); *A. Kretschmann*, Soziale Tatsachen, APuZ 67:32/33 (2017), S. 11 ff.; *A. Kretschmann/A. Legnaro*, Abstrakte Gefährdungslagen. Zum Kontext der neuen Polizeigesetze, APuZ 69:21/23 (2019), S. 11 ff.; *dies.*, Die „drohende Gefahr" als Schlüsselbegriff einer Sekuritisierung des Rechts, Zeitschrift für Rechtssoziologie 40 (2020), S. 3 ff. Siehe auch – allerdings ohne theoretischen Überbau – H.-J. Lange/C. Endreß/M. Wendekamm (Hrsg.), Versicherheitlichung des Bevölkerungsschutzes, 2013.

[66] Siehe etwa *Gusy*, Ziele, Aufträge und Maßstäbe, in: Gusy/Kugelmann/Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, 2017, S. 55 (67 ff.); *T. Walter*, Der Staat als Sicherheitsgarant?, 2019, S. 58 ff.; *Barczak*, Der nervöse Staat, 2. Aufl. 2021, S. 445, 595.

[67] *C. Aradau*, Security and the Democratic Scene, Journal of International Relations and Development 7:4 (2004), S. 388 ff.; *L. Hansen*, Reconstructing Desecuritisation, Review of International Studies 38:3 (2012), S. 525 ff.; *P. Bourbeau/J. Vuori*, Security, Resilience and Desecuritization, Critical Studies on Security 3:3 (2015), S. 253 ff.

In eine ähnliche Richtung geht die Deutung von Sicherheit als „Dispositiv", das Techniken, Technologien und Praktiken bündelt, die in einer charakteristischen Art und Weise der Konstituierung und Ausübung von Macht dienen – und das als solches zum Widerspruch herausfordert.[68]

b) Folgen für das Rechtssystem: Identifikation von Aufmerksamkeitsfeldern I

Es lässt sich durchaus in Frage stellen, ob ein jeder Form staatlicher Sicherheitspolitik entgegengebrachter Radikalverdacht die praktischen Effekte der Sicherheitsrhetorik des Staates nicht deutlich überschätzt.[69] Aus rechtswissenschaftlicher Sicht bedeutsamer ist, dass sich eine „Diskursverschiebung", wie sie verbreitet diagnostiziert wird, juristisch erst dann sicher fassen lässt, wenn sie in rechtlich verbindlichen Entscheidungen ihren Niederschlag findet. Die semantische Tatsache, dass eine Materie wie der Katastrophenschutz als Sicherheitsfrage diskutiert wird, löst ebenso wenig wie ihre Zuordnung zu einem rein analytisch-deskriptiv verstandenen „Sicherheitsrecht" qualifizierbare Rechtsfolgen aus. Auch die schnelle Folge von vom Vorsorgegedanken beherrschten, freiheitseinschränkenden Rechtsänderungen, wie sie etwa im Fall der Terrorismusbekämpfung begegnet, oder der stete Ausbau „technischer" Sicherheitsmaßnahmen durch das KRITIS-Konzept[70] können zwar je Anlass für rechtspolitische Kritik an den Einzelmaßnahmen und an deren Kumulation geben, rechtfertigen jedoch für sich noch nicht das Urteil, es komme zu einer Einsickerung des Ausnahmezustands in den Normalzustand bzw. zu einer „Denormalisierung des Normalzustands",[71] solange nicht gezeigt wird, dass damit auch eine Verschiebung der verfassungsrechtlichen Bewertungsmaßstäbe oder eine Erosion der zu ihrem Schutz berufenen Kontrollinstanzen erfolgt. Soweit aber eine entsprechende Kontrolle gewährleistet bleibt, ist

[68] Zum notorisch unscharfen Dispositiv-Begriff – so bleibt bei Foucault selbst etwa unklar, ob es nur ein bestimmtes oder mehrere unterschiedliche Sicherheitsdispositive gibt – siehe die knappe Definition bei *M. Foucault*, Dispositive der Macht, 1978, S. 119 f.: „ein entschieden heterogenes Ensemble, das Diskurse, Institutionen, architekturale Einrichtungen, reglementierende Entscheidungen, Gesetze, administrative Maßnahmen, wissenschaftliche Aussagen, philosophische, moralische oder philanthropische Lehrsätze, kurz: Gesagtes ebensowohl wie Ungesagtes umfaßt". Vgl. die instruktive Aufschlüsselung der diesbezüglichen Literatur bei *Folkers*, Das Sicherheitsdispositiv der Resilienz, 2018, S. 51 ff.

[69] Vgl. *Folkers*, Das Sicherheitsdispositiv der Resilienz, 2018, S. 51 ff., in Auseinandersetzung mit *Beck*, Weltrisikogesellschaft, 2008, S. 151.

[70] Siehe hierzu die spezifische Kritik bei *M. Dunn Cavelty/K. Kristensen*, Introduction, in: dies. (Hrsg.), The Politics of Securing the Homeland, 2008, S. 1 ff.

[71] So die Formulierung bei *Barczak*, Der nervöse Staat, 2. Aufl. 2021, S. 447; vgl. auch die Verweise a. a. O., S. 446, auf die ältere Literatur, insbes. *U. Berlit/H. Dreier*, Die legislative Auseinandersetzung mit dem Terrorismus, in: Sack/Steinert (Hrsg.), Protest und Reaktion, 1984, S. 227 (297).

auch eine entgrenzte Verwendung der Sicherheitssemantik durch die Politik als Ausdruck demokratischer Präferenzen hinzunehmen.

Die spezifisch juristische Kritik muss daher die Auseinandersetzung mit den individuellen Maßnahmen einerseits und den womöglich im Wandel befindlichen Maßstäben andererseits suchen. Diese Arbeit findet in der Rechtswissenschaft nun durchaus intensiv statt und ist durch den neuen Sicherheitsdiskurs keineswegs suspendiert.[72] Auch die Gerichte zeigen bislang wenig Neigung, ihre Maßstäbe für die Prüfung sicherheitspolitisch begründeter Maßnahmen in Frage zu stellen. Folgenden „Aufmerksamkeitsfelder" (*Wolfgang Hoffmann-Riem*) – die im weiteren Verlauf der Arbeit näher auszuloten sein werden[73] – drängen sich jedoch für die weitere rechtswissenschaftliche Forschung auf:

aa) Grundrechte

Staatliche Maßnahmen, die im „Vorfeld" konkreter Gefahren Zugriffsmöglichkeiten staatlicher Behörden schaffen, werden vor allem in grundrechtlicher Hinsicht einer derart umfassenden Kontrolle unterzogen, dass der Versuch, deren Linien hier auf einer abstrakten Ebene nachzuzeichnen, den vorliegenden Rahmen sprengen würde.[74] Allgemein lässt sich nur festhalten, dass jene von der Kritik an den Praktiken der Versicherheitlichung vorgebrachten Punkte – die Vorverlagerung von Eingriffen, die Personalisierungstendenzen der Gefahrenabwehr, die Entdifferenzierung der Eingriffsnormen durch umfassende Informationsweitergabe innerhalb des Staatsapparats etc. – in der Grundrechtsdogmatik umfassend bearbeitet und von der Verfassungsgerichtsbarkeit intensiv begleitet werden.[75]

bb) Gewaltenteilung

Weniger Aufmerksamkeit hat demgegenüber bislang eine weitere mit Versicherheitlichung assoziierte Konsequenz erhalten, nämlich deren Drang zur Verschiebung von Zuständigkeitsgrenzen. Soweit allerdings mögliche Ver-

---

[72] So selbstverständlich auch in der Arbeit von *Barczak*, Der nervöse Staat, 2. Aufl. 2021. Siehe entsprechend die Literatur zum „Sicherheitsverfassungsrecht" oben in § 4 Fn. 4.

[73] Insbes. § 5.

[74] Vgl. beispielhaft aus dem jüngeren Schrifttum die umfassenden Darstellungen zu heimlichen Maßnahmen bei *T. Schwabenbauer*, Heimliche Grundrechtseingriffe, 2013; *P. Hauck*, Heimliche Strafverfolgung und Schutz der Privatheit, 2014; *Bäcker*, Kriminalpräventionsrecht, 2015, S. 451 ff.; *D. Brodowski*, Verdeckte technische Überwachungsmaßnahmen, 2016; *M. Müller/T. Schwabenbauer*, Verfassungs-, unions- und konventionsrechtliche Vorgaben, in: Lisken/Denninger, HdbPolR, 7. Aufl. 2021, Kap. G I.

[75] Zu heimlichen Maßnahmen vgl. beispielhaft BVerfGE 133, 277 (328, Rn. 121); 141, 220 (264 f., Rn. 92); 150, 244 (283, Rn. 98); 155, 119 (178 f., Rn. 129); vgl. auch EuGH, C-203/15 v. 21.12.2016, Rn. 100 – Tele2 Sverige.

schiebungen von der Legislative hin zur Exekutive im Raum stehen, wird dieser Vorgang durchaus unter grundrechtlichen Gesichtspunkten thematisiert (Vorbehalt des Gesetzes).[76] In Feldern wie dem Recht der Nachrichtendienste oder auch allgemein bei der Regelung zur Erhebung und zum Austausch von personenbezogenen Daten durch und zwischen (Sicherheits-)Behörden hat jedoch mittlerweile infolge des hohen Maßes an Grundrechtsschutz und der daraus resultierenden umfassenden Befassungsnotwendigkeit des Gesetzgebers die Vergesetzlichung ein derart hohes Maß erreicht, dass sich eher die Frage stellt, ob nicht gerade der Zwang zur Befassung des Gesetzgebers Dysfunktionalitäten im demokratischen Prozess erzeugen kann.[77] Hinzu kommt, dass in bestimmten, stark technisch geprägten Bereichen des Sicherheitsrechts (im weiteren Sinne) gute Gründe dafür sprechen, den Gesetzgeber von Detailregelungen zu entlasten und das in der Exekutive gespeicherte oder von ihr leichter zu organisierende Fachwissen für das Recht zu nutzen.[78] Auf diesen Punkt wird noch ausführlich zurückzukommen sein.[79]

cc) Föderale Kompetenzverteilung

Schließlich kann die Kompetenzordnung auch durch die dem „neuen" Sicherheitsverständnis inhärente Tendenz zur Hochzonung herausgefordert werden. Das Konzept einer integrierten Regulierung, die den erwähnten „All-Gefahren-Ansatz" verfolgt, verlangt zwar keine Regulierung „aus einer Hand"; eine Hochzonung kann jedoch jene als schwerfällig und fehlerbehaftet geltenden föderalen Abstimmungsprozesse vermeiden und liegt daher durchaus in der Logik des Neuansatzes.[80] Allerdings lassen sich entsprechende Unitarisie-

[76] Hierzu *I. Katsarov*, Sicherheitsgesetzgebung zwischen Legislative und Exekutive, 2014; *A. Kapitza*, Entparlamentarisierung der Sicherheitsgesetzgebung, 2015; *C. Gusy/A. Kapitza*, Entparlamentarisierung der Sicherheitsgesetzgebung, in: Möllers/van Ooyen (Hrsg.), Jahrbuch Öffentliche Sicherheit 2014/2015, 2015, S. 367 ff.

[77] Zum notwendigen Maß an Bestimmtheit insbes. BVerfGE 100, 313 (359 f., Rn. 165; 372 f., Rn. 207 f.); 110, 33 (55 f., Rn. 111 ff.); 113, 348 (375 ff., Rn. 116 ff.); 118, 168 (186 ff., Rn. 93 ff.); 120, 274 (315 ff., Rn. 209 ff.); 120, 378 (407 f., Rn. 94); 125, 260 (328, Rn. 226 f.); 130, 151 (202, Rn. 169); 133, 277 (336 f., Rn. 140 f.). Zu den komplexeren Bestimmtheitsanforderungen bei heimlicher Datenverarbeitung jüngst BVerfGE 155, 119 (181, Rn. 133). Zur Notwendigkeit einer intensiven parlamentarischen Begleitung des gesamten Informationszyklus siehe nur BVerfGE 141, 220 (324, Rn. 277).

[78] Grundlegend BVerfGE 49, 89 (134 f.).

[79] Hierzu unten § 5 II. 2. b).

[80] Zur föderalen Organisation der Sicherheitsbehörden (im engeren Sinne) und deren Pathologien vgl. die instruktiven Darstellungen von *D. Kugelmann*, Polizei und Polizeirecht in der föderalen Ordnung des Grundgesetzes, in: Härtel (Hrsg.), Handbuch Föderalismus, Bd. III, 2012, § 52; *C. Gusy*, Organisation und Aufbau der deutschen Nachrichtendienste, in: Dietrich/Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017, Kap. IV § 1; *ders.*, Nachrichtendienste in der sicherheitsbehördlichen Kooperation, in: a. a. O., Kap. IV § 2; *M. Greßmann*, Nachrichtendienste und Strafverfolgung, in: a. a. O., Kap. IV

rungstendenzen seit jeher im Sicherheitsrecht diagnostizieren.[81] In jeder Krise wird nach stärkerer Zentralisierung gerufen.[82] Der Zug zum Zentrum ist also kein Spezifikum des „neuen" Sicherheitsrechts. Wo der für das föderale System des Grundgesetzes insgesamt charakteristische Unitarisierungs- und Verflechtungsdrang endet[83] und wo ein etwaiger Zentralisierungseffekt einer Politik der Versicherheitlichung beginnt, lässt sich daher nicht allgemein bestimmen. In Einzelkonstellationen kann allerdings durchaus der Versuch einer entsprechenden Einflussnahme beobachtet werden. Viel Beachtung gefunden haben insofern die bereits berichteten Bestrebungen des Bundes, unter Verweis auf Effizienzerwägungen und übergeordnete Sicherheitsinteressen das föderal „zersplitterte" Katastrophenschutzrecht an sich zu ziehen und mit dem in originärer Bundeskompetenz stehenden Zivilschutz zu verschmelzen.[84] Das

§ 3; *M. Bäcker*, Organisationsverfassungsrechtliche Grundlagen der Polizeiarbeit, in: Lisken/Denninger, HdbPolR, 7. Aufl. 2021, Kap. B III.; *U. Münch*, Wenn Terrorangst auf Bundesstaatlichkeit trifft, in: Pelizäus/Nieder (Hrsg.), Das Risiko, 2019, S. 271 ff.

[81] Hierzu etwa *H.-J. Lange*, Innere Sicherheit im Politischen System der Bundesrepublik Deutschland, 1999, S. 105 ff.; *A. Laschet*, Innere Sicherheit als Gemeinschaftsaufgabe für Bund, Länder und die Europäische Union, in: Jahrbuch des Föderalismus 2018, S. 21 ff.; *J. Riedl*, Entwicklungslinien der Politik Innerer Sicherheit in Deutschland, in: Jahrbuch des Föderalismus 2018, S. 37 ff.; *H. Hofmann*, Die bundesstaatliche Architektur der inneren Sicherheit, in: Jahrbuch des Föderalismus 2018, S. 51 ff.; *C. Binninger*, Das Nebeneinander von Bundes- und Landesbehörden in der Inneren Sicherheit, in: Jahrbuch des Föderalismus 2018, S. 88 ff.; *Löffelmann*, Die Zukunft der deutschen Sicherheitsarchitektur, GSZ 2018, S. 85 ff. Stellvertretend für das Verfassungsschutzrecht *R. Frauenrath*, Die Verfassungsschutzbehörden im Gefüge der deutschen Sicherheitsarchitektur, in: Lange/Wendekamm (Hrsg.), Die Verwaltung der Sicherheit, 2019, S. 155 ff.; *K. F. Gärditz*, Zentralisierung von Verfassungsschutzaufgaben und bundesstaatliche Kompetenzarchitektur, AöR 144 (2019), S. 81 ff.; *T. Wischmeyer*, Der Verfassungsschutzverbund, in: Dietrich/Gärditz et al. (Hrsg.), Nachrichtendienste in vernetzter Sicherheitsarchitektur, 2020, S. 35 ff.

[82] *J. Riedl*, Innere Sicherheit in Wahlkampfzeiten, in: Jahrbuch des Föderalismus 2017, S. 221 ff., unter Verweis auf entsprechende Analysen für die USA bei *T. Birkland*, After Disaster, 1997.

[83] Zu den dafür verantwortlichen Faktoren und den allgemeinen Zentralisierungstendenzen siehe aus der Literatur nur stellvertretend *G. Lehmbruch*, Der unitarische Bundesstaat in Deutschland, in: Benz/Lehmbruch (Hrsg.), Föderalismus. PVS Sonderheft 32, 2002, S. 53 ff.; *D. Hanschel*, Konfliktlösung im Bundesstaat, 2012, S. 84 ff.; *P. M. Huber*, Der ungeliebte Bundesstaat, NVwZ 2019, S. 665 ff. Zu dem in den 1970er-Jahren etablierten „Verflechtungsbegriff" grundlegend *F. Scharpf/B. Reissert/F. Schnabel*, Politikverflechtung, 1976, S. 28 ff.; zusammenfassend: *F. Scharpf*, Optionen des Föderalismus in Deutschland und Europa, 1994, S. 15 ff. Allgemein zur bundesstaatlichen Problematik auch *P. Lerche*, Föderalismus als nationales Ordnungsprinzip, in: VVDStRL 21 (1964), S. 66 ff.; *K. Hesse*, Der unitarische Bundesstaat, 1962; *ders.*, Aspekte des kooperativen Föderalismus in der Bundesrepublik, in: Ritterspach/Geiger (Hrsg.), FS G. Müller, 1970, S. 141 ff.; *M. Jestaedt*, Bundesstaat als Verfassungsprinzip, in: Isensee/Kirchhof (Hrsg.), HStR, Bd. II, 3. Aufl. 2004, § 29; *J. Isensee*, Idee und Gestalt des Föderalismus im Grundgesetz, in: Isensee/Kirchhof (Hrsg.), HStR, Bd. VI, 3. Aufl. 2008, § 126.

[84] Dazu bereits oben § 4 I. 2. d). Vertiefend *A. Musil/S. Kirchner*, Katastrophenschutz im föderalen Staat, DV 39 (2006), S. 373 ff.; Lange/Gusy (Hrsg.), Kooperation im Katastrophen- und Bevölkerungsschutz, 2015.

Beispiel zeigt zugleich, dass die Zählebigkeit der föderalen Strukturen nicht unterschätzt werden darf. Denn hier – wie auch sonst in vielen Fällen[85] – sind die Zentralisierungspläne letztlich im Gefüge des föderalen Systems versandet. Versuche zur Änderung der grundgesetzlichen Kompetenzordnung blieben jedenfalls bislang ohne Erfolg.[86] Und das neu gefasste Gesetz über den Zivilschutz und die Katastrophenhilfe des Bundes (ZSKG) dehnt zwar an einzelnen Punkten das grundgesetzliche Kompetenzregime, bricht jedoch aus dessen Korsett nicht aus.[87] Auch im Recht der kritischen Infrastrukturen ist der grundgesetzliche Kompetenzrahmen bisher stabil.[88] So folgt das bundesrechtliche Regime relativ punktgenau den vorhandenen sektorspezifischen Kompetenztiteln.[89] Der Begriff der kritischen Infrastruktur im Bundesrecht wird daher ganz entscheidend durch die grundgesetzliche Kompetenzordnung geprägt – nicht umgekehrt.

Doch selbst wenn das „neue" Sicherheitsrecht effektiv zur Zentralisierung beitrüge, stellt sich die Frage, ob die Auswirkungen auf die Verfassung nicht eher peripherer Natur wären. In der staatsrechtlichen Literatur ist die freiheitsschützende Qualität des Föderalismus („vertikale Gewaltenteilung") zwar ein etabliertes Argument. Gerade im sicherheitsbehördlichen Kontext wird aus den negativen historischen Erfahrungen mit zentralisierter Polizeigewalt auf die die freiheitssichernde Funktion einer auf Bund und Länder verteilten Organisation der Sicherheitsbehörden geschlossen.[90] Gleichzeitig lässt

---

[85] Entsprechend zum Verfassungsschutzrecht *Wischmeyer*, Der Verfassungsschutzverbund, in: Dietrich/Gärditz et al. (Hrsg.), Nachrichtendienste in vernetzter Sicherheitsarchitektur, 2020, S. 35 (38).

[86] *Kloepfer/Walus/Deye/Schärdel*, Handbuch des Katastrophenrechts, 2015, S. 75; *Meyer-Teschendorf*, Fortentwicklung der Rechtsgrundlagen für den Bevölkerungsschutz, DVBl. 2009, S. 1221 (1227 ff.). Zur jüngsten Diskussion um eine Reform des Bevölkerungsschutzes, siehe *H. Bubrowski*, Katastrophenschutz stärken, Streit vermeiden, F.A.Z., 5.7.2022.

[87] *Kloepfer/Walus/Deye/Schärdel*, Handbuch des Katastrophenrechts, 2015, S. 75 f.; *Pohlmann*, Bundeskompetenzen im Bevölkerungsschutz, in: Lange/Endreß/Wendekamm (Hrsg.), Versicherheitlichung des Bevölkerungsschutzes, 2013, S. 249 (255 f.); *Thiele*, Zivile Sicherheit im Katastrophenrecht, in: Gusy/Kugelmann/Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, 2017, S. 539 (550 ff.).

[88] Dazu näher *Möllers/Pflug*, Verfassungsrechtliche Rahmenbedingungen des Schutzes kritischer IT-Infrastrukturen, in: Kloepfer (Hrsg.), Schutz kritischer Infrastrukturen, 2010, S. 47 (53 f.).

[89] Einschlägige spezielle Kompetenztitel, auf die sich das IT-SiG 2015 gestützt hat, sind Art. 73 Abs. 1 Nr. 6 GG (Luftverkehr); Art. 73 Abs. 1 Nr. 6a, Art. 74 Abs. 1 Nr. 23 GG (Eisenbahnen); Art. 74 Abs. 1 Nr. 21 GG (Schifffahrt); Art. 74 Abs. 1 Nr. 19 GG (Gesundheit); Art. 73 Abs. 1 Nr. 7 GG (Telekommunikation). Spielräume öffnet vor allem der traditionell weit verstandene Kompetenztitel für das Recht der Wirtschaft (Art. 74 Abs. 1 Nr. 11 GG). Weiter dazu unten § 5 III. 1. a).

[90] Zu letzterer vgl. nur BVerfGE 133, 277 (323). Allgemein zum Argument vgl. *Gärditz*, in: Bonner Kommentar, 4/2018, Vorbemerkungen zu Art. 83 ff. GG, Rn. 31, 161, 171 ff. m. w. N.

sich jedoch in der Praxis beobachten, dass „Nepotismus, Ämterpatronage und stabile Interessengeflechte" – also die Übel übermäßiger Machtkonzentration – „in kleineren, homogeneren politischen Räumen mitunter besonders gut gedeihen".[91] Es sind daher oftmals weniger prinzipielle als praktische Gründe, die ein Festhalten an den föderalen Strukturen als sinnvoll erscheinen lassen. Denn dass gerade im Falle der Verwaltungskompetenzen eine Zentralisierung stets mit Effektivitätsgewinnen einhergeht, dass etwa der Informationsfluss in einer zentral dem Bund unterstehenden Verwaltungseinheit besser funktioniert als im föderalen Informationsverbund, wird mit guten Gründen in Frage gestellt.[92]

4. Zwischenfazit

Grundrechte, Gewaltenteilung und föderale Grundstruktur werden durch das neue „Sicherheitsdispositiv" herausgefordert, erweisen sich jedoch bisher als durchaus widerständig. Bei allen Pathologien, die der gegenwärtigen Sicherheitsgesetzgebung in verlässlichem Turnus aus Karlsruhe, Straßburg und Luxemburg attestiert werden, und bei allen Verzerrungen, die den von der Innenansicht der Sicherheitsbehörden dominierten, alternative und zivilgesellschaftliche Stimmen marginalisierenden sicherheitspolitischen Diskurs prägen,[93] erscheint es übersteigert, Sicherheitsbegriff und Ausnahmezustand in eins zu setzen, um „Sicherheit, Prävention und Ausnahmezustand übereinstimmende, tendenziell totalitäre Züge" zu attestieren.[94]

Stattdessen gilt es auch mit Blick auf die in der politischen Philosophie ebenso wie in der Verfassungsdogmatik konservierte Einsicht, dass auf die Sicherheitsgewährleistung durch den Staat ein Anspruch besteht, der in der Verwundbarkeit der isolierten Individuen seinen Ursprung hat,[95] die Tätigkeiten

[91] *Gärditz*, in: Bonner Kommentar, 4/2018, Vorbemerkungen zu Art. 83 ff. GG, Rn. 174.

[92] Dazu näher *Gusy*, Nachrichtendienste in der sicherheitsbehördlichen Kooperation, in: Dietrich/Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017, Kap. IV § 2 Rn. 5; *Wischmeyer*, Der Verfassungsschutzverbund, in: Dietrich/Gärditz et al. (Hrsg.), Nachrichtendienste in vernetzter Sicherheitsarchitektur, 2020, S. 35 (45).

[93] Offen hierzu *Gusy*, Sicherheitsrecht als Rechtsgebiet?, in: Dietrich/Gärditz (Hrsg.), FS Graulich, 2019, S. 9 (22).

[94] So aber *Barczak*, Der nervöse Staat, 2. Aufl. 2021, S. 371. Vgl. auch a. a. O., S. 362: „Aus dem Belagerungszustand der konstitutionellen Epoche ist im Zeitalter der vorsorgenden Sicherheitsgesellschaft ein Ausnahmezustand im Sinne einer Technik des Zuvorkommens geworden".

[95] Auch hierzu treffend die Formulierung bei *Folkers*, Das Sicherheitsdispositiv der Resilienz, 2018, S. 10: „Sicherheit ist nicht nur eine Ablenkungsstrategie von Regierenden, […] sondern fundamentaler Anspruch eines Lebens, dessen grundlegende Eigenschaft darin liegt, verwundbar und deshalb schutzbedürftig zu sein […]. Wer das nicht wahrhaben will […], reproduziert damit nur eine fatale Vorstellung politischer Subjektivität, die vollkommen bedürfnislos und autonom die politische Sphäre betritt, und lässt zudem die Ansprüche und

des vorsorgenden Staates in seiner Ambivalenz zu würdigen. Damit soll nicht einer beliebigen Vorverlagerung der staatlichen Eingriffsmacht das Wort geredet werden. Vielmehr gilt es, einen differenzierten Blick auf die von der Sicherheitspolitik adressierten Bereiche zu werfen. Gerade dort, wo diese „neues" Terrain betritt, etwa auf dem Feld der Informationssicherheit, lassen sich gute Gründe für einen vorsorgenden Zugriff finden – die damit verbundenen Probleme dürfen nicht ignoriert, sondern müssen identifiziert und rechtsstaatlich eingehegt werden.

II. Versicherheitlichungstendenzen im Cyberraum

1. Der Informationssicherheitsdiskurs als illiberale Diskursverschiebung?

a) Entgrenzter Begriff und entgrenzter Diskurs

Wenn, wie erwähnt, der Informationssicherheits*diskurs* als Beleg für die These einer illiberalen Diskursverschiebung herangezogen wird, stützt sich dieses Urteil auf eine Reihe von Beobachtungen.[96]

Verweisen lässt sich *erstens* darauf, dass in Wissenschaft und Gesellschaft Szenarien der Daseinsvorsorge, der konventionellen Gefahrenabwehr, der technischen Sicherheit, der Strafverfolgung, der nachrichtendienstlichen Aufklärung und des (Kriegs-)Völkerrechts oft gleichermaßen pauschal dem Phänomenbereich „Cybersicherheit" zugeordnet werden.[97] Dies beeinflusst auch die politische Programmsetzung. So stehen etwa in den deutschen Cybersicherheitsstrategien von 2016 und 2021 als Handlungsfelder die Einführung von Gütesiegeln für IT-Sicherheit zwanglos neben der Abwehr von Cyberspionage, dem Auftrag zur Weiterentwicklung der Cyber-Verteidigungspolitik der Nato und dem Cyber Capacity Building der Bundeswehr.[98] Entsprechend weit wird allgemein auch der Begriff des Cyber*angriffs* („cyberattack") gebraucht; gemeint sind damit typischerweise alle möglichen auf IT-Systeme

Motivlagen faktisch handelnder politischer Subjekte außer Acht. Aber gerade weil Sicherheit ein so grundlegendes Bedürfnis des prekären Lebens ist, ist sie auch gefährlich. Das Verlangen nach Sicherheit lässt sich nämlich auf vielfältige Weise missbrauchen und ausbeuten."

[96] Beispielhaft *H. Nissenbaum*, Security, Ethics and Information Technology 7 (2005), S. 61 ff.; *M. Dunn Cavelty*, Cyber-Security and Threat Politics, 2008; *L. Hansen/H. Nissenbaum*, Digital Disaster, International Studies Quarterly 53 (2009), S. 1155 ff.; *D. Delaney*, Cybersecurity, Journal of Legislation 40 (2013–2014), S. 251 ff.

[97] Vgl. in diesem Sinne nur die populären Überblicksdarstellung bei *P. Singer/A. Friedman*, Cybersecurity and Cyberwar, 2014; *R. Baecker*, Computers and Society, 2019, S. 187 ff.

[98] *BMI*, Cyber-Sicherheitsstrategie für Deutschland, 2016; *BMI*, Cybersicherheitsstrategie, 2021. Etwas fokussierter nunmehr *BMI*, Cybersicherheitsagenda, 2022.

und Netzwerke bezogenen Schädigungshandlungen, also nicht nur die im Völker- und Verfassungsrecht definierten Fälle eines militärischen „Angriffs" (vgl. Art. 26 Abs. 1 GG; Art. 39 UN Charta).[99] Dieser Sprachgebrauch indiziert, dass sich die Kartierung des Problems nicht an völker- und verfassungsrechtlichen Kategorien orientiert. Der Begriff der Informationssicherheit selbst leistet hier keinen Widerstand. So lautet die zur Beschreibung der „Security Architecture" von IT-Systemen entwickelte Standarddefinition der International Telecommunication Union (ITU): „The term security is used in the sense of minimizing the vulnerabilities of assets and resources. An asset is anything of value. A vulnerability is any weakness that could be exploited to violate a system or the information it contains. A threat is a potential violation of security. […] Threats can be classified as accidental or intentional and may be active or passive."[100] Wenn aber Informationssicherheit schlicht die Abwesenheit von Unsicherheit ist, sind alle Arten von Mitteln erforderlich, um einen hinreichend sicheren Zustand herzustellen.[101] Dies kann für eine Diskursverschiebung von Freiheit zur Sicherheit ausgenutzt werden.

Zweitens, so die Kritik, ist der Diskurs um Cybersicherheit durch eine starke „Überdeterminierung" der Thematik geprägt, die in Verbindung mit einer „ständigen Mobilisierung von ‚Worst Case'-Szenarien" letztlich einer Militarisierung von Cyberfragen Vorschub leistet.[102] Verweisen kann diese Kritik darauf, dass jedenfalls bis Mitte der 2010er-Jahre eine klare Diskrepanz zwischen der unter dem Stichwort „cyber war" beschworenen Gefahrenlage einerseits, die einen erheblichen Aufwuchs der militärischen und nachrichtendienstlichen Kapazitäten zu rechtfertigen half, und den tatsächlich eingetretenen Schäden andererseits, die nur minimal waren, herrschte.[103]

---

[99] Paradigmatisch *K. Eichensehr*, The Law and Politics of Cyberattack Attribution, UCLA L. Rev. 67 (2020), S. 520 (522 mit Fn. 1).

[100] *ITU*, Security Architecture for Open Systems Interconnection for CCITT Applications. Recommendation X.800, 1991, A.2.1. und A.2.4.

[101] Dazu vertiefend und spezifischer zur IT-Sicherheit unten § 6 II.

[102] *M. Dunn Cavelty*, Die materiellen Ursachen des Cyberkriegs, Journal of Self-Regulation and Regulation 1 (2015), S. 167 (175). Diese *cyber doom*-Szenarien, die bis in die frühen 1990er-Jahre zurückreichen (vgl. J. Arquilla/D. Ronfeldt [Hrsg.], In Athena's Camp, 1997; *G. Rattray*, Strategic Warfare in Cyberspace, 2001), werden instruktiv kontextualisiert bei *Stevens*, Cybersecurity and the Politics of Time, 2016, S. 95 ff. Andere Akzentsetzung jetzt allerdings bei *Dunn Cavelty/Wenger*, Cyber Security Meets Security Politics, Contemporary Security Policy 41:1 (2020), S. 5 (16, 21). Vgl. auch die knappe und nüchterne völkerrechtliche Bestandsaufnahme bei *Walter*, Cyber Security als Herausforderung für das Völkerrecht, JZ 70 (2015), S. 685 (686).

[103] Siehe bereits *T. Rid*, Cyber War Will Not Take Place, Journal of Strategic Studies 35:1 (2012), S. 5 ff. Eine nuancierte empirische Studie zum Zeitraum von 2001 bis 2011 findet sich bei *B. Valeriano/R. Maness*, Cyber War versus Cyber Realities, 2015, die strukturelle Gründe dafür anführen, dass sich im zwischenstaatlichen Verhältnis Zurückhaltung („cyber restraint") durchsetzen wird: „Our theory of cyber restraint depends on four processes: (1) the nature of the weapon and its reproducibility, making it a one-shot weapon of limited ef-

Drittens ist gut dokumentiert, dass in diversen internationalen Foren illiberale Akteure den offenen Begriff der Informationssicherheit strategisch nutzen, um unter Verweis auf Informationssicherheitsinteressen Grundstandards der offenen Internetkommunikation auszuhebeln.[104]

b) Zur Rolle des Militärs und der Nachrichtendienste im Bereich der Informationssicherheitsgewährleistung

Es ist aber nicht allein diese semantisch-diskursive Ebene, aus der sich das Misstrauen gegen staatliche Aktivitäten im Bereich der Informationssicherheit speist. Hingewiesen wird ferner darauf, dass auf Seiten des Staates bei der Entwicklung der vernetzten Informationstechnik im Allgemeinen und von Informationssicherheitstechnologien im Besonderen gerade das Militär und die Nachrichtendienste eine entscheidende Rolle gespielt haben.[105] Diese Instanzen gaben auch wichtige Anstöße für Forschung und Entwicklung im Bereich IT-Sicherheit und beteiligten sich intensiv an der dortigen Standardsetzung.[106]

---

fectiveness; (2) the potential for blowback, given that initiating states are often weaker than the state they seek to infiltrate; (3) the natural potential of collateral damage in cyberspace since the technology is not limited to military space; and (4) the potential harm to civilians due to these considerations." (a. a. O., S. 4 f.). Ein Plädoyer für eine bessere empirische Validierung bei *B. Valeriano/R. Maness*, How We Stopped Worrying about Cyber Doom and Started Collecting Data, Politics and Governance 6:2 (2018), S. 49 ff.

[104] Zu den Bestrebungen Russlands und anderer Staaten, im Rahmen der World Conference on International Telecommunications (WCIT) der International Telecommunications Union (ITU) 2012 über das Argument „Cybersecurity" Einfluss auf die Standards der Internetkommunikation zu nehmen, näher *C. Glen*, Internet Governance: Territorializing Cyberspace?, Politics & Policy 42 (2014), S. 635 ff.; *L. Kello*, Cyber Threats, in: Weiss/Daws (Hrsg.), The Oxford Handbook on the United Nations, 2. Aufl. 2018, S. 528 (563 ff.). Siehe weiter nur *A. Biselli*, „Ende des freien Internets in seiner bisherigen Form", Netzpolitik.org, 12.3.2015.

[105] Siehe dazu allgemein *P. Edwards*, The Closed World, 1996; *P. Mirowski*, Machine Dreams, 2002; *Y. Levine*, Surveillance Valley, 2018. Zur Frühgeschichte *P. Kidwell*, The Role of Governments in the Spread of Novel Computing Devices in the Nineteenth and Early Twentieth Century United States, IEEEA 41:1 (2019), S. 7 ff. Spezifisch zur (Militär-)Geschichte des Internets siehe unten § 6 Fn. 63. Zur Regulierungsgeschichte des Internets im Überblick *Kettemann*, The Normative Order of the Internet, 2020, S. 107 ff. Als instruktive Parallelgeschichte *Peters*, How Not to Network a Nation. The Uneasy History of the Soviet Internet, 2016. Vgl. bereits allgemein zum Verhältnis von Technologieentwicklung und Sicherheitspolitik oben in § 3 Fn. 6.

[106] Zur Beteiligung staatlicher Stellen, insbesondere der NSA und des US-Militärs, an der Entwicklung von IT-Sicherheitstechnologien und IT-Sicherheitsstandards siehe *J. Yost*, History of Computer Security Standards, in: Leeuw/Bergstra (Hrsg.), The History of Information Security, 2007, S. 595 ff.; *M Warner*, Cybersecurity: A Pre-history, Intelligence and National Security 27:5 (2012), S. 781 ff.; *ders.*, Notes on the Evolution of Computer Security Policy in the US Government, 1965–2003, IEEEA 37:3 (2015), S. 8 ff.; *S. Lipner*, The Birth and Death of the Orange Book, IEEEA 37:2 (2015), S. 19 ff.; *J. Yost*, The Origin and Early History of the Computer Security Software Products Industry, IEEEA 37:2 (2015), S. 46 ff.; *Stevens*, Cybersecurity and the Politics of Time, 2016, S. 4 ff.

Auch heute noch sind Militär und Nachrichtendienste wesentliche Akteure beim Ausbau der staatlichen Aktivitäten im Bereich Cybersicherheit.[107] In der Literatur werden die Nachrichtendienste teilweise sogar als diejenigen Instanzen charakterisiert, die *de facto* den stärksten Impuls zur Normsetzung im Bereich IT-Sicherheit geben.[108] Und in der Praxis lässt sich an der deutschen IT-Sicherheitsgesetzgebung gut beobachten, dass ein Ausbau der „zivilen" IT-Sicherheit regelmäßig mit signifikanten Budgeterhöhungen und Kompetenzzuwächsen der Sicherheitsbehörden einhergeht.[109]

Die Brisanz dieses Einwands erhöht sich nochmals, wenn man mit der populären These vom „Überwachungskapitalismus" eine symbiotische Beziehung von multinationalen Unternehmen und staatlichen Sicherheitsakteuren, insbesondere den Nachrichtendiensten, diagnostiziert, wobei Letztere ihr Wohlwollen gegen den umfassenden Zugriff auf die privaten Datensammlungen der Unternehmen eintauschten.[110] Tatsächlich ist der Bereich Informationssicherheit von einer intensiven Kooperation zwischen staatlichen und privaten Akteuren geprägt. Sogar in operativen Belangen arbeiten staatliche und private Stellen in Gestalt von Computer Emergency Response Teams (CERTs)[111]

[107] *Dunn Cavelty*, Die materiellen Ursachen des Cyberkriegs, Journal of Self-Regulation and Regulation 1 (2015), S. 167 (172).

[108] *I. Georgieva*, The Unexpected Norm-Setters, Contemporary Security Policy 41:1 (2020), S. 33 ff.

[109] Hierzu für das IT-SiG 2015 näher *Wischmeyer*, Informationssicherheitsrecht, DV 50 (2017), S. 155 (180).

[110] Allgemein *S. Zuboff*, The Age of Surveillance Capitalism, 2019. Paradigmatischer Fall ist die sog. „Vorratsdatenspeicherung", die die privaten Telekommunikationsanbieter zur anlasslosen Speicherung der bei ihnen anfallenden Telekommunikationsverkehrsdaten verpflichtet und die Behörden unter bestimmten Bedingungen zum Abruf dieser Daten ermächtigt. Gerade hier ist die gerichtliche Kontrolle jedoch extrem engmaschig, vgl. aus der jüngeren Rechtsprechung EuGH, C- 511/18 u. a. v. 6.10.2020, Rn. 87 ff. – La Quadrature du Net; EuGH, C-623/17 v. 6.10.2020, Rn. 30 ff. – Privacy International; EuGH, C-746/18 v. 2.3.2021, Rn. 30 ff. – H. K./Prokuratuur; EuGH, C-140/20 v. 5.4.2022, Rn. 31 ff. – G.D.; EuGH, C-793/19 u. a. v. 20.9.2022, Rn. 47 ff. – SpaceNet.

[111] CERTs oder auch Computer Security Incident Response Teams (CSIRTs) sind seit Ende der 1980er-Jahre eine international etablierte Organisationsform zum Umgang mit IT-Sicherheitsvorfällen. Instruktiv dazu bereits *D. Fox*, CERT, DuD 2002, S. 493 ff. Zahlreiche öffentliche und private Organisationen – Behörden, Unternehmen, Hochschulen etc. – betreiben innerhalb ihres Verantwortungsbereichs entsprechende Teams, die zugleich über nationale, europäische und internationale CERT-Verbünde miteinander vernetzt sind. Zum beim BSI angesiedelten CERT-Bund siehe https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html. Zum bei der Europäischen Kommission angesiedelten CERT-EU vgl. die Interinstitutionelle Vereinbarung über die Organisation und die Funktionsweise eines IT-Notfallteams für die Organe, Einrichtungen und sonstigen Stellen der Union (CERT-EU) v. 20.12.2017, ABl. 2018 C 12/1 (vgl. insbes. Art. 5 zur Zusammenarbeit des CERT-EU mit Privaten).

Hand in Hand. Insgesamt teilen staatliche Stellen und Private ein Interesse an möglichst umfassender Datenspeicherung.[112]

Bedenkt man schließlich, dass Informationssicherheit als Element von „Cyberpower" für die Außen- und Sicherheitspolitik heute eine zentrale Bedeutung gewonnen hat und zu einem wichtigen Faktor in jenem Ringen zwischen Staaten und Blöcken um Dominanz im Cyberraum geworden ist,[113] wird klar, dass die Militarisierung und Vernachrichtendienstlichung des Informationssicherheitsproblems kein zufälliges Ereignis ist, sondern dem hohen strategischen Interesse staatlicher Stellen an der Materie entspricht.[114]

c) Digitale Technik als „Ideologie"

Neben der entgrenzenden Rhetorik und der intensiven Befassung von Militär und Nachrichtendiensten mit Informationssicherheit stützt sich die Versicherheitlichungsthese schließlich auch auf den „ideologischen" Charakter der digitalen Technik. Die These, Technologie sei nicht nur als Mittel für Repressionszwecke nutzbar, sondern habe eine ihr eigene Affinität zur Herrschaftsstabilisierung und zur Unfreiheit ist aus der älteren Technikkritik bekannt, wird heute aber regelmäßig auch auf digitale Technologien angewendet.[115] Das von *Herbert Marcuse* früh entwickelte Argument bringt diese Position immer noch präzise auf den Punkt:

„For the concept of technical reason is itself perhaps ideology. Not merely its application, but technique itself is domination […]. The aims and interests of domination are not 'additional' or dictated to technique from above – they enter into the construction of the technical apparatus itself. For technique is a social and historical project: into it

[112] Dazu *R. Deibert*, Trajectories for Future Cybersecurity Research, in: Gheciu/Wohlforth (Hrsg.), The Oxford Handbook of International Security, 2018, S. 531 („Cybersecurity is also characterized by a unique convergence of national security and business interests around surveillance"); *D. Avant/V. Haufler*, Public–Private Interactions and Practices of Security, in: Gheciu/Wohlforth (Hrsg.), The Oxford Handbook of International Security, 2018, S. 350 (360). Allgemein zur engen Beziehung zwischen öffentlichem und privatem Sektor im Bereich Cybersecurity *K. Eichensehr*, Public-Private Cybersecurity, Tex. L. Rev. 95:3 (2016–2017), S. 467 ff.; *N. Sales*, Privatizing Cybersecurity, UCLA L. Rev. Discourse 65 (2018), S. 620 ff.

[113] Dazu bereits oben § 1 Fn. 57 und 58.

[114] Zu dieser Diskussion M. Dunn Cavelty/V. Mauer/S. Krishna-Hensel (Hrsg.), Power and Security, 2007; *D. Betz/T. Stevens*, Cyberspace and the State, 2011; *Dunn Cavelty*, Die materiellen Ursachen des Cyberkriegs, Journal of Self-Regulation and Regulation 1 (2015), S. 167 ff.; *M. Mueller*, Souveränität im Cyberspace?, Journal of Self-Regulation and Regulation 1 (2015), S. 65 ff. Für Europa: *Kello*, Cyber Defence, in: Meijer/Wyss (Hrsg.), The Handbook of European Defence Policies and Armed Forces, 2018, S. 658 (664 ff.).

[115] Einflussreich: *E. Morozov*, The Net Delusion: The Dark Side of Internet Freedom, 2011; *R. MacKinnon*, Consent of the Networked, 2012; *Hildebrandt*, Smart Technologies and the End(s) of Law, 2016; *Zuboff*, The Age of Surveillance Capitalism, 2019.

is projected what a society and its ruling interests decide to make of man and things. The aims of domination are 'substantive', and belong to the form of technical reason itself."[116]

Unterstellt wird hier also, dass der zu beobachtende Zusammenhang zwischen der staatlichen Einflussnahme auf (digitale) Technik und staatlicher Repression[117] im „Projekt" der Technik selbst wurzelt. Auch und gerade technische und politische Gewährleistung von Informationssicherheit kann sich dem dann nicht entziehen.

d) Kritische Würdigung

Die hier präsentierten Argumentationsansätze stützen sich auf einzelne plausible Beobachtungen. Sie bleiben allerdings den Nachweis schuldig, dass staatliche Bemühungen um Informationssicherheit *strukturell* illiberalen Grenzverschiebungen Vorschub leisten. Es trifft zwar zu, dass der teleologische Begriff der Informationssicherheit die vor allem im internationalen Raum beobachtbaren Tendenzen, mit seiner Hilfe illiberale Politik zu machen, begünstigen kann. Zusammen mit der für den Diskurs charakteristischen Neigung zur Übertreibung („cyber doom") rechtfertigt dies durchaus, staatlichen Initiativen mit einem gewissen Misstrauen zu begegnen. Auch ist die starke Militarisierung der Informationssicherheitsfrage in der gegenwärtigen Politik Tatsache. Ob dies eine generelle Skepsis an allen staatlichen Aktivitäten in diesem Bereich rechtfertigt, kann jedoch nicht geklärt werden, ohne vorher die Gründe zu analysieren, die für einen „All-Gefahren-Ansatz" im Sinne des „neuen" Sicherheitsrechts im Umgang mit Informationssicherheitsrisiken sprechen.

2. Zur Notwendigkeit eines „All-Gefahren-Ansatzes" im Cyberraum

Gezeigt werden soll im Folgenden, dass die weite Fassung, die der Begriff der Informationssicherheit in den relevanten technischen Normen erfahren hat, und die darauf reagierenden regulatorischen Strategien, die dem Themenfeld ein breites Spektrum an Instrumenten zuordnen, das vom Produktsicherheitsrecht bis zur militärischen Cyberkapazität reicht, jedenfalls nicht nur als Ablenkungsstrategien zur Bemäntelung illiberaler Politik oder als Modus zur Konstruktion von Unsicherheitsgefühlen verstanden werden dürfen. Viel-

[116] *H. Marcuse*, Industrialization and Capitalism, New Left Review (1965), S. 3 (16). Für eine instruktive Kritik daran siehe den gleichnamigen Beitrag in *J. Habermas*, Technik und Wissenschaft als „Ideologie" (1968), 1989, S. 48 ff.

[117] Dazu mit Details *S. Feldstein*, The Rise of Digital Repression, 2021. Siehe auch eindrucksvoll am Beispiel Chinas *S. Ringen*, The Perfect Dictatorship, 2016.

mehr ist dieser umfassende Ansatz grundsätzlich angemessen im Lichte des realen und drängenden Problems, wie die Sicherheit der komplexen, weitgehend anonymen, inhärent globalen und intensiv miteinander vernetzten Informationstechnologie gewährleistet werden kann. Ob und inwieweit die konkreten Maßnahmen zur Umsetzung dieses Ansatzes den rechtlichen Maßstäben gerecht werden, ist dann in den folgenden Kapiteln der Arbeit im Detail zu entfalten.

a) Komplexität der Problemlage

Die Komplexität der Lage lässt sich bereits an der Zahl, Art und den Interessen der aktiv involvierten Akteure vor Augen führen.[118] Als potenzielle *Gefährder* begegnen im Cyberraum unter anderem: Staaten und deren „Proxies"[119]; private, vom Staat unterstützte oder tolerierte Gruppen; terroristische oder kriminelle Gruppierungen; herkömmliche Unternehmen, die Wirtschaftsspionage für sich nutzen wollen; individuelle Hacker, die durch alle möglichen Motive getrieben werden. Nicht nur, aber gerade auch im Bereich der Informationssicherheit ist die Trennung von staatlichen und privaten Gefährdern überaus brüchig geworden. Es gilt, dass „the relationship between non-state actors and states often resembles a networked relationship where non-state actors complement state policies and goals materially, functionally or ideologically".[120] Gleiches gilt, wenn man untersucht, wer einen notwendigen *Beitrag* zur Gefährdung leistet. Dies sind nicht nur jene, die Angriffe durchführen; vielmehr nutzen Angreifer regelmäßig öffentliche oder private Dienste oder Infrastrukturen, die teils Schwachstellen aufweisen, teils aber auch dem Stand der Technik entsprechen, mit oder ohne Wissen der auf diese Weise Involvierten. So bedienen sich Angreifer oft der in Drittländern belegenen Netzinfrastrukturen und der Computersysteme unbeteiligter privater Dritter. Auch das *Interesse* der Angreifer kann differieren und reicht von Angriffen, die auf Schädigung der betroffenen IT-Systeme oder sonstiger, davon abhängiger Güter aus sind, über den Willen zur Ausspähung vertraulicher Daten bis hin zum

---

[118] Die folgende Aufschlüsselung folgt *Bannelier/Christakis*, Cyber-Attacks – Prevention-Reactions, 2017, S. 11. Zu den passiv, also auf Seite der Verteidiger, Involvierten siehe unten § 6 II. 4.

[119] Verstanden hier im Sinne von Art. 8 der „Articles on Responsibility of States for Internationally Wrongful Acts" der International Law Commission (ILC) von 2001: „The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct." Umfassend zur Problematik *T. Maurer*, Cyber Mercenaries, 2018.

[120] So treffend *N. Tsagourias/M. Farrell*, Cyber Attribution, EJIL 31:3 (2020), S. 941 (962). Gleiches gilt auf der Seite der Abwehrenden, siehe oben § 4 Fn. 112.

idealistischen Bestreben, neue Schwachstellen aufzudecken.[121] Ähnlich divers ist das Bild der potenziellen *Opfer* entsprechender Gefährdungen: Auch hier können Staaten betroffen sein, in ihrer Gänze oder in Gestalt einzelner Behörden oder Verwaltungszweige; daneben sind selbstverständlich auch Unternehmen aus allen möglichen Sektoren und – teils als Kollateralschaden, teils aber auch als eigentliches Angriffsziel – Individuen betroffen.

b) Attributionsproblem

Allein hierdurch entsteht ein Gefährdungsspektrum, das mit den konventionellen Kategorien der Gefahrenabwehr kaum hinreichend erfasst werden kann. Hinzu kommt die bereits erwähnte Tatsache, dass sich der Ursprung von Cyberrisiken in vielen Fällen nicht klar zurechnen („attribuieren") lässt.[122] Dabei ist zu differenzieren: Weisen Produkte oder Dienste Schwachstellen auf, etwa Programmierfehler, ist es oftmals nicht schwierig, erste Ansprechpartner zu identifizieren und Verantwortlichkeiten zu benennen. Anders ist dies hingegen, wenn Dritte solche Schwachstellen für eigenes Handeln ausnutzen. Solchermaßen Verantwortliche können aufgrund der weitgehenden Anonymität, die das Internet ermöglicht, in aller Regel nicht oder nur unter sehr großen Schwierigkeiten ermittelt werden. Hier hat das Attributionsproblem seinen eigentlichen Sitz.[123] Allerdings ist zu beachten, dass auch dann, wenn ermittelt werden kann, wem die den konkreten Ausfall herbeiführenden Programme, Systeme oder Infrastrukturen zuzuordnen sind, nicht gesichert ist, dass diese nicht durch Vierte – die „eigentlichen" Angreifer – kompromittiert worden sind etc.

Das Fehlen klarer Identitätsverifizierungsmechanismen im Internet, die Komplexität und die rasche Entwicklung der Technologie und letztlich auch die begrenzten Ressourcen der zur Aufklärung berufenen Akteure ermöglichen daher den Verantwortlichen vielfach, ihr Handeln und ihre Angriffswege effektiv zu verschleiern. Bis heute bleibt auch nach intensiven Recherchen oft unklar, wem ein Angriff zugerechnet werden kann. Selbst dort, wo Indizien –

---

[121] Die Angriffsformen gehen ineinander über, vgl. *B. Schneier*, There's No Real Difference Between Online Espionage and Online Attack, The Atlantic, 6.3.2014. Im Übrigen ist die Motivationslage bei jeder Angriffsform komplex, vgl. *F. Egloff*, Intentions and Cyberterrorism, in: Cornish (Hrsg.), The Oxford Handbook of Cyber Security, 2021, S. 187 ff.

[122] Im Sinne der Differenzierung von *K. F. Gärditz*, Der digitalisierte Raum des Netzes als emergente Ordnung, Der Staat 54 (2015), S. 113 (117), handelt es sich bei der Frage, inwieweit im Netz einzelne Akteure für „emergente Eigenschaften" der von ihnen erzeugten Probleme verantwortlich gemacht werden können, in erster Linie um ein „praktisches" Zurechnungsproblem, nicht um eine „theoretische" Frage. Freilich hat das praktische Problem solche Ausmaße, dass sich die Frage nach einer theoretischen Neukonfiguration der Verantwortung geradezu aufdrängt. Dazu näher sogleich und unter § 6 II. 4.

[123] Als Einführung in den technischen Sachverhalt instruktiv *C. Guitton*, Inside the Enemy's Computer, 2017; *D. Tran*, The Law of Attribution, Yale J. L. & Tech. 20 (2017), S. 376 (386 ff.); sowie die Nachweise in den folgenden Fußnoten.

etwa: typische Verfahrensweisen (*tradecraft*), die genutzten physischen und virtuellen Infrastrukturen und Dienste (*infrastructure*), die Art der verwendeten Manipulation (*malware*), die aus den Schadensfolgen abzuleitende Absicht der Angreifer (*intent*) und sonstige Erkenntnisse (*external sources*)[124] – in eine konkrete Richtung deuten, kann kaum je sicher ausgeschlossen werden, dass die vermeintlichen Beweise nicht von den „echten" Angreifern konstruiert worden sind (*false flag*).[125] Hierauf haben in der Vergangenheit Länder wie Russland und Nordkorea verwiesen, wenn ihnen in der Öffentlichkeit die Verantwortung für Angriffe zugeschrieben wurde.[126]

In jüngerer Zeit hat die digitale Forensik, auch durch die umfassende Nutzung privaten Sachverstands,[127] zwar Fortschritte erzielt.[128] Gerade im Fall öffentlichkeitswirksamer Attacken werden daher mehr und mehr öffentliche Zuschreibungen vorgenommen.[129] Nach wie vor ist jedoch gerade bei kompe-

[124] So die an *Office of the Director of National Intelligence*, A Guide to Cyber Attribution, 14.9.2018, orientierte Zusammenfassung wichtiger Analysekategorien bei *Tsagourias/Farrell*, Cyber Attribution, EJIL 31:3 (2020), S. 941 (947 ff.), die a. a. O., S. 949, illustrativ schildern, auf welche Indizien IT-Forensiker hoffen müssen: „Forgetting, for example, to turn on a proxy or route through a particular virtual private network (VPN), selecting the wrong stored username or password from an autofill option on a web browser, typing a text string for name or payment information that is from another persona or real identity or using a proper (real) name in correspondence are all examples of simple, small mistakes that can reveal a true identity and/or permit investigators to make an association with a false identity. Mistakes are therefore critical in attribution determinations because they can reveal patterns and relationships."

[125] *F. Skopik/T. Pahi*, Under False Flag, Cybersecurity 3:1 (2020), S. 1 ff.

[126] Vgl. allgemein *M. Libicki*, Cyberdeterrence and Cyberwar, 2009, S. 44; Beispiele bei *Finnemore/Hollis*, Constructing Norms for Global Cybersecurity, AJIL 110 (2016), S. 425 (435 f.). Eine überzeugende Rekonstruktion der damit verbundenen strategischen Interessen mit Hilfe des Konzepts der „implausible deniability" bei *R. Cormac/R. Aldrich*, Grey is the New Black, International Affairs 94:3 (2018), S. 477 ff.

[127] Zur Rolle privaten Sachverstands für Attributionsermittlungen *Eichensehr*, Public-Private Cybersecurity, Tex. L. Rev. 95:3 (2016–2017), S. 467 (489 ff.); *Sales*, Privatizing Cybersecurity, UCLA L. Rev. Discourse 65 (2018), S. 620 ff.; *S. Romanosky/B. Boudreaux*, Private-Sector Attribution of Cyber Incidents, International Journal of Intelligence and CounterIntelligence 34 (2021), S. 463 ff. Zu den damit verbundenen Problemen allgemein *J. Maddocks*, Outsourcing of Governmental Functions in Contemporary Conflict, Va. J. Int'l L. 59 (2019), S. 47 ff.; *K. Eichensehr*, Decentralized Cyberattack Attribution, AJIL Unbound 113 (2019), S. 213 ff.; *dies.*, The Law and Politics of Cyberattack Attribution, UCLA L. Rev. 67 (2020), S. 520 (547 ff.). Aus der Praxis siehe etwa *D. Sanger/J. Barnes/N. Perlroth*, White House Weighs New Cybersecurity Approach After Failure to Detect Hacks, New York Times, 15.3.2021.

[128] Vgl. die Dokumentation unter https://www.cfr.org/cyber-operations/#Timeline.

[129] Dazu *M. Finnemore/D. Hollis*, Beyond Naming and Shaming, EJIL 31:3 (2020), S. 969 (970). Hierzu zählen etwa die Attacken auf den Deutschen Bundestag und auf das Democratic National Committee (DNC) sowie die Verbreitung der „WannaCry"- und der „NotPetya"-Ransomware. Vgl. etwa auch die in Anhang I zur Verordnung (EU) 2019/796 des Rates vom 17.5.2019 (dazu § 2 Fn. 29) aufgeführten und als Verantwortliche für bestimmte Angriffe ausgewiesenen Akteure.

tenten Angreifern der Zuschreibungsprozess überaus ressourcenintensiv. Regelmäßig sind nur Wahrscheinlichkeitsaussagen möglich.[130] Die erforderlichen Detailinformationen – verwendete IP-Adressen, Registrierungsinformationen für Domains oder sonstige von den Angreifern genutzte Infrastrukturen, Informationen über finanzielle Transaktionen etc. – sind zudem nur mit erheblichem Aufwand und oft nur unter Nutzung hoheitlicher Autorität, teils sogar nur mittels nachrichtendienstlicher Fähigkeiten zu erlangen. Auch ihre Interpretation verlangt hohe Expertise. Hinzu kommt, dass die Attribuierung selbstverständlich kein wertneutraler Prozess ist; vielmehr sind Ermittlung und Auswertung der Fakten stets durch Vorannahmen geprägt – gerade im Lichte der strategischen Relevanz der Frage bleibt daher Vorsicht im Umgang mit Attribuierungen geboten.[131]

Vor diesem Hintergrund erklärt sich, weshalb die Frage nach der Attribution zu einem Zentralproblem der Informationssicherheitsforschung geworden ist.[132] Ein Teil der Literatur widmet sich dabei den primär technischen Fragen der Verantwortungsermittlung.[133] Andere diskutieren intensiv über die politischen und rechtlichen Standards für die Zurechnung bzw. die Implikationen fehlender Zurechnungsmöglichkeiten.[134] Die rechtliche Debatte ist be-

[130] *T. Rid/B. Buchanan*, Attributing Cyber Attacks, Journal of Strategic Studies 38 (2015), S. 4 (7).

[131] *F. Egloff/M. Dunn Cavelty*, Attribution and Knowledge Creation Assemblages in Cybersecurity Politics, Journal of Cybersecurity 7:1 (2021), S. 1 ff.

[132] Zu sekundären Funktionalitäten der Attributions- bzw. Verantwortungsfrage, insbesondere ihrer Fähigkeit, Öffentlichkeit für die mit der Gewährleistung von Informationssicherheit verbundenen Herausforderungen zu erzeugen, instruktiv *T. Steffens*, Attribution of Advanced Persistent Threats, 2020, S. 23 ff.; *F. Egloff*, Contested Public Attributions of Cyber Incidents and the Role of Academia, Contemporary Security Policy 41:1 (2020), S. 51 (56). Zur normgenerierenden Funktion entsprechender „accusations" *Finnemore/Hollis*, Beyond Naming and Shaming, EJIL 31:3 (2020), S. 969 (981 ff.).

[133] Umfassend zum technischen Hintergrund *Steffens*, Attribution of Advanced Persistent Threats, 2020. Instruktiv zur Einführung auch *H. Lin*, Attribution of Malicious Cyber Incidents, Columbia SIPA Journal of International Affairs 2016, S. 75 ff.; *J. Davis/B. Boudreaux et al.*, Stateless Attribution, 2017, S. 9 ff.

[134] Die Diskussion (außen-)politischer und (völker-)rechtlicher Fragen geht hier häufig ineinander über. Aus der großen Zahl an primär politikwissenschaftlichen Beiträgen zur Thematik siehe nur zur Einführung: *Rid/Buchanan*, Attributing Cyber Attacks, Journal of Strategic Studies 38 (2015), S. 4 ff.; *J. Lindsay*, Tipping the scales, Journal of Cybersecurity 1:1 (2015), S. 53 ff.; *Lin*, Attribution of Malicious Cyber Incidents, Columbia SIPA Journal of International Affairs 2016, S. 75 ff.; *M. Mueller/K. Grindal et al.*, Cyber attribution, The Cyber Defense Review 4:1 (2019), S. 107 ff.; *K. Ziolkowski*, Attribution von Cyber-Angriffen, GSZ 2019, S. 51 ff.; *S. Goel*, How Improved Attribution in Cyber Warfare Can Help De-Escalate Cyber Arms Race, Connections 19:1 (2020), S. 87 ff. Völkerrechtliche Fragen stehen im Zentrum u. a. bei *Krieger*, Krieg gegen anonymus, AVR 50 (2012), S. 1 ff.; *W. Banks*, State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0, Tex. L. Rev. 95 (2017), S. 1487 ff.; *N. Tsagourias*, Cyber attacks, self-defence and the problem of attribution, Journal of conflict and security law, 17:2 (2012), S. 229 ff.; *Eichensehr*, The Law and Politics of Cyberattack Attribution, UCLA L. Rev. 67 (2020), S. 520 ff.; *Finnemore/*

sonders im Völkerrecht weit fortgeschritten.[135] Dort konzentriert sich die Debatte zum einen auf die *materiellen* Standards, d. h. auf die Frage, unter welchen Bedingungen Staaten entsprechende Schäden zuzurechnen sind.[136] Hier ist insbesondere herausfordernd, zu bestimmen, wann das Handeln privater Gruppen als staatliches Handeln zählt – in der Praxis „delegieren" einige Staaten regelmäßig aggressive Aktivitäten im Cyberraum wie (Wirtschafts-)Spionage, die Begehung von Straftaten (etwa durch Einsatz von Ransomware) oder auch weitergehende strategische Schädigungen an „privat" organisierte Gruppierungen.[137] Erschwert wurde diese Diskussion dadurch, dass die Vorfrage, ob und inwieweit die allgemeinen Standards der Staatenverantwortlichkeit[138] überhaupt im „Cyberraum" Geltung beanspruchen können, erst seit Kurzem allgemein positiv beantwortet wird.[139] Gestritten wird zum anderen über die

Hollis, Beyond Naming and Shaming, EJIL 31:3 (2020), S. 969 ff.; *Tsagourias/Farrell*, Cyber Attribution, EJIL 31:3 (2020), S. 941 ff. Siehe auch die Beiträge zum „Symposium on Cyber Attribution" in AJIL Unbound 113 (2019) mit der Einführung von *M. Hakimi*, Introduction to the Symposium on Cyber Attribution, AJIL Unbound 113 (2019), S. 189 f.

[135] Im Überblick *M. Schmitt*, Cybersecurity and International Law, in: Geiß/Melzer (Hrsg.), The Oxford Handbook of the International Law of Global Security, 2021, S. 661 ff.

[136] Zum Stand der Völkerrechtsentwicklung in diesem Bereich *Walter*, Cyber Security als Herausforderung für das Völkerrecht, JZ 70 (2015), S. 685 (687 ff.); *Banks*, State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0, Tex. L. Rev. 95 (2017), S. 1487 (1493): „substantially underdeveloped customary international law on attribution of cyber operations". Zum sehr begrenzten Einfluss des Tallinn Manual 2.0 auf die Praxis *D. Efrony/Y. Shany*, A Rule Book on the Shelf?, AJIL 112:4 (2018), S. 583 ff. Zu möglichen Ansätzen für eine stärkere Verrechtlichung der Materie siehe nur *K. Mačák*, From Cyber Norms to Cyber Rules, Leiden Journal of International Law 30:4 (2017), S. 877 ff.; *D. Hollis/M. Waxman*, Promoting International Cybersecurity Cooperation, Temple Int'l & Comp. L. J. 32 (2018), S. 147 ff.; *N. Tsagourias*, The Slow Process of Normativizing Cyberspace, AJIL Unbound 113 (2019), S. 71 ff. Sehr optimistisch demgegenüber *Pernice*, Global Cybersecurity Governance, Global Constitutionalism (2018), S. 112 (129 ff., 132 ff.); *Kettemann*, The Normative Order of the Internet, 2020, S. 233 ff. und passim (vgl. allerdings a.a.O, S. 155 ff., die instruktive Darstellung der grundlegenden Konflikte, die einer positiven Entwicklung der Völkerrechtsentwicklung im Wege stehen).

[137] Zu den entsprechenden Standards *Tsagourias/Farrell*, Cyber Attribution, EJIL 31:3 (2020), S. 941 (951 ff.).

[138] Maßgeblich sind die „Articles on Responsibility of States for Internationally Wrongful Acts" der International Law Commission (ILC) von 2001.

[139] Vgl. hierzu die Dokumentation der Aktivitäten der UN unter https://www.un.org/disarmament/ict-security/. Dort tagten im Auftrag der Generalversammlung eine Open-ended Working Group und eine Group of Governmental Experts (GGE). Die letzte GGE war bereits die sechste zu dieser Thematik eingesetzte Gruppierung. Siehe zuvor insbesondere die Empfehlungen der vierten GGE: *United Nations General Assembly*, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22.7.2015, A/70/174. Die Arbeit der fünften GGE scheiterte dann u. a. daran, dass über die Anwendbarkeit des Völkerrechts auf den Cyberspace keine Einigung erzielt werden konnte, vgl. *E. Korzak*, UN GGE on Cybersecurity: The End of an Era?, Diplomat, 31.7.2017; *A. Sukumar*, The UN GGE Failed: Is International Law in Cyberspace Doomed as Well?, Lawfare, 4.7.2017; *M. Schmitt/L. Vihul*, Interna-

prozessuale Frage, unter welchen Bedingungen[140] und in welchem Forum[141] der Nachweis der Verantwortlichkeit zu erbringen ist. Dass Ermittlungen oft mit nachrichtendienstlichen Mitteln operieren müssen, schon weil die Informationen nur in kooperationsunwilligen Drittstaaten gewonnen werden können, führt dazu, dass die Früchte dieser Anstrengungen in rechtsstaatlichen Verfahren oft nur eingeschränkt verwertbar sind, was die Beweisproblematik nochmals verschärft.[142] Unterhalb der Ebene des Völkerrechts, etwa bei der

tional Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms, Just Security, 30.6.2017. Dies löste eine intensive Debatte über die Anwendbarkeit des Völkerrechts und des Souveränitätsprinzips auf den digitalen Raum aus, vgl. die Beiträge im Symposium „Sovereignty, Cyberspace, and Tallinn Manual 2.0" in AJIL Unbound 111 (2017), S. 205 ff.; *Efrony/Shany*, A Rule Book on the Shelf?, AJIL 112:4 (2018), S. 583 (653); *T. Moulin*, Reviving the Principle of Non-Intervention in Cyberspace, Journal of Conflict and Security Law 25:3 (2020), S. 423 (426 ff.); siehe auch allgemein *A. Grigsby*, The End of Cyber Norms, Survival 59:6 (2017), S. 109 ff.; *A. Henriksen*, The End of the Road for the UN GGE Process, Journal of Cybersecurity 5:1 (2019), S. 1 ff. Siehe aber jetzt den Bericht der sechsten GGE: *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. 69 ff. Allgemein zur begrenzten Problemlösungskapazität des UN-Systems in Sachen Informationssicherheit *Kello*, Cyber Threats, in: Weiss/Daws (Hrsg.), The Oxford Handbook on the United Nations, 2. Aufl. 2018, S. 528 ff. Einen skeptisch-konstruktiven Blick auf die völkerrechtliche Normentwicklung in diesem Zusammenhang entwickeln *Finnemore/Hollis*, Constructing Norms for Global Cybersecurity, AJIL 110 (2016), S. 425 ff. Vgl. auch den Literaturüberblick unter https://www.thehagueprogram.nl/cyber-norms-bibliography.

[140] Dazu ausführlich *Eichensehr*, The Law and Politics of Cyberattack Attribution, UCLA L. Rev. 67 (2020), S. 520 (559 ff.); *Tsagourias/Farrell*, Cyber Attribution, EJIL 31:3 (2020), S. 941 (951 ff.). Auch hier ist der Stand der Völkerrechtsentwicklung gegenwärtig unbefriedigend, vgl. das Fazit bei *Tsagourias/Farrell*, Cyber Attribution, EJIL 31:3 (2020), S. 941 (959): „the absence of well-articulated standards of proof and their mutability create uncertainty which may affect the credibility, reliability and also the validity of legal determinations." Beispielhaft hierfür die nichtssagende Formulierung der *United Nations General Assembly*, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22.7.2015, para 28(f). Bemerkenswerterweise geht die Forderung nach der Entwicklung anspruchsvoller Beweisstandards auf völkerrechtlicher Ebene vor allem von Russland und China aus, während die USA und die EU insoweit auf größeren Einschätzungsspielräumen beharren, vgl. dazu kritisch *Eichensehr*, The Law and Politics of Cyberattack Attribution, UCLA L. Rev. 67 (2020), S. 520 (545, 566 ff.).

[141] Mit entsprechenden institutionellen Vorschlägen *Mueller/Grindal/Kuerbis/Badiei*, Cyber attribution, The Cyber Defense Review 4:1 (2019), S. 107 ff.; kritisch dazu *Tsagourias/Farrell*, Cyber Attribution, EJIL 31:3 (2020), S. 941 (959 ff.) m. w. N.; für ein dezentrales System plädierend *Eichensehr*, The Law and Politics of Cyberattack Attribution, UCLA L. Rev. 67 (2020), S. 520 (587 ff.). Instruktiv ferner *Finnemore/Hollis*, Beyond Naming and Shaming, EJIL 31:3 (2020), S. 969 ff.

[142] Dass Attributionsermittlungen ihrerseits oft Datenschutz- und Informationssicherheitshürden überwinden müssen, betonen *S. Goel/B. Nussbaum*, Attribution Across Cyber Attack Types, IEEE Open Journal of the Communications Society 2 (2021), S. 1082 ff. Hinzu kommt, dass die Auswahl der Informationsziele, die Art und Weise der Informati-

Suche nach den für Cyberkriminalität Verantwortlichen stellen sich im Übrigen ganz entsprechende Schwierigkeiten.[143]

Diese spezifisch (völker-)rechtlichen Probleme sollen hier nicht gelöst werden. Stattdessen sind die Auswirkungen des Attributionsproblems auf die Gestaltung von Informationssicherheitspolitik und -recht zu beleuchten. Diese sind erheblich: Ist nicht bestimmbar, wer oder was die Ursache für Informationssicherheitsrisiken gesetzt hat, ob also überhaupt ein Angriff oder nicht vielleicht doch „nur" ein technisches Versagen vorliegt bzw. in ersterem Fall, wem dieser zuzurechnen ist, verringert dies die Effektivität aller Formen der personenbezogenen Sicherheitsgewährleistung, insbesondere durch die Androhung von Strafen oder – im Kontext der Informationssicherheit mangels strafrechtlicher Erreichbarkeit der Täter üblich – durch die Verhängung individualbezogener Wirtschaftssanktionen.[144] Selbst wenn man die jüngsten Verbesserungen der Forensik in Rechnung stellt, reichen diese für personenscharfe Zuschreibungen oft nicht aus. Die personale Verantwortungslogik des Rechts kommt hier an ihre praktischen Grenzen.

Anders mag dies auf mittlere Sicht im Völkerrechtsverkehr sein, wozu die Fortschritte bei der Identifikation größerer Verantwortungsstrukturen, einschließlich Staaten, beitragen. Aktuell jedoch schwächen, wie beschrieben, rechtliche Unklarheiten die Effektivität herkömmlicher, auf Attribuierung und Abschreckung beruhender Instrumente des Völkerrechts.[145]

Jedenfalls im zivilen Kontext sind jedoch Regulierungsmechanismen, die beim Gefährder bzw. Störer anknüpfen, um diesen zur Verantwortung zu ziehen, auf mittlere Sicht wohl nur sehr eingeschränkt leistungsfähig. Eine angemessene Abgrenzung der Freiheitssphären kann mit ihrer Hilfe kaum gelingen. Würde Regulierung allein hierauf setzen, könnte sie den real bestehenden Sicherheitsbedarf kaum decken. Vor diesem Hintergrund erweist sich die vergleichsweise frühe Reaktion des Strafrechtsgesetzgebers auf das Informationssicherheitsproblem, die sogar in entsprechende völkerrechtliche Abkommen – allen voran die „Budapester Konvention gegen Datennetzkriminalität" (Cy-

---

onsgewinnung und deren Aufbereitung durch Nachrichtendienste ihre Eigenheiten und Pfadabhängigkeiten aufweist, vgl. *Egloff/Dunn Cavelty*, Attribution and Knowledge Creation Assemblages in Cybersecurity Politics, Journal of Cybersecurity 7:1 (2021), S. 1 (2).

[143] Vgl. *Tsagourias/Farrell*, Cyber Attribution, EJIL 31:3 (2020), S. 941 (946), mit Nachweisen zu entsprechenden Entscheidungen der U.S.-Strafjustiz sowie zur Entscheidungspraxis im Fall von Wirtschaftssanktionen gegen Individuen. Zur intensiven Sanktionspraxis der USA in diesem Bereich siehe auch *Eichensehr*, The Law and Politics of Cyberattack Attribution, UCLA L. Rev. 67 (2020), S. 520 (532 ff.).

[144] Vgl. dazu oben § 1 Fn. 44 und § 2 Fn. 29. Differenzierend hierzu mit Blick auf die Attributionskosten *J. Lindsay*, Tipping the Scales, Journal of Cybersecurity 1:1 (2015), S. 53 ff.

[145] Vgl. als Ausweg den innovativen Vorschlag zum Institut der „accusation" bei *Finnemore/Hollis*, Beyond Naming and Shaming, EJIL 31:3 (2020), S. 969 ff.

bercrime Convention) des Europarats aus dem Jahr 2001[146] – gemündet ist, als ungeeignet, um allein einen nachhaltigen Beitrag zur Stabilisierung der Informationssicherheitslage zu leisten, wirkten und wirken die strafrechtlichen Sanktionen doch gerade auf professionelle Akteure kaum abschreckend.[147] Ähnliches gilt für das Haftungs- und das Versicherungsrecht.[148]

Dieser Befund steht dem Vorhaben, mittels rechtlicher Regulierung die IT-Sicherheitslage zu verbessern, allerdings keineswegs grundsätzlich im Wege. Aus der Schwierigkeit der Zurechnung von Angriffen darf nicht auf die faktische Unregulierbarkeit der Materie geschlossen werden. Wären (rechtliche) Maßnahmen zur Stärkung der Informationssicherheit nur dann möglich und sinnvoll, wenn sich (potenzielle) Störer und konkrete Gefährdungssituationen klar identifizieren ließen, würde das *problem of attribution* tatsächlich zum Fundamentaleinwand gegen die Regulierbarkeit von Informationssicherheit. Private und hoheitliche Präventionsmaßnahmen sind jedoch auf derartige Kenntnisse nicht zwingend angewiesen. Wenn sich die primär Verantwortlichen nicht identifizieren lassen, kann und muss die Sicherheitsgewährleistung eben bereits im Vorfeld der Entstehung konkreter Gefahren ansetzen. Dies erzeugt Druck auf jene Akteure (Hersteller, Betreiber, System-Administratoren, normsetzende Stellen etc.), die präventiv die Resilienz der IT-Infrastrukturen verbessern, Präventionsmaßnahmen entwickeln oder Ausfallkapazitäten bereithalten können. Diese Akteure lassen sich meist ohne große Schwierigkeiten identifizieren. Einige werden dabei für Staaten greifbarer als andere sein, aber das teilt dieser Sachbereich mit vielen anderen Materien. Damit ist nicht gesagt, dass Maßnahmen, deren Ziel ist, die unterschiedlichen Angreifer – seien es Hacker, Hacktivisten, Kriminelle oder Staaten[149] – zur Verantwortung zu ziehen, sinnlos sind. Doch sollte sich das Informationssicherheitsrecht nicht auf diesen Regulierungsvektor beschränken. Wie noch zu zeigen sein wird, ist dies genau der Ansatz, den die Informationssicherheitsregulierung in Übereinstimmung mit dem Grundgedanken des Zivilen Sicherheitsrechts heute verfolgt.[150]

---

[146] Übereinkommen über Cyberkriminalität des Europarats v. 23.11.2001 (Cybercrime Convention), in Kraft getreten am 1.7.2004, von der Bundesrepublik unterzeichnet am 23.11.2001, ratifiziert am 9.3.2009 und in Deutschland in Kraft getreten am 1.7.2009 gem. Gesetz v. 5.11.2008, BGBl. II 2008 S. 1242 (1243) und BGBl. II 2010 S. 218.

[147] Zum Begriff der Computerkriminalität umfassend *A. Haase*, Computerkriminalität im Europäischen Strafrecht, 2017, S. 57 ff.

[148] Zu dem in hohem Maße praxisrelevanten Problem, das die (fehlende) Attribuierbarkeit für die Versicherbarkeit von Cyberrisiken darstellt, vgl. *Eichensehr*, The Law and Politics of Cyberattack Attribution, UCLA L. Rev. 67 (2020), S. 520 (522 f.). Zur Ineffektivität der bisherigen Ansätze zur Versicherung von Informationssicherheitsrisiken ausführlich jetzt *J. Wolff*, Cyberinsurance Policy, 2022.

[149] Treffend als die vier „Autoren der Cyber-Unsicherheit" bezeichnet bei *Finnemore/Hollis*, Constructing Norms for Global Cybersecurity, AJIL 110 (2016), S. 425 (434 f.).

[150] Siehe unten § 6 II. 4.

c) Untauglichkeit der Unterscheidung von security und safety zur Erfassung von Informationssicherheitsrisiken

Neben dem Attributionsproblem, das die Möglichkeit informationssicherheitsbezogener Regulierung in Frage stellt, Maßnahmen nach dem Grad der persönlichen Verantwortlichkeit abzustufen, lassen auch weitere Spezifika von Informationssicherheitsrisiken die Wahl eines „All-Gefahren-Ansatzes" prima facie als sachgemäß erscheinen. Insbesondere erscheint es nicht sinnvoll, je eigenständige Regime für die Abwehr von Angriffen auf IT-Systeme einerseits und für deren technische Sicherung andererseits vorzusehen.

Die Differenzierung zwischen *security* und *safety* ist zwar im technischen und im regulatorischen Diskurs anerkannt und manifestiert sich insbesondere in den ingenieurwissenschaftlichen Disziplinen in einer starken Trennung der jeweiligen Fachgruppen.[151] Dabei werden unter *safety* primär technische Sicherungsmaßnahmen gefasst, die vor solchen Schädigungen Dritter schützen sollen, die durch Fehlfunktionen des Systems selbst, durch dessen (unwillentlich) fehlerhafte Bedienung oder auch durch Naturereignisse verursacht werden. *Safety*-Maßnahmen sichern damit den störungsfreien Betrieb von Systemen und umfassen die Prävention von Ausfällen und Unfällen. Hier setzen insbesondere die das Produktsicherheitsrecht (*product safety*) konstituierenden rechtlichen und technischen Normen an.[152] Im Fall von IT-Systemen zählen hierzu etwa Maßnahmen zur Fehlervermeidung bei der Code-Erstellung. Mit *security* werden hingegen Maßnahmen verbunden, die absichtlich oder unabsichtlich handelnde (menschliche) Angreifer vom System abwehren sollen. Trotz bleibender Abgrenzungsprobleme hat die Unterscheidung nach allgemeiner Auffassung grundsätzlich einen analytischen Wert. Teile der Rechtswissenschaft empfehlen dementsprechend zur Rationalisierung und Einhegung eines übermäßig weiten Sicherheitsbegriffs allgemein die Trennung von *safety*- und *security*-bezogenen Regulierungsmaßnahmen.[153]

---

[151] Zum Folgenden siehe nur *Kaufmann*, Das Themenfeld „Zivile Sicherheit", in: Gusy/Kugelmann/Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, 2017, S. 3 (5); *Eckert*, IT-Sicherheit, 10. Aufl. 2018, S. 7.

[152] Vgl. die dortige Definition von Sicherheit/*safety* in Annex I, 1.2.1, der EU-Maschinen-Richtlinie 2006/42/EG sowie § 3 Abs. 1 ProdSG. Aus der technischen Normung siehe beispielhaft für Industrieroboter ISO 10218–1 „Robots and robotic devices – Safety requirements for industrial robots – Part 1: Robots". Die Integration von IT-Sicherheitsfragen, die auch die *security*-Dimension erfassen, stellt das Recht der Produktsicherheit daher vor erhebliche Herausforderungen. Dazu weiter unten § 6 II. 6. Mit dem Konzept der *functional safety*, das auch aus *safety*-Sicht verstärkte Reflexion über mögliche Fehlfunktionen verlangt (grundlegend IEC 61508–1:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems), versucht die technische Normung aktuell darauf zu reagieren, dass der „klassische" *safety*-Begriff im IT-Kontext wenig leistungsfähig ist.

[153] *Rusteberg*, Zivile Sicherheit in der Sicherheitsarchitektur des deutschen Bundesstaates, in: Gusy/Kugelmann/Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, 2017, S. 113 (117 ff.).

Speziell im Bereich der Informationssicherheit verlangt – wie weithin konsentiert – bereits die Komplexität der zu Grunde liegenden Technik einen integrierten Ansatz. So lässt sich die *safety* von Systemen vielfach nicht hinreichend beurteilen, ohne eine mögliche Kompromittierung durch *security*-Szenarien (Angriffe von außen) mitzudenken.[154] Umgekehrt dienen Maßnahmen zur Steigerung der „Betriebssicherheit" auch zur vorbeugenden Abwehr anonymer, schwer oder noch nicht als Störer greifbarer Dritter. Hinzu kommt, dass die *safety*-Mechanismen vernetzter IT besonders attraktive Angriffsziele darstellen; schon deshalb müssen beide Perspektiven hier zusammengedacht werden.[155] Schließlich ist die systemische Natur von IT-Sicherheitsrisiken zu bedenken.[156] Unter den Bedingungen umfassender Vernetzung stellen jedes IT-System und jeder Datentransfer eine potenzielle Risikoquelle dar. Mit steigendem Vernetzungsgrad sind zudem Interaktionen zwischen unterschiedlichen Gefährdungslagen möglich. Mögen einzelne Schwachstellen für sich gesehen harmlos erscheinen, können sie in Verbindung miteinander den entscheidenden Weg für Angreifer bereiten.

Regulierung und Normung in diesem Bereich müssen somit ein breites Arsenal von Instrumenten nutzen, um Schäden sowohl an IT-Systemen als auch durch IT-Systeme zu verhindern. Vor diesem Hintergrund erscheint es konsequent, dass gerade Informationssicherheit – nämlich im Bereich der Kritischen Infrastrukturen – eines der Felder war, in dem der Wandel des Sicherheitsbegriffs hin zum integrierten „All-Gefahren-Ansatz" des neuen Sicherheitsrechts seinen Ausgang genommen hat.[157]

3. Folgen für das Rechtssystem: Identifikation von Aufmerksamkeitsfeldern II

Auch wenn daher nach Sachlage die Wahl eines integrierten Regulierungsansatzes für den Bereich der Informationssicherheit zwingend ist, erzeugen die

[154] Dementsprechend stellen die maßgeblichen technischen Normen im Bereich IT-Sicherheit stets den *security*-Gedanken bzw. -Begriff in den Vordergrund. Dies gilt etwa für den BSI IT-Grundschutz, für die ISO 2700x-Reihe zu Informationssicherheit und Informationssicherheitsmanagement, für die Reihe IEC 62443 Industrial Communication Networks – Network and System Security und für den NIST 800–82 Guide to Industrial Control Systems (ICS) Security. Zu diesen Normenreihen siehe unten § 6 II. 6. b).

[155] *L. Fischer/M. Messerschmidt*, Ohne Security keine Safety in Kritischen Infrastrukturen, AG Kritis, 4.5.2020, S. 4.

[156] Dazu bereits *Deutscher Bundestag*, Neunter Zwischenbericht der Enquete-Kommission „Internet und digitale Gesellschaft" – Zugang, Struktur und Sicherheit im Netz, 19.3.2013, BT Drs. 17/12541, S. 56. Siehe instruktiv weiter *Eckert*, IT-Sicherheit, 10. Aufl. 2018, S. 37, zur „IT-Sicherheitskette", die nur so stark wie ihr schwächstes Glied ist. Weiter auch unten § 6 II. 1. c).

[157] Siehe oben § 4. I. 2. d); siehe auch *Wiater*, Sicherheitspolitik zwischen Staat und Markt, 2013, S. 22 f.

tatsächlichen Unschärfen dennoch rechtliche Unschärfen. So wird die für die völker- und verfassungsrechtliche Maßstabsbildung wichtige Einordnung anhand der Kategorien der inneren oder der äußeren Sicherheit erschwert, wenn ungewiss ist, woher ein Angriff kommt, oder wenn fremde staatliche Akteure mit privaten Akteuren kollusiv zusammengewirkt haben.[158] Technische Gründe führen dazu, dass staatliche Abwehrmaßnahmen selten klar als „offensiv" (Angriff) oder „defensiv" (Verteidigung) klassifiziert werden können.[159] Auch die Abstufung von Maßnahmen nach Risikoursachen ist schwierig, wirken in der Praxis doch oft ganz unterschiedliche Faktoren zusammen: So werden gezielte Angriffe auf IT-Systeme durch fahrlässige Handlungen Dritter (etwa fehlerhaft verwendete USB-Sticks), eine bestimmte Technikgestaltung (etwa unsicher programmierte Software) oder auch Naturereignisse (etwa Stromausfälle) erleichtert – keine der Bedingungen lässt sich hinwegdenken, ohne dass die Gefährdungssituation entfiele.[160] Auch die Schadenswirkung ist diffus; Schädigungen können öffentlichen ebenso wie privaten Gütern gelten. Weitere für das Recht wichtige Unterscheidungen wie die zwischen öffentlicher und privater Sicherheitsvorsorge ließen sich ergänzen.[161]

Wie das Recht diese großflächige Infragestellung dieser Kategorien verarbeitet, wird noch näher zu untersuchen sein. Hier soll zunächst festgehalten werden, dass dieser Befund nicht a priori zu einer Relativierung der den Differenzierungen zu Grunde liegenden Prinzipien zwingt; vielmehr gilt, was *Christoph Gusy* übergreifend für das Konzept der Zivilen Sicherheit festgehalten hat, dass dessen breiter Ansatz „nicht sinnvolle und notwendige Differenzen einebnen oder hinwegdefinieren, sondern deren Befragung auf Gegenstandsangemessenheit und Sachgerechtigkeit ermöglichen" will.[162]

Es sind somit auch im Fall der Informationssicherheit die bereits oben identifizierten Aufmerksamkeitsfelder – die Beeinträchtigung der Grundrechte,

---

[158] Zur Relevanz dieser Unterscheidung siehe nur *Möstl*, Die staatliche Garantie für die öffentliche Sicherheit und Ordnung, 2002, S. 277 ff.; *Stoll*, Sicherheit als Aufgabe, 2003, S. 15.

[159] Dem trägt etwa das Tallinn Manual 2.0 in seiner Definition einer militärischen „cyber operation" in der Form Rechnung, dass diese sowohl offensive als auch defensive Maßnahmen umfasst, vgl. Schmitt (Hrsg.), Tallinn Manual 2.0, 2017, S. 415 (Rule 92): „[…] whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."

[160] Der BSI-Grundschutz unterscheidet sogar 47 Formen elementarer Gefährdungen, die von unterschiedlichen Varianten höherer Gewalt über diverse organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen bis hin zu verschiedenen vorsätzlichen Handlungen reichen, vgl. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Elementare-Gefaehrdungen/elementare-gefaehrdungen_node.html.

[161] Dazu oben § 4 Fn. 112.

[162] *Gusy*, Ziele, Aufträge und Maßstäbe, in: Gusy/Kugelmann/Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, 2017, S. 55 (72).

die Auswirkungen auf die Gewaltenteilung und auf die föderale Kompetenzverteilung –, denen bei der Regulierung des Bereichs besondere Beachtung geschenkt werden muss, weil sie aus Effektivitätsgründen naheliegenden regulatorischen Lösungen Grenzen ziehen können, weil sie aber auch im Lichte der komplexen Gegebenheiten der Materie ihrerseits an einzelnen Stellen womöglich der Fortentwicklung bedürfen. Insbesondere die historisch bedingte und bei der Feldanalyse nicht zu ignorierende starke Präsenz von Militär und Nachrichtendiensten im Bereich der Informationssicherheitsgewährleistung ist eine ernstzunehmende Belastung für eine rechtsstaatskonforme Ausgestaltung der Materie.

Welche Herausforderungen sich hier stellen, sei abschließend anhand eines Beispiels illustriert.[163] 2011 hat die Bundesregierung auf Grundlage der seinerzeitigen Nationalen Cyber-Sicherheitsstrategie beim BSI ein Nationales Cyber-Abwehrzentrum (NCAZ) als Informationsverbund von BSI, BBK, Sicherheitsbehörden (u. a. dem BKA), Diensten (u. a. BfV und BND), der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und der Bundeswehr errichtet, dessen Gestalt sich am Gemeinsamen Terrorismusabwehrzentrum (GTAZ) orientiert.[164] Im NCAZ werden also Behörden mit dem Auftrag personenbezogener Risikoabwehr und technische Sicherheitsbehörden, die nach hergebrachtem Verständnis getrennt aufgestellt sind, in einen gemeinsamen institutionellen Rahmen eingebunden. Unabhängig von der Frage nach der Funktionalität des NCAZ[165] zeigt dessen Konstruktion wie in einem Brennglas die Herausforderungen, mit denen effektive Informationssicherheitsregulierung konfrontiert ist: Die Koordinierung der von Behörden mit ganz unterschiedlichen Aufgaben und Eingriffsermächtigungen generierten Informationen im Verbund wirft heikle grundrechtliche Fragen nach den Möglichkeiten und Grenzen der Informationsweitergabe – insbesondere auch im Lichte des sogenannten (informationellen) Trennungsgebotes zwischen Polizei und Nachrichtendiensten – auf.[166] Diese Fragen erledigen sich offensichtlich nicht durch den Verweis auf die übergeordnete Notwendigkeit des Informations-

[163] Auf das folgende Beispiel wird unten bei § 5 III. 1. b) aa) noch einmal zurückzukommen sein.

[164] Vgl. die Selbstdarstellung unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/Nationales-IT-Lagezentrum/Nationales-Cyber-Abwehrzentrum/nationales-cyber-abwehrzentrum_node.html. Aus der Literatur zum NCAZ siehe die Nachweise unten § 5 Fn. 229.

[165] Dazu unten § 5 Fn. 229 und 233.

[166] Siehe dazu nur allgemein *M. Zöller*, Informationssysteme und Vorfeldmaßnahmen, 2002; *A. Sommerfeld*, Verwaltungsnetzwerke am Beispiel des Gemeinsamen Terrorismusabwehrzentrums des Bundes und der Länder (GTAZ), 2015; sowie jetzt den Überblick bei *M. Albers*, Sicherheitsbehördliche Vernetzung und Datenschutz, in: Seckelmann (Hrsg.), Digitalisierte Verwaltung – Vernetztes E-Government, 2. Aufl. 2019, S. 509 (522 ff.); *Bäcker*, Organisationsverfassungsrechtliche Grundlagen der Polizeiarbeit, in: Lisken/Denninger, HdbPolR, 7. Aufl. 2021, Kap. B III. Rn. 261 ff.

austauschs zum Zweck der Informationssicherheit. Ebenso wenig kann jedoch die juristische Analyse das Ziel dieses Zusammenschlusses bei der Bewertung der Maßnahmen ganz außer Acht lassen. Mit Blick auf die Gewaltenteilung stellt das fehlende Errichtungsgesetz beim NCAZ (ähnlich wie beim GTAZ und bei ZITiS) in Frage, ob die hier organisierte Zusammenarbeit auf einer hinreichenden Rechtsgrundlage beruht, was allgemein die Frage nach der Rolle des Gesetzgebers in Sachen IT-Sicherheit aufwirft. Schließlich erweist sich die nur in Ansätzen erfolgte Einbeziehung der Länder ebenso wie die Koordination mit der europäischen Ebene, mithin die föderale Kompetenzordnung, als erhebliche Herausforderung für den Erfolg des NCAZ.[167] Denn, wie bereits am Beispiel von KRITIS erörtert, liegt ein auf Bundesebene vorangetriebener „All-Gefahren-Ansatz" quer zum grundgesetzlichen Kompetenzrahmen, der die Gefahrenabwehr grundsätzlich den Ländern zuweist.[168]

Das Beispiel demonstriert, wie die überkommenen Maßstäbe des Verfassungsrechts durch die Informationssicherheitsregulierung herausgefordert werden. Es darf jedoch nicht dahingehend missverstanden werden, dass die Maßstäbe keinerlei Orientierung mehr böten. Vielmehr gilt es aus Sicht der Rechtswissenschaft, auf ihrer Grundlage neue Wege zur Bewältigung der komplexen Herausforderungen zu suchen.

III. Facetten der Informationssicherheit

Das Sicherheitsrecht zeigt sich heute als eine überaus vielfältige Materie, die nicht mehr einem konkreten Leitbild von Verwaltung verpflichtet ist, sondern die je nach Sachbereich mit mehr oder weniger passgenauen Regelungen auf die anfallenden Sicherheitsbedarfe reagiert.[169] Die Kritik an dieser Flexibilisierung von Sicherheitsbegriff und Sicherheitsrecht („Versicherheitlichung") trifft dabei, zumindest im Fall der Informationssicherheit, in verschiedenen Punkten zu. Gerade wenn man die Technik, die durch die Regulierung von Informationssicherheit adressiert wird, wie hier als soziales System und als Ensemble von Praktiken, Verfahren, und Präferenzen begreift,[170] liegt es nahe,

[167] Siehe hierzu die Überlegungen bei *S. Herpig/C. Bredenbrock*, Cybersicherheitspolitik in Deutschland – Akteure, Aufgaben und Zuständigkeiten. Im Fokus: Das Cyber-Abwehrzentrum, April 2019, S. 8 f. Zur Kompetenzproblematik näher unten § 5 III. 1. b) aa).

[168] Dazu oben § 4 I. 3. b) cc). Siehe auch *B. Pistorius*, Föderalismus und Cybersicherheit, in: Jahrbuch des Föderalismus 2018, S. 74 ff.

[169] Dementsprechend die Feststellung bei *Gusy*, Ziele, Aufträge und Maßstäbe, in: Gusy/Kugelmann/Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, 2017, S. 55, dass es ebenso wenig „die" Sicherheitsgewährleistung wie „das" Sicherheitsrecht gibt.

[170] Dazu oben § 3 I. 3. Spezifisch für Cybersicherheit nochmals *M. Dunn Cavelty*, Cybersecurity Research Meets Science and Technology Studies, Politics and Governance 6:2 (2018), S. 22 ff.

den dort herrschenden diskursiven Formationen kritische Aufmerksamkeit zuzuwenden.[171]

So muss bei der nachfolgenden Analyse des rechtlichen Instrumentariums im Blick behalten werden, dass es sich hierbei nicht um technische Expertise handelt, die in deliberativen politischen Prozessen zur reflexiven Entscheidung geronnen ist. Auch wenn in einem aus der Technik heraus gewachsenen Diskurs wie dem der Informationssicherheit eine natürliche Neigung dazu bestehen mag, Fragen der rechtlichen Steuerung und Regulierung bzw. der Governance in den technischen Kategorien des Risikomanagements zu denken, sind subpolitische Kategorien wie „Sachzwang" oder „Natur der Technik" ungeeignet, um aus sich heraus eine bestimmte rechtliche Ausgestaltung zu rechtfertigen. Dass sich mit einzelnen Kontroll- und Risikominimierungsmaßnahmen immer Interessen und damit Wertungen verbinden, ist eine elementare Einsicht des Technikrechts.

Gleichzeitig darf die berechtigte Skepsis gegenüber Strategien der Versicherheitlichung nicht aus dem Blick verlieren, dass die digitale Gesellschaft durchaus realen und mit dem konventionellen Instrumentarium schwer in den Griff zu bekommenden Risiken ausgesetzt ist; nicht jeder Versuch, die etablierten Maßstäbe zu überprüfen und neue Wege zu gehen, darf daher als Schritt Richtung Ausnahmezustand oder illiberale Gouvernementalität verstanden werden. Dort, wo tatsächlich überschießende Reaktionen festzustellen sind, muss darauf – ganz im Sinne des *desecuritization*-Gedankens – jedoch mit einer Kultur der Rationalisierung, des Kompromisses und der „Normalisierung" reagiert werden.[172]

Insgesamt bleibt es dabei, dass Informationssicherheit, als Aufgabe verstanden, das ganze Spektrum von Gefährdungslagen adressieren muss, ohne dass damit vorab eine Aussage über die politische oder gar rechtliche Qualität der jeweiligen Maßnahmen verbunden sein sollte. Der Sicherheitsbegriff wird somit im Folgenden als offenes Konzept verwendet, das seinen normativ relevanten Gehalt erst aus der Aufarbeitung des spezifischen Kontextes der *Informations*sicherheit sowie vor allem mit Blick auf die maßgeblichen rechtlichen Regelungen – einschließlich etwaiger verfassungsrechtlicher Grenzen – erhält.[173] Für die juristische Beurteilung wird durch die Verwendung des Oberbegriffs der Sicherheit nichts vorweggenommen. Festhalten lässt sich, dass der

[171] Eine instruktive Perspektive auf die Art und Weise, in der sich Expertise im Bereich Cybersicherheit durch Rituale als solche konstituiert und identifiziert, bei *J. Shires*, Enacting Expertise: Ritual and Risk in Cybersecurity, Politics and Governance 6:2 (2018), S. 31 ff.

[172] Siehe oben § 4 Fn. 67. Speziell für die Cybersicherheit auch *J. Burton/C. Lain*, Desecuritising Cybersecurity, Journal of Cyber Policy 5:3 (2020), S. 449 ff.

[173] Zur Notwendigkeit, den offenen Begriff der Sicherheit mit Blick auf die jeweiligen Verwendungskontexte zu konkretisieren siehe *D. Brooks*, What Is Security, Security Journal 23 (2009), S. 225 ff.; *C. Smith/D. Brooks*, Security Science, 2013, S. 6 ff.

Begriff der Informationssicherheit neutral ist sowohl was die Entstehung der Gefährdungslage (Naturereignisse, Private, hoheitliche Akteure, Drittstaaten etc.) als auch was die Art und Intensität der Gefahr bzw. des Risikos sowie die Natur der Schutzgüter betrifft. Dies erfordert ein aufgeklärtes, facettenreiches Regelungsregime, das auf die jeweiligen Herausforderungen und die dadurch betroffenen Sicherheitsdimensionen abgestimmte Antworten entwickelt.

Zweiter Teil

Gewährleistung von Informationssicherheit durch Recht

§ 5 Unions- und verfassungsrechtliche Rahmenbedingungen des Informationssicherheitsrechts

> „Die gesetzliche Fixierung eines bestimmten Sicherheitsstandards durch die Aufstellung starrer Regeln würde […], wenn sie sich überhaupt bewerkstelligen ließe, die technische Weiterentwicklung wie die ihr jeweils angemessene Sicherung der Grundrechte eher hemmen als fördern. Sie wäre ein Rückschritt auf Kosten der Sicherheit."[1]

Bevor in den folgenden Kapiteln das Recht der Informationssicherheit im Detail analysiert wird, sollen hier die verfassungsrechtlichen Rahmenbedingungen entfaltet werden, die der Materie Struktur verleihen. Im Vordergrund stehen die grund- und organisationsrechtlichen Vorgaben des Grundgesetzes und des Unionsprimärrechts.[2] Im Einklang mit den etablierten Kategorien der Grundrechtsdogmatik wird zunächst zwischen den Grenzen, die die Grundrechte in ihrer Gestalt als Abwehrrechte staatlichen Interventionen ziehen (I.), und den objektiv-rechtlichen Forderungen, die die Grundrechte mit Blick auf eine Erhöhung des Informationssicherheitsniveaus stellen (II.), differenziert. Dabei zeigt sich, dass unter den Bedingungen der Digitalisierung eine sichere und funktionierende Informationstechnik als allgemeine Wirksamkeitsvoraussetzung der Grundrechte verstanden werden muss. Das sogenannte „IT-Grundrecht" enthält nicht den grundrechtlichen „Kern" der staatlichen Regulierungsverantwortung für die IT-Sicherheit, sondern setzt nur für einen kleinen Ausschnitt der relevanten Systeme einen allerdings deutlichen Akzent. Im Anschluss sind ausgewählte Kompetenz- und Legitimationsfragen zu erörtern (III.). Eine Prüfung konkreter regulatorischer Maßnahmen erfolgt an

---

[1] BVerfGE 49, 89 (137).

[2] Letzteres wird hier – ungeachtet fortbestehender Eigenheiten – als Verfassungsrecht verstanden, vgl. dazu grundlegend *N. MacCormick*, Beyond the Sovereign State, The Modern L. Rev. 56:1 (1993), S. 1. Zu der daraus resultierenden Theorie des *constitutional pluralism* und deren Kritik siehe im Überblick M. Avbelj/J. Komárek (Hrsg.), Constitutional Pluralism in the European Union and Beyond, 2012; *M. Loughlin*, Constitutional Pluralism: An Oxymoron?, Global Constitutionalism 3:1 (2014), S. 9 ff.; *R. Kelemen*, The Dangers of Constitutional Pluralism, in: Davies/Avbelj (Hrsg.), Research Handbook on Legal Pluralism and EU Law, 2018, S. 392 ff.

dieser Stelle nicht. Hier geht es zunächst nur darum, die Maßstäbe zu bestimmen, an denen sich die Informationssicherheitsregulierung messen lassen muss, und insbesondere jene Punkte verfassungsrechtlich nachzuschärfen, die im vorigen Kapitel als Aufmerksamkeitsfelder für die Informationssicherheitsregulierung identifiziert wurden.[3]

I. Grundrechte als Grenze staatlicher Informationssicherheitsregulierung

Im Bereich der Informationssicherheitsregulierung sind die Grundrechte als Abwehrrechte gegen den Staat in zwei sehr unterschiedlichen Konstellationen gefordert.[4] Grund dafür ist, dass staatliches Handeln im Feld der Informationssicherheit – wie dargestellt – gegenläufige Ziele verfolgen kann.[5] Streben staatliche Maßnahmen eine Erhöhung des Informationssicherheitsniveaus an und nehmen sie zu diesem Zweck private Akteure in die Pflicht, ist dies in erster Linie (aber nicht ausschließlich) an den Wirtschaftsgrundrechten der betroffenen Digitalunternehmen zu messen (1.). Anders liegt dies, wenn staatliche Stellen Schwächen der Informationstechnik ausnutzen, etwa zu Überwachungszwecken, oder selbst zur Schwächung des Informationssicherheitsniveaus beitragen, etwa durch ein Verbot von Verschlüsselungstechniken. Hier steht der Schutz (kommunikativer) Privatheit im Vordergrund (2.). Insgesamt kann das Informationssicherheitsproblem aus grundrechtlicher Sicht nur adäquat erfasst werden, wenn dessen Querschnittsnatur Rechnung getragen wird (3.).

1. Grundrechte als Abwehrrechte gegen Maßnahmen zur Erhöhung des Informationssicherheitsniveaus

a) Schutz privater Betreiber informationstechnischer Systeme

In dem weitgehend privat geordneten Sektor digitaler Dienste und Infrastrukturen hat staatliche Informationssicherheitsregulierung nur dann Erfolg, wenn sich Private für die damit verfolgten Ziele einsetzen.[6] Wie beschrieben verlässt der Gesetzgeber insoweit mehr und mehr den Weg informeller Kooperation.

---

[3] Dazu oben § 4 I. 3. b) und § 4 II. 3.

[4] Zur abwehrrechtlichen Funktion der Grundrechte grundlegend *M. Sachs*, in: K. Stern, Das Staatsrecht der Bundesrepublik Deutschland, Bd. III/1, 1988, § 66; *ders.*, Abwehrrechte, in: Merten/Papier (Hrsg.), Bd. 2, 2006, § 39; *W. Cremer*, Freiheitsgrundrechte, 2003, S. 74 ff.; *Poscher*, Grundrechte als Abwehrrechte, 2003; *M. Borowski*, Grundrechte als Prinzipien, 2007, S. 222 ff.

[5] Zur ambivalenten Rolle des Staates als Garant und als Gefährder der Informationssicherheit bereits oben § 1 III.

[6] Dazu ebenfalls bereits oben § 1 IV.

Stattdessen reagiert er mit Normen wie Art. 32 DSGVO auf die Informationssicherheitskrise. Danach sind Verarbeiter personenbezogener Daten verpflichtet, unter Berücksichtigung des Stands der Technik geeignete technische und organisatorische Maßnahmen zu treffen, um die Sicherheit der ihnen anvertrauten Daten zu gewährleisten. Entsprechend geht der Gesetzgeber vor, wenn er Systembetreibern gegenüber Informations- und Meldepflichten bei IT-Sicherheitsvorfällen anordnet, Zertifizierungen verlangt oder sie für Zwischenfälle in Haftung nimmt.[7]

Der Gesetzgeber kommt mit diesen und weiteren Normen unter anderem seiner objektiv-rechtlichen Verpflichtung zum Schutz des Grundrechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) bzw. auf Datenschutz (Art. 8 GRCh) der betroffenen Kunden nach.[8] Aus abwehrrechtlicher Sicht greifen derartige Vorgaben jedoch in unternehmerische Freiheiten ein, insbesondere in die Berufsfreiheit (Art. 15 GRCh bzw. Art. 12 GG[9]), sind also rechtfertigungsbedürftig.[10] Gleiches gilt mit Blick auf die als

[7] Zur Einordnung des Art. 32 DSGVO und analoger Vorschriften in die Ordnungsstruktur des Informationssicherheitsrechts ausführlich unten § 6 II.

[8] Dazu sogleich unter § 5 II. Zum Unionsrecht näher unten § 5 Fn. 178.

[9] Die folgenden Ausführungen orientieren sich in erster Linie an den Grundrechten des Grundgesetzes. Diese sind zwar gegenüber den Unionsgrundrechten regelmäßig nur nachrangig anwendbar, vgl. BVerfG 152, 152 (179 ff., Rn. 63 ff.); 152, 216 (233 ff., Rn. 42 ff.). Da sich zwischen GG und GRCh beim Schutz der hier einschlägigen Grundrechte keine relevanten Wertungsunterschiede auftun und da die deutsche Grundrechtsdogmatik für verschiedene einschlägige Konstellationen ein besonders ausdifferenziertes Instrumentarium entwickelt hat, liegt das hiesige Vorgehen – auch im Lichte von Art. 52 Abs. 4 GRCh – jedoch nahe. Vgl. ähnlich *Krönke*, Öffentliches Digitalwirtschaftsrecht, 2020, S. 70 Fn. 175. Ebd. auch der zutreffende Hinweis, dass sich aus der Eigentumsfreiheit (Art. 17 GRCh; Art. 14 Abs. 1 GG) keine gegenüber der Berufsfreiheit weitergehenden Anforderungen ergeben dürften. Zum Verhältnis von Berufs- und Eigentumsfreiheit zueinander auch mit Blick auf die Unionsgrundrechte siehe weiter *T. Wischmeyer/E. Herzog*, Daten für alle?, NJW 2020, S. 288 (289 ff.). Zur EMRK, für die sich ein Schutz der Berufsfreiheit nur mittelbar über Art. 8 EMRK herleiten lässt, näher *C. Grabenwarter/K. Pabel*, Europäische Menschenrechtskonvention, 7. Aufl. 2021, § 25 Rn. 37 ff.

[10] *Christoph Krönke* hat jüngst Tendenzen im rechtswissenschaftlichen Schrifttum kritisiert, die Eingriffen in die Berufsfreiheit digitalwirtschaftlicher Unternehmen ein verhältnismäßig geringes Gewicht attestieren wollen, weil die digitale Technik und insbesondere deren ökonomisch motivierte Nutzung inhärent „riskant" sei; dem Gesetzgeber würden hier unter dem Gesichtspunkt der Vorsorge zu große Spielräume eingeräumt, vgl. *Krönke*, Öffentliches Digitalwirtschaftsrecht, 2020, S. 38 ff., unter kritischem Verweis auf u. a. *U. Di Fabio*, Grundrechtsgeltung in digitalen Systemen, 2016, S. 90 ff.; *Hoffmann-Riem*, Innovation und Recht – Recht und Innovation, 2016, S. 670 ff.; *ders.*, Schutz der natürlichen und der gesellschaftlichen Umwelt, EurUP 16 (2018), S. 2 (4 ff.); *M. Martini*, Blackbox Algorithmus, 2019, S. 113 ff. Zu entsprechenden dogmatischen Konsequenzen des Risikorechts siehe bereits oben § 4 I. 2. b). Dagegen mahnt *Krönke*, a. a. O., S. 42 ff., einen „ausgewogeneren" Ansatz an, der konkrete Risikozusammenhänge belegt und der auch angesichts der real durch die Digitalwirtschaft geschaffenen Risiken die grundrechtlich radizierten Interessen der Unternehmen nicht aus dem Blick verliert. Angesichts der auch von *Krönke* konstatierten relati-

Beschränkungsverbote wirkenden Grundfreiheiten des Unionsrechts, die zu den Grundrechten allgemein in einem Spezialitätsverhältnis stehen.[11]

Bei der grundrechtlichen Bewertung derartiger regulatorischer Vorgaben zur Informationssicherheit, die im Lichte der hergebrachten „Stufen"-Dogmatik als Eingriffe in die Berufsausübungsfreiheit zu qualifizieren sind,[12] müssen folgende übergreifende Aspekte berücksichtigt werden.

aa) Systemische Natur und Kaskadeneffekte von IT-Sicherheitsrisiken

Trotz der hohen Bedeutung, die der Berufsfreiheit generell für eine freiheitliche, auf der Selbstverantwortung der Einzelnen aufbauende Wirtschaftsverfassung zukommt[13] und die selbstverständlich auch für die Digitalwirtschaft als Motor künftiger Wettbewerbsfähigkeit und als „Wohlstandstreiber" in Anschlag zu bringen ist,[14] zieht die Rechtsprechung gesetzlichen Maßnahmen zur Wirtschaftsregulierung traditionell keine engen Grenzen.[15] So reicht es bekanntlich zur Rechtfertigung von Berufsausübungsregelungen aus, wenn sich

ven Schwäche des Schutzgehalts von Art. 12 GG und des hohen Rangs der verfassungsrechtlichen Gegeninteressen, allen voran des Rechts auf informationelle Selbstbestimmung, dürften die praktischen Effekte der von *Krönke* angeregten Perspektivverschiebung jedoch sehr gering sein.

[11] Letztere entfalten für die hier untersuchte Konstellation keine besondere Prägekraft und werden daher im Folgenden weitgehend ausgeblendet. Zum Konkurrenzverhältnis näher *T. Mann*, in: Sachs, GG, 9. Aufl. 2021, Art. 12 Rn. 9 f.; *M. Ruffert*, in: Epping/Hillgruber, BeckOK GG, 48. Ed. 15.8.2021, Art. 12 Rn. 6. Siehe zum Verhältnis der Grundfreiheiten zu Art. 15 Abs. 2 GRCh jetzt auch EuGH, C- 230/18 v. 8.5.2019, Rn. 52 ff. – PI/Landespolizeidirektion Tirol.

[12] Vgl. hierzu umfassend *M. Burgi*, in: BK GG, Art. 12 (2019) Rn. 37 ff., 122 ff., 184 ff. Unter den der Berufsfreiheit zugeordneten Teilgehalten dürften entsprechende Regelungen regelmäßig die „Unternehmerfreiheit" berühren (siehe auch Art. 16 GRCh), vgl. *Burgi*, a. a. O., Rn. 46; siehe weiter BVerfGE 50, 290 (363 f.). Die Abgrenzung der „drei Stufen" ist bekanntlich alles andere als eindeutig; Schwierigkeiten bereitet es insbesondere, wenn Berufsausübungsregelungen faktisch als Berufswahlbeschränkungen wirken (vgl. BVerfGE 30, 292 [313]). Bei Vorgaben zur Informationssicherheit ist allerdings kaum zu befürchten, dass diese den Marktzutritt behindern, da ein eigenständiger Markt für „unsichere" Produkte nicht besteht.

[13] Vgl. nur BVerfGE 32, 311 (317); siehe weiter auch *R. Schmidt*, Staatliche Verantwortung für die Wirtschaft, in: Isensee/Kirchhof (Hrsg.), HStR, Bd. IV, 3. Aufl. 2006, § 92 Rn. 22 f.; *M. Ruffert*, in: Epping/Hillgruber, BeckOK GG, 48. Ed. 15.8.2021, Art. 12 Rn. 12; *T. Mann*, in: Sachs, GG, 9. Aufl. 2021, Art. 12 Rn. 22, je m. w. N.

[14] Dazu ausführlich *Krönke*, Öffentliches Digitalwirtschaftsrecht, 2020, S. 59 ff.: „digitalwirtschaftliche Wohlstandsvorsorge" als Staatsziel, in Anlehnung an *M. Burgi*, Wohlstandsvorsorge als Staatsziel und als Determinante im Wirtschaftsverwaltungsrecht, AöR Beiheft 2014, S. 30 ff.

[15] Vgl. nur *F. Hufen*, Berufsfreiheit – Erinnerung an ein Grundrecht, NJW 1994, S. 2913 ff.; *Burgi*, in: BK GG, Art. 12 (2019) Rn. 201, 234 ff. Für das Unionsrecht entsprechend *H. Jarass*, in: Jarass, GRCh, 4. Aufl. 2021, Art. 16 Rn. 29; *J. Schwarze/P. Voet van Vormizeele*, in: Schwarze, EU-Kommentar, 4. Aufl. 2019, Art. 16 GRCh Rn. 2; *M. Ruffert*, in: Calliess/Ruffert, EUV/AEUV, 6. Aufl. 2022, Art. 15 GRCh Rn. 17.

Regelungen auf „vernünftige Erwägungen des Gemeinwohls" stützen können.[16] Diese Hürde werden Maßnahmen zur Hebung des Informationssicherheitsniveaus in aller Regel nehmen können. Es besteht auch kein Anlass, die viel konstatierten Schwächen der Stufen-Lehre durch Modifikationen der Anforderungen an die Rechtfertigung zu beheben,[17] weil die hiesigen Vorgaben auch im Ergebnis nicht annähernd das Gewicht von Berufswahlregelungen erreichen. Besonders weit reichen die gesetzlichen Eingriffsmöglichkeiten dort, wo die Wirkungen des abwehrrechtlich geschützten Handelns „weit über das wirtschaftliche Schicksal des eigenen Unternehmens hinausreichen".[18] Dieses Kriterium wird herkömmlich für regulatorische Vorgaben gegenüber Großunternehmen herangezogen.[19] Angesichts der systemischen Natur von IT-Sicherheitsrisiken und der Kaskadeneffekte, die IT-Zwischenfälle nach sich ziehen können,[20] dürfte es im Falle von Regeln zur Informationssicherheit Eingriffe gegenüber allen Unternehmen der Digitalwirtschaft legitimieren können.

bb) Mangelnde IT-Sicherheit kein Ausdruck privater Macht

Geringe Relevanz für das Informationssicherheitsrecht hat hingegen die – in der Literatur überwiegend zustimmend aufgenommene – Tendenz der jüngeren Rechtsprechung, die Regulierung von Digitalunternehmen über die Figur der mittelbaren Drittwirkung zu begründen.[21] Zwar sind viele digitale Märkte durch marktmächtige Akteure geprägt, die ihren Nutzern, auch im Bereich essentieller Dienstleistungen, einseitig Bedingungen diktieren können.[22] Daraus lässt sich zwar keine unmittelbare Grundrechtsbindung der Unternehmen ableiten, doch ist es plausibel, dass Gesetzgeber und Rechtsprechung den grundrechtlichen Interessen der Nutzer in solchen Fällen besonders Rechnung tragen müssen.[23] Allerdings wirkt sich die mittelbare Grundrechtsbindung der

[16] Grundlegend BVerfGE 7, 377 (405).

[17] Vgl. dazu gleich in § 5 Fn. 26.

[18] Grundlegend BVerfGE 50, 290 (363).

[19] *Burgi*, in: BK GG, Art. 12 (2019) Rn. 101 ff.

[20] Dazu oben § 4 II. 2. c).

[21] So – in Weiterführung der Ansätze in BVerfGE 128, 226 (249, Rn. 59); 148, 267 (280 f., Rn. 32 ff.) – BVerfG (K), NJW 2019, 1935, Rn. 15; BGH, NJW 2021, 3179, Rn. 64. Aus der Literatur zur jüngsten Drittwirkungsrechtsprechung siehe nur *A. Hellgardt*, Wer hat Angst vor der unmittelbaren Drittwirkung?, JZ 73 (2018), S. 901 ff.; *F. Michl*, Situativ staatsgleiche Grundrechtsbindung privater Akteure, JZ 73 (2018), S. 910 ff.; umfassend jetzt *A. Kulick*, Horizontalwirkung im Vergleich, 2020, S. 407 ff. und passim.

[22] Ausführlich *Krönke*, Öffentliches Digitalwirtschaftsrecht, 2020, S. 50 f. Vgl. zusammenfassend BVerfGE 152, 152 (185, Rn. 77): „Dabei können insbesondere auch die Unausweichlichkeit von Situationen, das Ungleichgewicht zwischen sich gegenüberstehenden Parteien, die gesellschaftliche Bedeutung bestimmter Leistungen oder die soziale Mächtigkeit einer Seite eine maßgebliche Rolle spielen".

[23] Zu den insoweit vertretenen Auffassungen zuletzt ausführlich BGH NJW 2021, 3179 (3185, Rn. 59).

Digitalunternehmen dort besonders aus, wo diese Unternehmen den Zugang zu quasi-öffentlichen Kommunikationsinfrastrukturen beherrschen. Die Verwundbarkeit ihrer Dienste oder Netze ist demgegenüber – ungeachtet der damit einhergehenden systemischen Risiken – gerade kein Zeichen von sozialer oder ökonomischer Macht, sondern Ausdruck technologischer Schwäche. Gewiss kann die unzureichende Investition in sichere IT als Entscheidung für ein „billigeres" und damit möglicherweise kurzfristig profitableres Geschäftsmodell, mithin als Ausdruck ökonomischer Freiheit interpretiert werden. Doch beruht die spezifische Gefährdungssituation der Nutzer, die Anlass und Grund für Informationssicherheitsregulierung ist, nicht auf der überlegenen Stellung des Digitalunternehmens; befürchtet wird vielmehr, dass dieses mitsamt seinen Nutzern bei einer unzureichenden Absicherung den Angriffen Dritter ausgeliefert ist. Dass ein Angriff auf Monopolisten für Angreifer gerade aufgrund ihrer Marktmacht faktisch besonders attraktiv sein kann, ändert daran nichts. Die an die mittelbare Grundrechtsbindung Privater anknüpfenden Rechtsfiguren finden daher im vorliegenden Kontext keine Anwendung.[24]

cc) Informationssicherheitsregulierung kein Eingriff in den Kernbereich der Digitalwirtschaft

Umgekehrt lässt sich zugunsten der Digitalunternehmen nicht ins Felde führen, dass informationssicherheitsrechtliche Vorgaben wie Meldepflichten oder Zertifizierungsregime in den Kernbereich ihres technologisch getriebenen Geschäftsmodells eingreifen und daher einer tendenziell strengeren Kontrolle unterliegen. Zwar wird zu Recht angemahnt, bei der Auslegung der Schutzgarantien die tatsächlichen Kontexte der Berufsausübung zu berücksichtigen.[25] Denn nicht jede Ausübungsregelung beeinträchtigt die davon je erfassten Berufe in gleicher Weise.[26] Im Falle der Digitalwirtschaft legt dies nahe, dem Gesetzgeber dort engere Grenzen zu ziehen, wo seine Regulierung an den Kernbereich spezifisch digitaler Geschäftsmodelle rührt – etwa die Plattformisierung, die Automatisierung von Prozessen durch Einsatz intelligenter Systeme oder auch die Durchführung von Big Data-Analysen.[27] Unabhängig davon,

[24] Zu diesen ausführlich *Krönke*, Öffentliches Digitalwirtschaftsrecht, 2020, S. 77 ff.

[25] Allgemein *R. Breuer*, Freiheit des Berufs, in: Isensee/Kirchhof (Hrsg.), HStR, 3. Aufl. 2010, § 170 Rn. 49 ff.

[26] In diesem Sinne etwa BVerfGE 11, 30 (42 ff.); 103, 172 (184, Rn. 33).

[27] Speziell mit Blick auf die Digitalisierung *Burgi*, in: BK GG, Art. 12 (2019) Rn. 46, 54 ff.; ausführlich auch *Krönke*, Öffentliches Digitalwirtschaftsrecht, 2020, S. 82 ff., u. a. mit dem jedenfalls faktisch sicherlich zutreffenden Hinweis, dass den „Anbieter eines cloudbasierten intelligenten Medizinprodukts […], das aufgrund seiner Funktionalitäten wesensmäßig auf die Verarbeitung großer Bestände personenbezogener Informationen angewiesen ist, datenschutzrechtliche Beschränkungen ungleich härter [treffen] als ein herkömmliches Unternehmen, für das die Beachtung des Datenschutzrechts nur einen Begleitumstand der beruflichen Tätigkeit bildet".

wie weit dieses Argument trägt, ist für das Informationssicherheitsrecht jedoch festzuhalten, dass die daraus resultierenden Pflichten nicht in diesen Zusammenhang gehören. Das Betreiben unsicherer Dienste oder Netze ist kein (digitales) Geschäftsmodell. Und die Pflicht, in IT-Sicherheit zu investieren, stellt keinen Eingriff in den eigentlichen Inhalt der unternehmerischen Tätigkeit dar, sondern betrifft lediglich Begleitumstände der Berufsausübung. Im Gegenteil gilt, um eine Formulierung des Bundesverfassungsgerichts aus der Vorratsdatenspeicherungsentscheidung aufzunehmen, dass Digitalunternehmen gerade in Sachen IT-Sicherheit „ohnehin ein hohes Maß an Technikbeherrschung" zeigen müssen.[28] Insoweit Maßnahmen zur Erhöhung der Informationssicherheit also in den Bereich ihrer ureigenen technischen Expertise fallen, spricht dies dagegen, dem Eingriff ein besonders hohes Gewicht zuzuerkennen.

dd) Zwischenfazit

All das bedeutet nicht, dass die Berufsausübungsfreiheit bei der Gestaltung des Informationssicherheitsrechts ignoriert werden kann. Die Verhältnismäßigkeit konkreter Maßnahmen wie Meldepflichten muss sich vielmehr stets auch an Art. 12 GG bzw. Art. 15 und 16 GRCh messen lassen. Doch dürften sich aus der Berufsausübungsfreiheit über das allgemeine rechtsstaatliche Gebot nach verhältnismäßiger und bestimmter bzw. normenklarer Rechtsetzung für das Informationssicherheitsrecht kaum weitergehende Impulse ergeben.

b) Schutz der Privatheitsinteressen Dritter

Vorgaben zur Informationssicherheit – etwa in Gestalt von technischen und organisatorischen Sicherungs- oder Meldepflichten – berühren jedoch nicht nur das unternehmerische Tätigwerden. Sie stehen insbesondere auch in einem komplexen Wechselverhältnis zum Recht der davon mittelbar betroffenen Dritten auf Privatheit.[29] Denn aus technischer Sicht lässt sich Datensicherheit vielfach nur durch Verarbeitung von personenbezogenen Daten, also auf Kosten des Datenschutzes, herstellen.[30, 31] Verpflichtet der Staat private Dritte zu

[28] BVerfGE 125, 260 (361, Rn. 300).

[29] Zum verfassungsrechtlichen Schutzgut der Privatheit sogleich in § 5 Fn. 38.

[30] Dazu allgemein näher *G. Schneider*, Some Thoughts on Harming Privacy by Protecting Critical Infrastructures, in: Gander/Perron et al. (Hrsg.), Resilienz in der offenen Gesellschaft, 2012, S. 133 ff.; *K. Einzinger*, Keine Cyber-Sicherheit ohne Datenschutz, DuD 39 (2015), S. 723 ff.; *M. Martini*, in: B. Paal/D. Pauly (Hrsg.), DS-GVO, 3. Aufl. 2021, Art. 32 Rn. 1b, 59a; *M. Hansen*, in: S. Simitis/G. Hornung/I. Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 32 DSGVO Rn. 11; *Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022, Rn. 194 f. Vertiefend: *F. Voskamp*, Datenschutz, in: Kipker (Hrsg.), Cybersecurity, 2020, Kap. 5; *L. Schulte/T. Wambach*, Zielkonflikte zwischen Datenschutz und IT-Sicherheit im

einer solchen Datenverarbeitung,[32] stellt dies nach allgemeinen Regeln einen mittelbaren Grundrechtseingriff in die Rechte der von der Verarbeitung betroffenen Endnutzer dar.[33] Je nach Konstellation sind Art. 10 GG oder das Recht auf informationelle Selbstbestimmung bzw. im Unionsrecht Art. 7 und 8 GRCh betroffen.[34]

Auf die genauen Gehalte der genannten Grundrechtsgarantien und ihr Verhältnis zueinander wird gleich ausführlich einzugehen sein.[35] An dieser Stelle ist nur hervorzuheben, dass der Staat durch den Eingriff in die genannten Grundrechte regelmäßig zugleich seiner Gewährleistungsverantwortung für eben diese Grundrechte nachkommt.[36] Das Spannungsverhältnis von Daten-

---

Kontext der Aufklärung von Sicherheitsvorfällen, DuD 2020, S. 462 ff.; *S. Jandt*, IT-Sicherheit als Mittel und als Bedrohung des Datenschutzes, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 17. Siehe auch instruktiv aus der Perspektive der IT-Sicherheitsforschung *A. Böken*, IT-Sicherheitsforschung, in: Kipker (Hrsg.), Cybersecurity, 2020, Kap. 15 Rn. 2 ff.

[31] Konkret zeigt sich das Spannungsfeld in ganz unterschiedlichen Konstellationen. Um hier sechs Fälle herauszugreifen: (i) So fallen etwa bei Meldungen über IT-Sicherheitsrisiken im Sinne des § 4b Abs. 1 BSIG regelmäßig sowohl personenbezogene Daten der Meldenden als auch personenbezogene Daten Dritter an, etwa deren IP-Adressen, Protokoll-Daten, Informationen über Domains, Passwörter etc., die das BSI als zuständige Behörde verarbeiten muss, vgl. *Keppeler*, in: Ritter (Hrsg.), Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2022, § 4b BSIG Rn. 201. (ii) Auch die Information der Opfer von Cyberangriffen durch das BSI setzt voraus, dass sich die Behörde die (Bestands-)Daten der zu Informierenden verschafft und diese anschließend weiter verarbeitet, vgl. hierzu § 5c BSIG (dazu näher unten § 6 II. 3. e] und f]). (iii) Zur Ermächtigung der Telekommunikationsdiensteanbieter, zum Zwecke einer Erhöhung der IT-Sicherheit Kundendaten zu verarbeiten siehe unten § 6 Fn. 199. (iv) Zahlreiche technische Verfahren zur IT-Sicherheit, insbes. auch die in § 8a Abs. 1a BSIG und § 165 Abs. 3 TKG geforderten „Systeme zur Angriffserkennung" (dazu näher § 6 II. 5. b]) basieren auf einer teils intensiven Auswertung personenbezogener Daten, vgl. *Schulte*, in: Ritter (Hrsg.), Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2022, § 8a BSIG Rn. 470 f. (v) Soweit das BSI nach § 8a Abs. 4a BSIG von KRITIS-Betreibern bei erheblichen Sicherheitsvorfällen alle notwendigen Informationen herausverlangen kann, umfasst dies regelmäßig auch personenbezogene Daten in Gestalt von IP-Adressen, E-Mails etc. (vi) Auch der Informationsaustauch in CERT-Netzwerken, die für die Implementierung von Cybersicherheitsvorgaben eine zentrale Bedeutung haben (vgl. § 6 II. 8. b]), ist datenschutzrechtlich relevant, vgl. nur *K. Einzinger/F. Skopik*, Über die datenschutzrechtliche Problematik in CERTs/CSIRTs-Netzwerken, DuD 41 (2017), S. 572 ff.

[32] Zur sicherheitspolitischen Dimension derartiger Verpflichtungen siehe oben § 4 II. 1. b).

[33] BVerfGE 107, 299 (313, Rn. 50); 125, 260 (310, Rn. 190).

[34] Zur Kontroverse um § 100 TKG a. F. (Recht der Diensteanbieter zur Verarbeitung von Bestands- und Verkehrsdaten der Teilnehmer und Nutzer, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen; entspricht weitgehend § 12 TTDSG) siehe *A. Roßnagel*, Das IT-Sicherheitsgesetz, DVBl. 2015, S. 1206 (1211 f.); *Ritter*, in: ders. (Hrsg.), Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2022, Teil 1 Rn. 48.

[35] Dazu unter § 5 I. 2.

[36] Hierzu § 5 II. Entsprechend zählt der Schutz der „Integrität und Vertraulichkeit" personenbezogener Daten auch einfachrechtlich zu den datenschutzrechtlichen Grundsätzen der Verarbeitung im Sinne von Art. 5 Abs. 1 lit. f DSGVO.

schutz und Datensicherheit ist also aus verfassungsrechtlicher Sicht in erster Linie eine interne Spannungslage innerhalb des Datenschutzes, die nicht durch eindeutige Vorrangregeln, sondern allein nach den Regeln des schonenden Ausgleichs bewältigt werden kann (vgl. etwa §§ 5 Abs. 7, 8a; 7c Abs. 1 S. 5, Abs. 4; 8b Abs. 7 BSIG; § 12 Abs. 1 TTDSG). Durch technische Lösungen kann die Spannungslage zwar punktuell reduziert, aber kaum je gänzlich beseitigt werden.

2. Abwehrrechte gegen Maßnahmen zur Senkung des Informationssicherheitsniveaus

Weit engere Grenzen ziehen die Grundrechte staatlichem Handeln demgegenüber, wenn dieses IT-Schwachstellen ausnutzt oder gar aktiv das Informationssicherheitsniveau senkt. Solche staatlichen Maßnahmen haben potenziell Auswirkungen auf alle möglichen Grundrechte, da grundrechtlich relevantes Handeln heute in zahlreichen Bereichen von der Vertraulichkeit, Verfügbarkeit und Integrität der dafür genutzten informationstechnischen Systeme abhängig ist.[37] Wenn der Schutz gegen staatliche Maßnahmen zur Schwächung der IT-Sicherheit dennoch in erster Linie im Lichte jener Grundrechte diskutiert worden ist, die sich dem verfassungsrechtlichen Schutz der Privatheit zuordnen lassen,[38] hat dies seinen Grund darin, dass staatliche Eingriffshandlungen jedenfalls bisher vor allem darauf zielen, den Schutz der Vertraulichkeit von IT-Systemen auszuhebeln. Entsprechende Befugnisse, etwa die Ermächti-

[37] Dazu bereits oben § 1 I. Siehe auch weiter unten bei § 5. I. 3. Illustrierend *Poscher/Lassahn*, Verfassungsrechtliche Dimensionen der IT-Sicherheit, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 7 Rn. 37: „Die geschützten Belange können dabei so mannigfaltig sein wie der weite Kreis aller IT-gestützten gesellschaftlichen oder privaten Vorgänge und Abläufe selbst: Wo IT-Systeme etwa Beatmungsmaschinen in Krankenhäusern steuern, ist das Recht auf Leben und körperliche Unversehrtheit betroffen (Art. 2 Abs. 2 S. 1 GG); wo politische Demonstrationen über Messaging-Dienste oä koordiniert werden, kann es auch unabhängig von der Erfassung personenbezogener Daten – etwa bei einem rein physischen Einwirken auf die Server – um das Recht auf Versammlungsfreiheit (Art. 8 GG) gehen, usw."

[38] Zum verfassungsrechtlichen Schutzgut der Privatheit, insbes. im Kontext staatlicher Eingriffe, näher *H.-D. Horn*, Schutz der Privatsphäre, in: Isensee/Kirchhof (Hrsg.), HStR, Bd. VII, 3. Aufl. 2009, § 149; *M. Nettesheim*, Grundrechtsschutz der Privatheit, in: VVDStRL 70 (2011), S. 7 ff.; *Schwabenbauer*, Heimliche Grundrechtseingriffe, 2013, S. 90 ff.; *Hauck*, Heimliche Strafverfolgung und Schutz der Privatheit, 2014, S. 84 ff.; *C. Gusy/J. Eichenhofer/L. Schulte*, e-privacy, JöR 64 (2016), S. 385 ff.; *Eichenhofer*, e-Privacy, 2021, S. 9 ff. Zur Fundierung der Privatheitsgarantie der einzelnen Grundrechte im Schutz der Menschenwürde, insbes. mit Blick auf Art. 10 GG: BVerfGE 67, 157 (171); 110, 33 (53, Rn. 105); 113, 348 (391, Rn. 162); 115, 166 (182, Rn. 64); 143, 1 (10, Rn. 35).

gung zur Durchführung einer „Quellen-TKÜ“,[39] finden sich dementsprechend vor allem im Sicherheitsrecht – jenem Komplex aus Regelungen des Gefahrenabwehrrechts, des Strafrechts und des Rechts der Nachrichtendienste, dessen gemeinsame Ausrichtung auf das verfassungsrechtliche Schutzgut Sicherheit und auf das praktische Ziel der Informationsgewinnung hier bereits dargestellt wurde.[40] Der Kreis der somit unmittelbar angesprochenen Grundrechte umfasst neben dem Telekommunikationsgeheimnis (a.) und dem Wohnungsgrundrecht (b.) insbesondere auch das allgemeine Persönlichkeitsrecht in seinen Ausprägungen als Recht auf informationelle Selbstbestimmung und als Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (c.).

a) Schutz der Vertraulichkeit und Integrität der Telekommunikation

Telekommunikation ist das Rückgrat der digitalen Gesellschaft.[41] Dank Mobilisierung und Miniaturisierung sind Telekommunikationstechnologien heute in immer mehr Lebenskontexte eingebettet.[42] Konnte das BVerfG vor einiger Zeit noch behaupten, dass private Kommunikation primär eine Wohnung und

[39] Einen Überblick über die einschlägigen Maßnahmen bieten *M. Heinemann*, Schutz informationstechnischer Systeme, 2015, S. 82 ff.; *K. Graulich*, Das Handeln von Polizei- und Ordnungsbehörden zur Gefahrenabwehr, in: Lisken/Denninger, HdbPolR, 7. Aufl. 2021, Kap. E Rn. 794 ff.

[40] Zur Charakterisierung dieses „Rechtsgebiets“ siehe oben § 4 Fn. 4. Spezifisch zur Wissensabhängigkeit der Materie *B. Rusteberg*, Wissensgenerierung in der personenbezogenen Prävention, in: Münkler (Hrsg.), Dimensionen des Wissens im Recht, 2019, S. 233 ff.

[41] Telekommunikation im grundrechtlichen Sinne bezeichnet nach herrschendem Verständnis die Übermittlung von Informationen durch unkörperliche Signale an individuelle Empfänger; ebenso wie im Telekommunikationsrecht (vgl. § 3 Nr. 60 und § 3 Nr. 65 TKG) kommt es nicht auf die Technik der Signalübermittlung – über Kabel, Funk oder Satellit, durch mobile, feste oder paketvermittelte Netze etc.– an, vgl. zuletzt BVerfGE 125, 260 (309, Rn. 189); 130, 151 (179, Rn. 111); 155, 119 (168, Rn. 98). Der Begriff ist technologieneutral bzw. „entwicklungsoffen“, vgl. BVerfGE 115, 166 (182 f., Rn. 67); *T. Groß*, in: Friauf/Höfling, GG, Art. 10 (2016), Rn. 15; *A. Guckelberger*, in: Schmidt-Bleibtreu/Hofmann/Henneke, GG, 15. Aufl. 2022, Art. 10 Rn. 20; *W. Durner*, in: Dürig/Herzog/Scholz, GG, Art. 10 (2020), Art. 10 Rn. 64, 108; *M. Martini*, in: v. Münch/Kunig, GG, 7. Aufl. 2021, Art. 10 Rn. 26, 63. Auch der IP-basierte Datenaustausch über das Internet ist von Art. 10 GG geschützt, BVerfG (K), NJW 2016, 3508, Rn. 34. Zur Entwicklung des Telekommunikationsbegriffs allgemein, der den Fernmeldebegriff weitgehend abgelöst hat (selbst das BVerfG bezeichnet heute das Fernmeldegeheimnis des Art. 10 GG als Telekommunikationsgeheimnis, vgl. zuletzt BVerfGE 155, 119 [168, Rn. 98]), *B. Schneider*, Fernmeldegeheimnis und Fernmeldeaufklärung, 2020, S. 23 f.; *M. Ogorek*, in: Epping/Hillgruber, BeckOK GG, 48. Ed. 15.8.2021, Art. 10 Rn. 35; kritisch *W. Durner*, in: Dürig/Herzog/Scholz, GG, Art. 10 (2020), Art. 10 Rn. 108.

[42] Dazu nur L. Floridi (Hrsg.), The Onlife Manifesto, 2015; *Hildebrandt*, Smart Technologies and the End(s) of Law, 2016, S. 41 ff., 77 ff., 263 ff. Frühzeitig hierzu BVerfGE 107, 299 (319, Rn. 68 f.).

nur sekundär Telekommunikationsmittel voraussetzt,[43] stellt sich dies heute – nicht zuletzt unter Pandemiebedingungen – anders dar.[44]

Die Nutzung von Telekommunikationsdiensten erhöht die individuellen Handlungsoptionen erheblich. Preis dafür ist, dass die Nutzer die Kontrolle über ihre Kommunikation partiell abgeben müssen. Hierdurch entstehen Risiken für die Privatheit, auf die die Grundrechtekataloge mit Vertraulichkeitsgarantien reagiert haben. Neben Art. 10 GG tritt der – seinerseits eng an Art. 8 Abs. 1 EMRK angelehnte – Art. 7 GRCh[45].[46] Für alle diese Garantien lässt sich in Anspruch nehmen, was das Bundesverfassungsgericht für Art. 10 GG formuliert hat: Sie sollen verhindern, dass Kommunikation unterbleibt oder nach Form und Inhalt verändert verläuft, weil die Beteiligten einen Zugriff Dritter fürchten.[47] In ihrer Funktion als klassische Abwehrrechte schützen Art. 10 GG bzw. Art. 7 GRCh die Beteiligten des Telekommunikationsvorgangs vor Eingriffen durch Hoheitsträger, etwa in Gestalt der Strafverfolgungsorgane

[43] So ausdrücklich BVerfGE 113, 348 (391, Rn. 163).

[44] Vgl. aber weiterhin BVerfGE 141, 220 (312 f., Rn. 238 f.).

[45] Art. 7 GRCh schützt zwar nicht wie Art. 8 Abs. 1 EMRK die „Korrespondenz", sondern die „Kommunikation", verfolgt damit jedoch einen identischen Schutzzweck, vgl. die Erläuterungen des Präsidiums zur Charta der Grundrechte, ABl. 2007/C 303, S. 17 (20). Der EuGH hat den Schutz der „Kommunikation" allerdings bisher nicht näher entfaltet, sondern Eingriffsmaßnahmen, die jedenfalls auch konkrete Kommunikationsvorgänge betrafen, vorrangig am Maßstab der von Art. 7 GRCh ebenfalls garantierten „Achtung des Privatlebens" sowie – ohne nähere Differenzierung der Schutzbereiche – an Art. 8 GRCh gemessen, vgl. EuGH, C- 293/12 u. a. v. 8.4.2014, Rn. 29 – Digital Rights Ireland; EuGH, Gutachten 1/15 v. 26.7.2017, Rn. 122 f. – PNR-Abkommen EU-Kanada; EuGH, C-207/16 v. 2.10.2018, Rn. 48 f. – Ministerio Fiscal; EuGH, C-311/18 v. 16.7.2020, Rn. 168 – Schrems II. Kritisch hierzu aus der Literatur *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 205 ff. Vgl. weiter sogleich unter § 5 I. 2. c) aa).

[46] Inwieweit Art. 10 GG neben den Unionsgrundrechten zur Anwendung kommt (vgl. dazu bereits oben § 5 Fn. 9), lässt sich nicht pauschal beantworten. Grund hierfür ist zum einen die unscharfe Abgrenzung zwischen allgemeinem Datenschutzrecht, das in Form der DSGVO weitgehend zwingende, also „vollvereinheitlichende" Vorgaben für die Mitgliedstaaten enthält, und dem in Form von Richtlinienrecht vorliegenden Telekommunikationsdatenschutz; dazu näher *European Data Protection Board*, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, 12.3.2019. Die Abgrenzung wird zum anderen durch die im Bereich des Sicherheitsrechts zunehmend extensive EuGH-Rechtsprechung erschwert, vgl. EuGH, C-203/15 v. 21.12.2016, Rn. 75 ff. – Tele2 Sverige; EuGH, C-207/16 v. 2.10.2018, Rn. 29 ff. – Ministerio Fiscal; EuGH, C-623/17 v. 6.10.2020, Rn. 44 ff. – Privacy International; EuGH, C-511/18 u. a. v. 6.10.2020, Rn. 99 ff.– La Quadrature du Net u. a. Dennoch selbstbewusst zur fortdauernden Relevanz des Art. 10 GG: BVerfGE 154, 152 (214 f., Rn. 84 f.); 155, 119 (163 ff., Rn. 85 ff.); *Durner*, in: Dürig/Herzog/Scholz, GG, Art. 10 (2020), Art. 10 Rn. 52; *Bäcker*, Sicherheitsverfassungsrecht, in: Herdegen/Masing et al. (Hrsg.), HVerfR, 2021, § 28 Rn. 129. In der Sache agieren EGMR, EuGH und BVerfG bei der Auslegung der jeweiligen Grundrechtsgarantien mittlerweile weitgehend synchron, sodass die Abgrenzungsproblematik in der Praxis meist dahinstehen kann.

[47] St. Rspr, vgl. BVerfGE 100, 313 (359, Rn. 162); 129, 208 (241, Rn. 198); 130, 151 (179, Rn. 111).

und sonstigen Sicherheitsbehörden.[48] Geschützt wird das Vertrauen in die Integrität des Übermittlungsakts, nicht jedoch das Vertrauen der Kommunikationspartner im Verhältnis zueinander.[49] Der Schutz endet nicht mit der Erhebung der Daten, sondern umfasst den gesamten Informationsverarbeitungszyklus (Speicherung, Verwendung, Übermittlung etc.). Jede Folgeverwendung von Informationen, die durch einen Eingriff in Art. 10 GG gewonnen wurden, muss somit erneut an Art. 10 GG gemessen werden.[50]

Die verfassungsrechtlich geschützten Räume werden naturgemäß auch zum Zwecke der Störung und Verletzung von Rechtsgütern genutzt. Für einzelne Delikte wie Kinderpornographie oder Hassrede hat sich die Digitalisierung als Brandbeschleuniger erwiesen. Entsprechenden Ermittlungs- und Bekämpfungsmaßnahmen sind nicht nur (grund-)rechtliche Grenzen gezogen; sie stoßen auch auf faktische Hindernisse, etwa wenn Kommunikationsumstände mit informationstechnischen Mitteln verschleiert oder Kommunikationsinhalte verschlüsselt werden. Um hier durchzudringen, ergänzt der Gesetzgeber das klassische Arsenal der Telefon- und Internetüberwachung in jüngerer Zeit um Ermächtigungsgrundlagen, die Schwachstellen der Informationssicherheit ausnutzen und den Zugriff auf für rechtswidrige Zwecke genutzte Zielsysteme ermöglichen. So gestatten etwa im Bundesrecht § 100a Abs. 1 S. 2 und 3 StPO sowie § 51 Abs. 2 BKAG den Behörden, zur Umgehung von sog. Ende-zu-Ende-Verschlüsselung auf den beteiligten Endgeräten Software zu installieren, die eine Überwachung der Telekommunikation an der „Quelle" ermöglicht.[51] Auf diese und zweckanaloge Maßnahmen wird noch einzugehen sein.[52] Hier ist zunächst nur hervorzuheben, dass sich solche Maßnahmen zur Manipulation der IT-Sicherheit auch am grundrechtlichen Telekommunikationsgeheimnis messen lassen müssen.[53] Gleiches gilt nach herrschendem Verständnis

[48] Grundrechtlicher, telekommunikationsrechtlicher und strafprozessualer Telekommunikationsbegriff sind nicht deckungsgleich, vgl. BVerfGE 124, 43 (55 f., Rn. 47); BVerfG (K), NJW 2016, 3508 (3509, Rn. 32); BGH, StB 47/20 v. 28.4.2021, Rn. 8 ff. Der telekommunikationsrechtliche Telekommunikationsbegriff umfasst seit der jüngsten Reform auch sog. Over-the-top-Kommunikationsdienste (OTT-Dienste) – internetbasierte Dienste zur interpersonellen Kommunikation wie Voice-over-IP (VoIP)-Telefonie, E-mail („Gmail") oder Instant-Messaging („WhatsApp") –, vgl. Art. 2 Nr. 4 lit. b und c, Nr. 5 Kodex-RL 2018/1972; § 3 Nr. 24, 61 TKG.

[49] BVerfGE 106, 28 (37, Rn. 23); 120, 274 (340 f., Rn. 290); 130, 151 (180, Rn. 114).

[50] BVerfGE 100, 313 (359, Rn. 163); 120, 274 (307, Rn. 184); 125, 260 (313, Rn. 196); 133, 277 (317, Rn. 95); 141, 220 (327, Rn. 285); 155, 119 (170, Rn. 101); BVerwG, NVwZ 2018, 731 (733, Rn. 24); *Durner*, in: Dürig/Herzog/Scholz, GG, Art. 10 (2020), Art. 10 Rn. 84.

[51] Zu Art. 10 GG als Maßstab für die Quellen-TKÜ siehe BVerfGE 120, 274 (309); 141, 220 (309, Rn. 228). Zu diesem Instrument ausführlich *F. Roggan*, Die strafprozessuale Quellen-TKÜ und Online-Durchsuchung, StV 2017, S. 821 ff.; *F. Freiling/C. Safferling/C. Rückert*, Quellen-TKÜ und Online-Durchsuchung, JR 2018, S. 9 ff.; *N. von zur Mühlen*, Zugriffe auf elektronische Kommunikation, 2019, S. 62 ff.

[52] Siehe hierzu unten § 7 I. und II.

[53] Zur Abgrenzung gegenüber Art. 2 I i.V.m. Art. 1 I GG gleich unter § 5 I. 2. c) aa).

für staatliche Beschränkungen der Möglichkeit, Eigenvorsorge zugunsten der Informationssicherheit zu betreiben, etwa in Form eines Verbots der Nutzung kryptographischer Verfahren, um den behördlichen Zugriff auf Kommunikation zu erleichtern.[54]

Für alle diese Eingriffe gilt unter dem Grundgesetz – abseits des nachrichtendienstlichen Kosmos – das allgemeine Schranken- und Rechtfertigungsregime des Art. 10 Abs. 2 S. 1 GG. Bei dessen Anwendung ist zu beachten, dass die Rechtsprechung verschiedene, zunächst oft für die Prüfung der Verhältnismäßigkeit von Eingriffen in das Grundrecht auf informationelle Selbstbestimmung entwickelte Vorgaben „sinngemäß auf die speziellere Garantie in Art. 10 GG übertragen" hat.[55] Die teils sehr detaillierten Vorgaben zur Bestimmtheit und Normenklarheit[56] sowie vor allem zur Verhältnismäßigkeit[57] der Eingriffsbestimmungen wirken für den Gesetzgeber wie qualifizierte Schranken-Schranken. Konkret orientiert sich der Schutzumfang an der Schwere des Eingriffs, die wiederum durch Merkmale wie Heimlichkeit und Streubreite sowie im Lichte der je gewählten Eingriffsschwellen bemessen wird.[58] Unbedingt zu schützen ist der Kernbereich.[59] Darüber hinaus gilt es, diverse organisations- und verfahrensrechtliche Schutzvorkehrungen zu beachten[60] – und eben auch dem Informationssicherheitsinteresse Rechnung zu tragen. Letzteres gilt laut BVerfG insbesondere dort, wo Private durch hoheitliche Vorgaben zur Datenspeicherung verpflichtet werden: In diesem Fall muss gewährleistet sein, dass,

[54] Einen Eingriff in Art. 10 GG bejahend insbes. *Groß*, in: Friauf/Höfling, GG, Art. 10 (2016), Rn. 70; *Ogorek*, in: Epping/Hillgruber, BeckOK GG, 48. Ed. 15.8.2021, Art. 10 Rn. 53; *Durner*, in: Dürig/Herzog/Scholz, GG, Art. 10 (2020), Art. 10 Rn. 71 ff., 117; *Martini*, in: v. Münch/Kunig, GG, 7. Aufl. 2021, Art. 10 Rn. 31, 103. Anders *C. Gusy*, in: Huber/Voßkuhle, GG, 8. Aufl. i. E., Art. 10 Rn. 66. Siehe auch *J. Gerhards*, (Grund-)Recht auf Verschlüsselung?, 2010, S. 139 ff., 269 ff.

[55] BVerfGE 100, 313 (359, Rn. 164); 124, 43 (60, Rn. 60); 125, 260 (310, Rn. 191); BVerwG, NVwZ 2018, 731 (733, Rn. 25).

[56] Dazu näher BVerfGE 110, 33 (53, Rn. 106); 113, 348 (375, Rn. 116); 125, 260 (328, Rn. 226); 130, 151 (202, Rn. 169).

[57] Hierzu umfassend BVerfGE 141, 220 (268 ff., Rn. 103 ff.); 154, 152 (239 ff., Rn. 141 ff.); 156, 11 (46, Rn. 89).

[58] Systematisierend BVerfGE 155, 119 (178 f., Rn. 129); siehe auch *Tanneberger*, Die Sicherheitsverfassung, 2014, S. 236 ff.; *T. Schwabenbauer*, Verfassungsrechtliche Vorgaben, in: Lisken/Denninger, HdbPolR, 7. Aufl. 2021, Kap. G II., Rn. 119 ff., 195 ff.

[59] Dazu näher BVerfGE 120, 274 (338 f., Rn. 280 ff.); 129, 208 (245 ff., Rn. 209 ff.); 141, 220 (305 ff., Rn. 215 ff.); 154, 152 (262 ff., Rn. 199 ff.) je m. w. N. Aus der Literatur siehe nur *J. Reichert*, Der Schutz des Kernbereichs, 2015; *C. Rottmeier*, Kernbereich privater Lebensgestaltung, 2017; *S. Schulenberg*, Der Schutz des Kernbereichs privater Lebensgestaltung, in: Scheffczyk/Wolter (Hrsg.), Linien der Rechtsprechung IV, 2017, S. 123 ff.; *Schwabenbauer*, Verfassungsrechtliche Vorgaben, in: Lisken/Denninger, HdbPolR, 7. Aufl. 2021, Kap. G II., Rn. 140 ff. Vertiefend zum Konzept *Bäcker*, Kriminalpräventionsrecht, 2015, S. 172 ff.

[60] Vgl. BVerfGE 100, 313 (359 ff., Rn. 163 ff.; 385 ff., Rn. 247 ff.); 124, 43 (70 ff., Rn. 91 ff.). Zur Rechtsprechung des EGMR vgl. die Nachweise bei BVerfGE 141, 220 (293 f., Rn. 172 ff.).

gemessen am jeweiligen Stand der Technik, ein besonders hohes Schutzniveau gewährleistet ist.[61] Hieran zeigt sich erneut die Bedeutung, die Informationssicherheit mit Blick auf den Schutz der Vertraulichkeit der Telekommunikationsbeziehungen hat. Die Judikatur des EuGH und des EGMR hat diesen Grad an Differenziertheit bisher nicht erreicht, verfolgt jedoch keinen grundsätzlich anderen Ansatz.

Insofern das Telekommunikationsgeheimnis einen Ausschnitt aus dem umfassenderen grundrechtlichen Schutz der Privatheit gewährleistet, ist es spezieller als das Recht auf informationelle Selbstbestimmung bzw. auf Privatheit und Datenschutz.[62]

b) Schutz des Zugangsbestimmungsrechts über die eigene Wohnung

Anders als im Falle des Telekommunikationsgeheimnisses betreffen staatliche Maßnahmen, die die Verfügbarkeit, Vertraulichkeit oder Integrität von IT-Systemen beeinträchtigen, nur unter bestimmten Bedingungen das von Art. 13 GG bzw. von den Parallelbestimmungen in Art. 8 Abs. 1 EMRK und Art. 7 GRCh geschützte Recht, über den physischen oder informationellen Zugang zu Gegenständen oder Vorgängen in der Wohnung zu entscheiden.[63] Nach allgemeinen Regeln liegt ein (Informations-)Eingriff in das Wohnungsgrundrecht vor, wenn im Zuge der hoheitlichen Informationsbeschaffung Beschränkungen überwunden werden, die gerade die Wohnung für derartige Zugriffe darstellt. Einen Katalog typischer Maßnahmen enthalten im Grundgesetz die Art. 13 Abs. 3 bis 5 GG. Für einen Eingriff ist dabei nicht erforderlich, dass staatliche Stellen eigene Überwachungstechnik in die Wohnung einbringen. Verschaffen sich Behörden etwa Zugriff auf den Computer eines Betroffenen, um die daran angeschlossenen Mikrofone zu manipulieren und Raumgespräche abzuhören, wird auch auf diese Weise der räumliche Privatheitsschutz,

---

[61] BVerfGE 125, 260 (325 ff., Rn. 221 ff.); 155, 119 (205, Rn. 188).

[62] BVerfGE 67, 157 (171); st. Rspr.

[63] In diesem Sinne zum Schutzgehalt von Art. 13 GG BVerfGE 103, 142 (150 f., Rn. 26); 109, 279 (309, Rn. 104; 325 f., Rn. 160 f.); 115, 166 (196, Rn. 114); 139, 245 (265, Rn. 56); 151, 67 (86, Rn. 53); 156, 63 (129, Rn. 228). Aus der Literatur *M. Herdegen*, in: BK GG, Art. 13 (1998) Rn. 1; *J. Berkemann*, in: Denninger et al., AK-GG, 3. Aufl. 2001, Art. 13 Rn. 21; *Papier*, in: Dürig/Herzog/Scholz, GG, Art. 13 (2014) Rn. 1; *J.-D. Kühne*, in: Sachs, GG, 9. Aufl. 2021, Art. 13 Rn. 7; *S. Kluckert*, in: Epping/Hillgruber, BeckOK GG, 48. Ed. 15.8.2021, Art. 13 Rn. 1; *P. Kunig/A. Berger*, in: v. Münch/Kunig, GG, 7. Aufl. 2021, Art. 13 Rn. 1. Zur Rechtsprechung des EGMR siehe die Zusammenstellung der maßgeblichen Entscheidungen in *European Court of Human Rights*, Guide on Article 8 of the European Convention on Human Rights, Stand 30.4.2022, IV. Rn. 409 ff. In der Rechtsprechung des EuGH spielt der Schutz der Wohnung, von Sonderkonstellationen abgesehen, bisher keine bedeutende Rolle.

den die Wohnung vermittelt, ausgehebelt.[64] Ein entsprechendes Vorgehen ist für die Behörden auch deswegen attraktiv, weil Grundrechtsberechtigte ihre Wohnungen immer seltener als informationelle Rückzugsräume verstehen und sich entsprechend verhalten. Stattdessen dient die Wohnung (auch) zur Nutzung vernetzter Systeme bzw. wird durch Installation von Smart-Home-Technologie und Sprachassistenzsystemen selbst vernetzt.[65] Der Trend zum „Home Office" erhöht das Risiko und stellt im Übrigen die etablierte und für die Dogmatik des Wohnungsgrundrechts zentrale Trennung von (Privat-) Wohnungen und Geschäftsräumen in Frage.[66] Darüber hinaus wird Art. 13 GG selbstverständlich relevant, wenn zur Installation von Überwachungssoftware auf den IT-Systemen der Betroffenen eine Wohnung betreten wird.[67]

Allerdings beeinträchtigt nicht jeder Zugriff auf ein IT-System, das sich in einer Wohnung befindet, das Wohnungsgrundrecht. Das BVerfG weist zurecht darauf hin, dass es aus Sicht der Behörden gerade beim Zugriff auf mobile Endgeräte schwer vorhersehbar und teils vom Zufall abhängt, ob sich das Gerät in einer Wohnung befindet, sodass Art. 13 Abs. 3 bis 6 GG Anwendung finden.[68] Hinzu kommt, dass ein derartiger Eingriff oftmals weder wohnungsspezifische Zugangshindernisse überwindet noch dazu dient, Erkenntnisse über das Verhalten gerade in der Wohnung zu gewinnen. Dem Bundesverfassungsgericht ist daher zu folgen, wenn es mögliche Schutzlücken nicht durch Umbildung des für Art. 13 GG tradierten Schutzguts, sondern durch Anerkennung einer eigenständigen Schutzgarantie in Form des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme auffangen will.[69]

Sofern jedoch das Wohnungsgrundrecht beeinträchtigt ist, stellt sich die Frage nach den maßgeblichen Schrankenregelungen. Während der Umgang mit den (qualifizierten) Gesetzesvorbehalten in Art. 8 Abs. 2 EMRK bzw. Art. 52 Abs. 1 und 3 GRCh keine dogmatischen Schwierigkeiten bereitet, ist im Falle von Art. 13 GG das weithin als „missglückt" geltende Schrankenre-

[64] Zu Art. 13 GG als Teil des grundgesetzlichen Privatheitsschutzes grundlegend BVerfGE 32, 54 (72 ff.); 42, 212 (219).

[65] Zur Datenerhebung aus dem „Smart Home" siehe *Müller/Schwabenbauer*, Verfassungs-, unions- und konventionsrechtliche Vorgaben, in: Lisken/Denninger, HdbPolR, 7. Aufl. 2021, Kap. G, Rn. 1339 f.; *R. Frau*, Der nachrichtendienstliche Zugriff auf Smarthome-Geräte, GSZ 2020, S. 149 ff.

[66] Zur Problematik *W. Ganz*, My Home(office) is my castle, ArbRAktuell 2018, S. 35 ff. Aktuelle Überlegungen auch bei *S. Müller*, Homeoffice in der arbeitsrechtlichen Praxis, 2. Aufl. 2020, § 3 Rn. 189 ff., 272 ff.

[67] BVerfGE 120, 274 (309 f., Rn. 191 ff.).

[68] BVerfGE 120, 274 (310 f., Rn. 194). A. A. etwa *Hauck*, Heimliche Strafverfolgung und Schutz der Privatheit, 2014, S. 420 f.

[69] BVerfGE 120, 274 ff. Dazu gleich unter § 5 I. 2. c) bb).

gime in Art. 13 Abs. 2 bis 7 GG zu beachten.[70] Dessen dogmatische Rekonstruktion wirft Fragen auf, die weit über das vorliegende Thema hinausweisen. Im Folgenden soll daher nur auf das Problem eingegangen werden, ob Eingriffsmaßnahmen, die von den in Art. 13 Abs. 2 bis 7 GG aufgeführten Typen abweichen, überhaupt gerechtfertigt werden können oder ob die Schrankenregelung des Art. 13 GG abschließend ist. Dies ist deswegen relevant, weil sich die vielfältigen Modi der Manipulation von IT-Systemen zum Zwecke der Wohnungsüberwachung nicht stringent in das Korsett der in Art. 13 GG benannten Eingriffsformen einordnen lassen. So kann etwa das Betreten der Wohnung zum Zwecke der Manipulation eines IT-Systems nicht auf Art. 13 Abs. 3 oder 4 GG gestützt werden und stellt auch weder eine Durchsuchung noch eine typische Begleitmaßnahme dar, die in der Anordnung zur akustischen oder optischen Überwachung „mitgeregelt" werden könnte. Die Frage stellt sich daher, ob das Fehlen einer speziellen Schrankenregelung derartige Maßnahmen per se verfassungswidrig macht.[71]

Die Kritik am Schrankenregime des Art. 13 GG reicht zurück bis in die 1960er-Jahre.[72] In seiner Ursprungsfassung differenzierte Art. 13 GG lediglich zwischen Durchsuchungen (Abs. 2) und sonstigen „Eingriffen und Beschränkungen" (Abs. 3 a. F., jetzt Abs. 7). Diese Aufteilung der Schrankenregelung auf zwei Absätze geht auf die 23. Sitzung des Grundsatzausschusses vom 19.11.1948 zurück.[73] Während weitgehend Einigkeit über die Anforderungen an die als besonders schwer bewertete Eingriffsform der Durchsuchung bestand,[74] wurde intensiv diskutiert, welche Maßstäbe an die tradierten behördlichen Nachschaurechte zu stellen wären.[75] Für sonstige Eingriffe durch die Verwaltungsbehörden sah der der Erstberatung zu Grunde liegende Text vor,

[70] Zu diesem Urteil siehe bereits *E. Kern*, Schutz des Lebens, der Freiheit und des Heims, in: Neumann/Nipperdey/Scheuner (Hrsg.), Die Grundrechte, Bd. II, 1954, S. 51 (102 ff.); vgl. weiter nur *G. Hermes,* in: Dreier, GG, Bd. I, 3. Aufl. 2012, Art. 13 Rn. 30; *Berkemann*, in: Denninger et al., AK-GG, 3. Aufl. 2001, Art. 13 Rn. 8 ff., 67; *Herdegen*, in: Dürig/Herzog/Scholz, GG, Art. 13 (2014), Rn. 23, 34, 47.

[71] Eine detaillierte Würdigung einzelner Eingriffsmaßnahmen soll hier nicht vorgenommen werden; stattdessen geht es darum, den verfassungsrechtlichen Rahmen für solche Einzelanalysen zu rekonstruieren.

[72] Näher *P. Dagtoglou*, in: BK GG, Art. 13 (1966 Zweitbearb.); *E. Stein*, Die Wirtschaftsaufsicht, 1967, S. 121 ff.; *M. Gentz*, Die Unverletzlichkeit der Wohnung, 1968. Siehe auch den Überblick bei *Berkemann*, in: Denninger et al., AK-GG, 3. Aufl. 2001, Art. 13 Rn. 11 f.

[73] Parl. Rat 5/I, S. 615.

[74] Einen ursprünglich enthaltenen Verweis auf das Strafprozessrecht strich man, weil die Rechtsordnung auch andernorts Durchsuchungsrechte enthalte, vgl. Parl. Rat 5/I, S. 88, 105 f.

[75] Vgl. die Diskussion zwischen *Schmid*, *Zinn* und *v. Mangoldt* in Parl. Rat 5/I, S. 106 f. Auf den Beschluss zur Einführung einer Sonderregelung für solche Durchsuchungen, die dem Gesichtspunkt der „Sicherstellung der Bewirtschaftung" Rechnung tragen sollten (a. a. O., S. 106, 108), kam man nicht zurück.

dass diese nur zulässig sein sollten, wenn sie dem „Interesse des gemeinen Wohles, insb. zur Behebung der Raumnot, zur Bekämpfung von Seuchengefahr, zum Schutze gefährdeter Jugendlicher" dienlich wären.[76] Diese Formulierung wurde kritisiert, weil sie vom allgemeinen Gesetzesvorbehalt der Weimarer Zeit kaum zu unterscheiden war. Gleichzeitig wurde darauf hingewiesen, dass der Gesetzesvorbehalt nicht überspannt werden dürfe, da in Sondersituationen auch gewohnheitsrechtlich anerkannte Eingriffsmöglichkeiten noch von Abs. 3 gedeckt sein müssten.[77] Die konkrete Formulierung wurde zwischen Hauptausschuss und Redaktionsausschuss kontrovers, allerdings weitgehend abstrakt erörtert.[78] Der letztlich gefundene Kompromiss unterschied dann zwischen Eingriffen ohne gesetzliche Grundlage in Fällen schwerer Gefahren und Maßnahmen auf gesetzlicher Grundlage, für die eine „dringende Gefahr" erforderlich war. Änderungsanträge im Plenum gab es nicht.[79] Dass diese Kategorien gerade mit Blick auf die tradierten behördlichen Nach- und Umschaurechte nicht praktikabel waren, wurde ab den 1960er-Jahren immer deutlicher. Dennoch steuerte der verfassungsändernde Gesetzgeber nicht nach. Auch als nach langen Diskussionen im Jahr 1998 die heutigen Absätze 3 bis 6 ergänzt wurden, die den Einsatz technischer Mittel zur optischen oder akustischen Überwachung von Wohnungen gestatteten und die verfassungsrechtliche Grundlage für die gesetzliche Einführung präventiver und repressiver Lausch- und Spähangriffe legten, wurde die alte Schrankenregelung nicht reformiert.[80]

Mangels eindeutiger verfassungstextlicher Direktiven entwickelten sich in der Literatur und Rechtsprechung sehr unterschiedliche dogmatische Positionen in dieser Frage. Die verfassungsrechtliche Diskussion zum Schrankenregime des Art. 13 GG wurde dabei gerade anfangs stark durch die behördlichen Betretungs- und Nachschaurechte getrieben. Diese Befugnisse, die sich vor allem im Gefahrenabwehr-, Umwelt- und Wirtschaftsverwaltungsrecht fanden und finden, sind – jedenfalls im herkömmlichen Sinne – keine Durchsuchungen i. S. d. Abs. 2; sie nutzen auch keine technischen Mittel i. S. d. Abs. 3 bis 6 und dienen als Routinemaßnahmen, jedenfalls ganz überwiegend, nicht der

[76] Parl. Rat 5/I, S. 88.

[77] Vgl. den Verweis *von Mangoldts* auf gewohnheitsrechtlich anerkannte behördliche Eingriffsmöglichkeiten, die von der Schrankenregelung gedeckt sein sollten, Parl. Rat 14, S. 1402.

[78] Parl. Rat 7, S. 141, 213; Parl. Rat 14, S. 1494 f.

[79] Parl. Rat 6, S. 454.

[80] Die neu geschaffenen Absätze waren ihrerseits das Produkt eines alles andere als geradlinigen und konsistenten Gesetzgebungsprozesses. Zu den rechtspolitischen Diskussionen der 1990er-Jahre und zum verfassungsändernden Gesetzgebungsverfahren im Einzelnen *J. Ziekow/A. Guckelberger*, in: Friauf/Höfling, GG, Art. 13 (2005) Rn. 15 ff.; *H. Greve*, in: Schmidt-Bleibtreu/Hofmann/Henneke, GG, 15. Aufl. 2022, Art. 13 Rn. 5 f.

Verhütung „dringender Gefahren" im Sinne des Abs. 7.[81] Nachdem das BVerfG zunächst Tendenzen erkennen ließ, derartige Maßnahmen durch ein sehr weites Verständnis des Begriffs der „dringenden Gefahr" zu rechtfertigen,[82] löste es sich in seiner Entscheidung von 1971 zu § 17 HwO von den geschriebenen Schrankenregelungen und entwickelte für die Betretungsrechte ein eigenständiges, verfassungsimmanent begründetes Schrankenregime.[83] Diese Entscheidung wurde und wird von Teilen der Wissenschaft kritisiert, weil die geschriebenen Schrankenregelungen in den Abs. 2 bis 5 und 7 abschließend seien.[84] Stützen kann sich diese Kritik in erster Linie auf den Wortlaut des Abs. 7 („im übrigen"). Sie wirft jedoch die Frage auf, ob bzw. auf welche Weise die tradierten Nachschaurechte dann gerechtfertigt werden können. Die hierzu vorgeschlagenen Lösungen – neben der Absenkung der Anforderungen an das Vorliegen einer „dringenden Gefahr" wird auch eine Modifikation des Begriffs der Durchsuchung empfohlen – sind allerdings ihrerseits schweren interpretatorischen Bedenken ausgesetzt.[85] Wenn gleichwohl kaum jemand bereit ist, niederschwellige oder aus sonstigen Gründen sinnvolle Eingriffsmaßnahmen, die sich nicht unter die Schrankenvorbehalte des Art. 13 GG subsumieren lassen, prinzipiell für unzulässig zu erklären, bleibt letztlich mit dem BVerfG nur der Rückgriff auf ungeschriebene Schranken.[86] Bei Lichte betrachtet ist das Schrankenregime des Art. 13 GG hierfür auch offen. Aus systematischen Gründen überzeugt es nämlich nicht, Abs. 7 als Auffangtatbestand („im übri-

[81] Siehe insbes. *G. Lübbe-Wolff,* Satzungsrechtliche Betretungsrechte und Art. 13 GG, DVBl. 1993, S. 762 (764 f.); *Kühne*, in: Sachs, GG, 9. Aufl. 2021, Art. 13 Rn. 51. Zum Begriff der „dringenden Gefahr" jetzt BVerfGE 141, 220 (296, Rn. 184); 156, 63 (129 f., Rn. 229). Siehe auch BGHSt 62, 22 (27, Rn. 49).

[82] BVerfGE 17, 232 (251 f.). In diese Richtung auch noch *J. Ennuschat*, Behördliche Nachschau in Geschäftsräumen, AöR 127 (2002), S. 252 (282 ff.).

[83] BVerfGE 32, 54 (77). Siehe aus jüngerer Zeit BVerfG (K), NVwZ 2007, 1049, Rn. 28; BVerfG (K), NJW 2008, 2426, Rn. 12. Vgl. weiter auch BVerfGE 97, 228 (266, Rn. 141); BVerwGE 78, 251 (255 f.).

[84] Vgl. *F. Schoch,* Die Unverletzlichkeit der Wohnung nach Art. 13 GG, JURA 2010, S. 22 (30), mit einer Zusammenfassung der Kritik in der Literatur.

[85] Eine Modifikation des Durchsuchungsbegriffs hat insbesondere *P. Dagtoglou*, in: BK GG, Art. 13 (1966 Zweitbearb.), Rn. 73, vorgeschlagen. Dagegen deutlich *Herdegen*, in: Dürig/Herzog/Scholz, GG, Art. 13 (2014), Rn. 48, 69 m. w. N.; *A. Voßkuhle*, Behördliche Betretungs- und Nachschaurechte, DVBl. 1994, S. 611 (615 f.); *Schoch*, Die Unverletzlichkeit der Wohnung nach Art. 13 GG, JURA 2010, S. 22 (30); *Kunig/Berger*, in: v. Münch/Kunig, GG, 7. Aufl. 2021, Art. 13 Rn. 68; *Berkemann*, in: Denninger et al., AK-GG, 3. Aufl. 2001, Art. 13 Rn. 72. Zur „dringenden Gefahr" siehe bereits oben § 4 Fn. 81.

[86] Jedenfalls für die administrativen Betretungsrechte und wohl auch für den Einsatz verdeckter Ermittler in Wohnungen greift die h. M. auf verfassungsimmanente Schranken zurück. Im Falle der verdeckten Ermittler findet sich diese Argumentation selbst bei Autoren, die diesem Konzept sonst klar ablehnend gegenüberstehen, siehe etwa *Hermes*, in: Dreier, GG, Bd. I, 3. Aufl. 2012, Art. 13 Rn. 92, der für verdeckte Ermittler Art. 13 Abs. 2 GG analog anwenden möchte. Changierend auch *Kunig/Berger*, in: v. Münch/Kunig, GG, 7. Aufl. 2021, Art. 13 Rn. 37, 71.

gen“) zu verstehen, wird doch die Durchsuchung (Abs. 2) als anerkanntermaßen besonders schwere Form des Eingriffs nur formal durch einen präventiven Richtervorbehalt – ein Rechtsinstitut mit faktisch sehr begrenzter Schutzwirkung – eingehegt, während die in Abs. 7 genannten Eingriffe hohe materielle Hürden überwinden müssen. Die beiden Absätze lassen sich daher nicht als Spezial- (Abs. 2) und Auffangtatbestand (Abs. 7) rekonstruieren, sondern stehen nebeneinander. Die Abs. 3 bis 5 regeln wiederum sehr spezielle, aus einer historisch kontingenten Diskussion um bestimmte Kriminalitätsformen („organisierte Kriminalität“) entwickelte Ermittlungspraktiken, enthalten darüber hinaus jedoch keine verallgemeinerungsfähigen Aussagen zu Grundrechtsbeschränkungen. Insgesamt erweist sich das (geschriebene) Schrankenregime des Art. 13 GG als eklektisch und unvollständig. Für die dort nicht geregelten Eingriffskonstellationen ist daher der Rückgriff auf verfassungsimmanente Schranken unumgänglich. Dem naheliegenden Einwand, auf diese Weise könnten die hohen Anforderungen der geschriebenen Schrankenregelungen unterlaufen werden, lässt sich dadurch begegnen, dass die in den Abs. 2 ff. festgeschriebenen formellen und materiellen Anforderungen als Maßstab für die nicht direkt von den qualifizierten Schrankenregelungen erfassten Eingriffsmaßnahmen analog herangezogen werden.[87] Zudem genießen die in den Art. 13 Abs. 2 bis 5 GG benannten Eingriffsformen einen „Typenschutz“: Für die diesen spezifischen Maßnahmen zu Grunde liegenden Spannungslagen ist das verfassungstextlich geronnene Schutzprogramm abschließend und darf nicht durch den Rückgriff auf anders strukturierte, wenn auch im Ergebnis ähnlich hohe verfassungsimmanente Schranken umgangen werden.

Für die hier in Rede stehenden Eingriffe in Art. 13 GG, die IT-Schwachstellen ausnutzen, heißt das, dass entsprechende Eingriffsbefugnisse nicht schon deshalb verfassungswidrig wären, weil das Schrankenregime des Art. 13 GG keine expliziten Vorgaben dafür macht. Vielmehr gilt es, im Lichte der konkreten Eingriffsmodalitäten sowie unter Berücksichtigung der in Art. 13 Abs. 2 bis 5 und 7 GG festgeschriebenen Anforderungen je geeignete Prüfungsmaßstäbe zu entwickeln. Im bereits angeführten Beispiel, in dem die Behörden Zugriff auf die an den Computer des Betroffenen angeschlossenen Mikrofone erlangen wollen, um Raumgespräche abzuhören, liegt etwa auf der Hand, dass ein derartiges Vorgehen mindestens den Anforderungen der Art. 13 Abs. 3 bzw. 4 GG

[87] Ähnlich zur „Obergrenzfunktion“ der Abs. 2 ff. *Kühne*, in: Sachs, GG, 9. Aufl. 2021, Art. 13 Rn. 25. Entsprechend, aber unflexibler, *Berkemann*, in: Denninger et al., AK-GG, 3. Aufl. 2001, Art. 13 Rn. 72, der für alle nicht von den Art. 13 Abs. 2 bis 5 und 7 erfassten Eingriffshandlungen die Schrankenregelung des Art. 13 Abs. 2 GG anwenden will. Das BVerfG verfährt auch außerhalb des Anwendungsbereichs von Art. 13 Abs. 1 GG ähnlich, wenn es die Maßstäbe für Online-Durchsuchungen fast durchgängig parallel zu den Maßstäben für Wohnungsüberwachungen konstruiert, vgl. BVerfGE 120, 274 (327 ff., Rn. 244 ff.); 141, 220 (270 f., Rn. 106 ff.; 326, Rn. 283).

genügen muss.[88] Im ähnlich gelagerten Fall, in dem Behördenvertreter zum Zweck der Manipulation eines IT-Systems (etwa: Online-Durchsuchungen und Quellen-TKÜ) die Wohnung des Betroffenen betreten, kann erneut aus dem Nichtvorhandensein einer speziellen Schranke nicht der Schluss gezogen werden, dass der Gesetzgeber ein solches Betretungsrecht nicht regeln kann. Auch hier gilt jedoch, dass angesichts der Natur und Schwere des Eingriffs mindestens die Anforderungen des Art. 13 Abs. 3 bzw. 4 erfüllt sein müssen.[89]

c) Schutz des allgemeinen Persönlichkeitsrechts

Soweit nicht die spezielleren Garantien des Telekommunikationsgeheimnisses und des Wohnungsgrundrechts einschlägig sind, berühren hoheitlich verantwortete Attacken auf IT-Systeme regelmäßig das aus Art. 2 Abs. 1 und Art. 1 Abs. 1 GG hergeleitete Recht auf informationelle Selbstbestimmung bzw. das Recht auf Achtung der Privatsphäre und auf Datenschutz aus Art. 7 und 8 GRCh sowie Art. 8 EMRK. Darüber hinaus hat das Bundesverfassungsgericht im Jahr 2007 in seiner Entscheidung zur Online-Durchsuchung ebenfalls aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ein „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" entwickelt, das für Systeme, die sensible personenbezogene Daten verarbeiten, eine spezielle Schrankenregelung schafft.[90] In welcher Form diese Grundrechtsgarantien staatlichen Maßnahmen zur Senkung des Informationssicherheitsniveaus Grenzen ziehen, soll im Folgenden betrachtet werden.

aa) Recht auf informationelle Selbstbestimmung

Staatliche Maßnahmen, die die IT-Sicherheit beeinträchtigen, kollidieren immer dann mit dem Recht auf informationelle Selbstbestimmung bzw. den korrespondierenden europarechtlichen Garantien, wenn im Zuge dessen personenbezogene Daten verarbeitet werden. Der Schutz der informationellen Selbstbestimmung deckt daher, wie bereits erwähnt, nicht die ganze Breite denkbarer Gefährdungslagen für IT-Systeme ab.[91] Legen staatliche Stellen mittels eines Angriffs auf IT-Systeme etwa ein Strom- oder Mobilfunknetz

---

[88] Vgl. *M. Soiné*, Die strafprozessuale Online-Durchsuchung, NStZ 2018, S. 497 ff.; *Frau*, Der nachrichtendienstliche Zugriff auf Smarthome-Geräte, GSZ 2020, S. 149 ff. Zu der von der Frage nach der maßgeblichen Schrankenregelung zu unterscheidenden Frage, ob bzw. inwieweit einfachrechtliche Befugnisnormen wie § 100c StPO für solche Operationen einen hinreichenden „maßnahmespezifischen Zuschnitt" aufweisen, siehe *M. Löffelmann*, Datenerhebung aus dem „Smart Home" im Sicherheitsrecht, GSZ 2020, S. 244 (250).

[89] *Soiné*, Die strafprozessuale Online-Durchsuchung, NStZ 2018, S. 497 (501).

[90] BVerfGE 120, 274 (313 f.). Dazu, inwieweit Art. 8 EMRK entsprechenden Schutz gewährt, siehe *F. Paefgen*, Der von Art. 8 EMRK gewährleistete Schutz vor staatlichen Eingriffen in die Persönlichkeitsrechte im Internet, 2017, S. 101 ff., 113 ff.

[91] Siehe oben § 5 Fn. 37.

lahm, betrifft dies typischerweise die informationelle Selbstbestimmung nicht. Angesichts seines überaus weiten Anwendungsbereichs kommt dem Recht auf informationelle Selbstbestimmung allerdings in der Praxis oftmals eine Auffangfunktion zu.[92] Die bisher geschaffenen Eingriffsbefugnisse, die staatlichen Stellen gestatten, die IT-Sicherheit zu manipulieren, zielen zudem vorrangig auf die Erhebung personenbezogener Informationen.[93] Aus diesen Gründen steht das Recht auf informationelle Selbstbestimmung in der Diskussion um die grundrechtliche Fundierung des Informationssicherheitsrechts bisher nicht zu Unrecht oft im Vordergrund.[94]

Genese und Anliegen des Rechts auf informationelle Selbstbestimmung sind hier bereits berichtet worden.[95] Berichtet wurde auch, dass das BVerfG trotz vielfältiger Kritik – an der vorgeblich eigentumsanalogen, herrschaftsrechtlichen Fundierung des Grundrechts,[96] an der subjektiv-rechtlichen Aufladung eines (bloß) instrumentellen Konzepts,[97] an der fehlenden Kontextsen-

[92] Dies betonen – ausgehend von einem anderen dogmatischen Grundverständnis (vgl. gleich § 5 Fn. 97) – auch *Poscher/Lassahn*, Verfassungsrechtliche Dimensionen der IT-Sicherheit, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 7 Rn. 34.

[93] Das schließt nicht aus, dass die Maßnahmen auch weitergehende Zwecke verfolgen können, was gegenüber der informationellen Selbstbestimmung speziellere Grundrechtsgarantien aktivieren kann, wenn etwa die durch Manipulationen der IT-Sicherheit gewonnenen Informationen zur Verhinderung einer Versammlung genutzt werden, vgl. *Poscher/Lassahn*, Verfassungsrechtliche Dimensionen der IT-Sicherheit, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 7 Rn. 33.

[94] So die Diagnose bei *Poscher/Lassahn*, Verfassungsrechtliche Dimensionen der IT-Sicherheit, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 7 Rn. 27 mit Verweis auf *B. Derin/S. Golla*, Der Staat als Manipulant und Saboteur der IT-Sicherheit?, NJW 2019, S. 1111 ff.; *D.-K. Kipker/D. Scholz*, Das IT-Sicherheitsgesetz 2.0, MMR 2019, S. 431 (432).

[95] Zur Genese und zu den Gehalten dieses Rechts siehe oben § 3 III. Zusammenfassend auch *Bull*, Informationelle Selbstbestimmung – Vision oder Illusion?, 2. Aufl. 2011, S. 22 ff. Zur unionalen Rechtsentwicklung siehe *J.-P. Schneider*, Stand und Perspektiven des Europäischen Datenverkehrs- und Datenschutzrechts, DV 44 (2011), S. 499 ff.

[96] Dazu *M. Albers*, Information, Rechtstheorie 33 (2002), S. 61 (81); *dies.*, Realizing the Complexity of Data Protection, in: Gutwirth/de Hert/Leenes (Hrsg.), Reloading Data Protection, 2014, S. 213 (225 ff.); *Britz*, Informationelle Selbstbestimmung, in: Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, 2010, S. 561 (566 ff.); *Schneider*, Stand und Perspektiven des Europäischen Datenverkehrs- und Datenschutzrechts, DV 44 (2011), S. 499 (502); *M. Eifert*, Autonomie und Sozialität, in: Bumke/Röthel (Hrsg.), Autonomie im Recht, 2017, S. 365 (371).

[97] *R. Poscher*, Die Zukunft der informationellen Selbstbestimmung, in: Gander/Perron et al. (Hrsg.), Resilienz in der offenen Gesellschaft, 2012, S. 167 (173 ff.); für den vorliegenden Kontext siehe auch *ders./Lassahn*, Verfassungsrechtliche Dimensionen der IT-Sicherheit, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 7 Rn. 31 ff. (wobei das „Recht" auf informationelle Selbstbestimmung als dogmatische Erweiterung des Eingriffsbegriffs und als Vorverlagerung des Schutzes aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG und anderen Grundrechten auf den Schutz bereits vor abstrakten Gefährdungen konzipiert wird); vgl. weiter auch *B. Rössler*, Der Wert des Privaten, 2001, S. 203 ff.; *Britz*, Informationelle Selbstbestimmung, in: Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, 2010, S. 561 (573 f.). Siehe aber BVerfGE 115, 166 (188); 150, 244 (263 f., Rn. 37); 155, 119 (166, Rn. 92).

sibilität des Rechts,[98] am prohibitivem Charakter des Risiko-Paradigmas,[99] am verfehlten bzw. illusionären Charakter des Selbstbestimmungskonzepts im informationellen Kontext,[100] an der Vernachlässigung der objektiv-rechtlichen Seite,[101] an der Verkürzung auf den Schutz personenbezogener Daten,[102] an der fehlenden Komplexität und Responsivität des (Abwehr-)Rechts in einer von steten (technischen) Veränderungen und Machtverschiebungen gezeichneten Informationsgesellschaft[103] etc. – bislang stets an der Grundkonzeption des Rechts als einer dem Einzelnen eingeräumten Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung der eigenen persönlichen (personenbezogenen) Daten zu bestimmen, und an seiner Verortung im allgemeinen Persönlichkeitsrecht festgehalten hat.[104]

Auch aus diesem Grund besteht über die wesentlichen „Schutzgehalte“[105] des Rechts auf informationelle Selbstbestimmung heute ebenso wie bei den korrespondierenden Garantien im Unions- (Art. 7 und 8 GRCh[106]) und Konventionsrecht (Art. 8 EMRK[107]) im Ergebnis wenig Streit – ganz unabhängig

[98] *Albers*, Informationelle Selbstbestimmung, 2005, S. 353 ff. Siehe aber BVerfGE 120, 378 (LS 2 und 401 ff.).

[99] *K.-H. Ladeur*, Das Recht auf informationelle Selbstbestimmung, DÖV 2009, S. 45 (53 f.).

[100] *Bull*, Informationelle Selbstbestimmung – Vision oder Illusion?, 2. Aufl. 2011; *Y. Hermstrüwer*, Informationelle Selbstgefährdung, 2016. Vgl. aber BVerfGE 152, 152 (189, Rn. 85).

[101] *K.-H. Ladeur*, Datenschutz, DuD 2000, S. 12 ff.; *ders.*, Das Recht auf informationelle Selbstbestimmung, DÖV 2009, S. 45 ff.; vgl. auch *W. Hoffmann-Riem*, Informationelle Selbstbestimmung in der Informationsgesellschaft, AöR 123 (1998), S. 513 (522 ff.); *Albers*, Informationelle Selbstbestimmung, 2005, S. 454 ff. Vgl. aber BVerfGE 125, 260 (325 ff.).

[102] Siehe *R. Broemel/H.-H. Trute*, Alles nur Datenschutz?, Berliner Debatte Initial 27:4 (2016), S. 50 (52).

[103] *Hoffmann-Riem*, Informationelle Selbstbestimmung in der Informationsgesellschaft, AöR 123 (1998), S. 513 ff.; vgl. auch *H.-H. Trute*, Der Schutz personenbezogener Daten in der Informationsgesellschaft, JZ 53 (1998), S. 822 ff. Zu den demokratiefunktionalen Aspekten des Datenschutzrechts weiter *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 94 f. Vgl. aber erneut BVerfGE 152, 152 (189, Rn. 85).

[104] Zur Rechtsprechungsentwicklung siehe nur *R. Poscher/J. Buchheim*, Staatsaufsicht und Datenschutz, DVBl. 2015, S. 1273 ff. Aus jüngerer Zeit siehe insbesondere BVerfGE 133, 277 (316 ff., Rn. 93 ff.); 141, 220 (264 ff., Rn. 90 ff.); 150, 244 (263 ff., Rn. 35 ff.); 150, 309 (330 ff., Rn. 54 ff.); 155, 119 (166 ff., Rn. 90 ff.).

[105] Zu diesem Begriff in Abgrenzung zu den Begriffen Schutzzielen, Schutzbedürfnissen und Schutzgut instruktiv *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 96 ff. m. w. N.

[106] Zum Verhältnis von Art. 7 und 8 GRCh aus Sicht des EuGH siehe oben § 5 Fn. 45. Zu den Gehalten und zum Verhältnis der Garantien aus der Literatur statt vieler *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 7 ff. und passim; *N. Bernsdorff*, in: Meyer/Hölscheidt, Charta, 5. Aufl. 2019, Art. 7 Rn. 14 ff.; *J.-P. Schneider*, in Wolff/Brink, BeckOK Datenschutzrecht, 41. Ed. 1.8.2022, Syst B. Rn. 18 ff.

[107] Zu den im vorliegenden Kontext relevanten Gehalten des Art. 8 EMRK ausführlich *Paefgen*, Der von Art. 8 EMRK gewährleistete Schutz vor staatlichen Eingriffen in die Persönlichkeitsrechte im Internet, 2017, S. 52 ff. und passim. Zur Frage, inwieweit die Kohärenz-

davon, ob man das Recht abwehrrechtlich rekonstruiert und die Schutzgehalte als Ausformungen des Verhältnismäßigkeitsgrundsatzes konzipiert oder ob man – wofür gute Gründe sprechen – das Grundrecht auch und gegebenenfalls sogar in erster Linie als an den Gesetzgeber gerichteten Auftrag versteht, den Umgang mit personenbezogenen Daten regelförmig, begrenzt, transparent und kontrollierbar zu gestalten.[108] Die grundrechtlichen Garantien stellen die Verarbeitung personenbezogener Daten dabei unter einen umfassenden Vorbehalt. Wenn das einfache Recht „personenbezogene Daten" weit definiert als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen" (Art. 4 Nr. 1 DSGVO; § 46 Nr. 1 BDSG),[109] dann entspricht das der bundesverfassungsgerichtlichen Feststellung, es gebe aufgrund der technischen Möglichkeiten heute „kein belangloses Datum" mehr,[110] da auch ein für sich nicht sensibles Datum durch die Verknüpfung mit anderen Daten weitreichende Rückschlüsse auf die Persönlichkeit des Betroffenen zulasse.[111]

Durch die starke Vorverlagerung des Schutzes auch auf nicht sensible Informationen[112] wirkt das Recht zunächst als allgemeines Regulierungsgebot: Überall dort, wo personenbezogene Daten verarbeitet werden sollen, muss der Gesetzgeber normenklare gesetzliche Erlaubnistatbestände schaffen.[113] Darüber hinaus verpflichtet das Recht zum sachgerechten Umgang mit personenbezogenen Daten, zur strengen Beachtung des Grundsatzes der Verhältnismäßigkeit, zur Schaffung rechtlicher Sicherungsmechanismen, insbesondere zur Einräumung von Betroffenenrechten sowie zu organisatorischen und verfahrensrechtlichen Schutzvorkehrungen und Kontrollmaßnahmen. Mit der Menschenwürde unvereinbar ist eine Registrierung und Katalogisierung der Persönlichkeit. Diese Schutzgehalte sind heute auch auf unions(-grund-) recht-

---

sicherungsklausel des Art. 52 Abs. 2 GRCh auch bezüglich den Art. 8 GRCh greift, der in der Entsprechungsliste nicht genannt ist und der als lex specialis zu Art. 7 GRCh verstanden wird, näher *Schneider*, in Wolff/Brink, BeckOK Datenschutzrecht, 41. Ed. 1.8.2022, Syst B. Rn. 19 f.

[108] Siehe dazu insbesondere die Nachweise oben § 5 Fn. 97 und 101.

[109] Zur Korrespondenz von verfassungs- und einfachrechtlichem Begriff des personenbezogenen Datums siehe BVerfG (K), NJW 2018, 2395 (2396, Rn. 44). Siehe weiter zum Begriff aus Sicht des Grundgesetzes BVerfGE 128, 1 (43 ff.); 130, 151 (183 f.). Zum Begriff aus unionsrechtlicher Sicht EuGH, C-582/14 v. 19.10.2016, Rn. 31 f., 46, 49 – Breyer; EuGH, C-25/17 v. 10.7.2018, Rn. 37 – Zeugen Jehovas. Ähnlich weit auch EGMR, 28341/95 v. 4.5.2000, Rn. 42 f. – Rotaru; EGMR, 63737/00 v. 17.7.2003, Rn. 36 – Perry.

[110] BVerfGE 65, 1 (45).

[111] Vgl. auch *Barczak*, in: Dreier, GG, Bd. I, 4. Aufl., i. E., Art. 2 Abs. 1 Rn. 91 m. w. N.

[112] Deutlich etwa BVerfGE 150, 244 (264, Rn. 38).

[113] Grundlegend BVerfGE 65, 1 (43). Zur Weite des Eingriffsbegriffs im Unionsrecht siehe EuGH, C-291/12 v. 17.10.2013, Rn. 28 ff. – Schwarz; EuGH, C-293/12 v. 8.4.2014, Rn. 34 – Digital Rights Ireland. Zur Perspektive der EMRK vgl. EGMR, 54934/00 v. 29.6.2006, Rn. 78 – Weber and Saravia.

licher Ebene anerkannt, teilweise auch durch Art. 8 Abs. 2 und 3 GRCh primärrechtlich vorstrukturiert,[114] jedenfalls aber umfassend sekundärrechtlich kodifiziert.[115] (National-)verfassungsrechtlich leitet das Bundesverfassungsgericht sie – methodisch weitgehend freischwebend – aus dem Verhältnismäßigkeitsgrundsatz her.[116] Besondere Relevanz entfaltet zudem das vom BVerfG im Kontext der informationellen Selbstbestimmung scharfgestellte Bestimmtheitsgebot. Bereits im Volkszählungsurteil hielt es das Gericht für notwendig, dass Anlass, Zweck und Grenzen des Eingriffs in der Ermächtigungsgrundlage „bereichsspezifisch und präzise" sowie normenklar bestimmt werden.[117] Der Gesetzgeber muss also selbst vorstrukturieren und begrenzen, wie personenbezogene Daten verarbeitet werden.[118] Gerade was die staatliche Datenverarbeitung betrifft, begründet das Erfordernis einer präzisen Bestimmung des Verwendungszwecks eine auf die spezifische Funktionalität des informationstechnischen Systems bezogene Rationalisierungs- und Rechenschaftspflicht. Dementsprechend wird eine „formalisierte Abschichtung der Erhebungs- und Verarbeitungsschritte in detailliert zu erfassende Eingriffe" verlangt, für die jedenfalls im öffentlichen Bereich auch je eine eigene hinreichend bestimmte gesetzliche Grundlage geschaffen werden muss.[119] Soweit Manipulationen der IT-Sicherheit im Kontext des auf Informations- und Wissensgenerierung zielenden Sicherheitsrechts erfolgen, bewegen sie sich schließlich

[114] Zu den sich an die Schrankenregelungen des Art. 8 GRCh knüpfenden Auslegungsproblemen, insbesondere zur Frage, wie sich die Schrankenregelungen der Absätze 2 und 3 zu Art. 52 Abs. 2 GRCh und Art. 16 AEUV verhalten, siehe nur *H. Jarass*, in: Jarass, GRCh, 4. Aufl. 2021, Art. 8 Rn. 13 ff.; *Schneider*, in Wolff/Brink, BeckOK Datenschutzrecht, 41. Ed. 1.8.2022, Syst B. Rn. 22 ff.

[115] Zusammenfassend hierzu *Eichenhofer*, e-Privacy, 2021, S. 207 ff., 325 ff.

[116] Vgl. bereits BVerfGE 65, 1, 44 ff. Aus der Folgerechtsprechung siehe insbesondere BVerfGE 133, 277 (365 ff., Rn. 204 ff.); 141, 220 (282 ff., Rn. 134 ff.); entsprechend für Art. 10 GG BVerfGE 154, 152 (286 ff., Rn. 265 ff.). Kritisch zur dogmatischen Herleitung *K. F. Gärditz*, Bundesnachrichtendienst semper reformanda, DVBl. 2021, S. 905 (910, 912).

Die besonderen Eigenschaften von Daten, namentlich ihre nahezu verlustfreie Kopierbarkeit, führen dazu, dass die Schutzkonzepte des Fernmeldegeheimnisses und des Rechts auf informationelle Selbstbestimmung teilweise parallel strukturiert sind. In diesem Sinne hat die Rechtsprechung die Anforderungen an Eingriffe in das Recht auf informationelle Selbstbestimmung und in Art. 10 GG weitgehend parallel ausgestaltet, wobei für die Erhebung und Weiterverarbeitung gerade von Telekommunikationsdaten im Einzelfall weitergehende Anforderungen gelten, vgl. BVerfGE 100, 313 (359, Rn. 164); 124, 43 (60, Rn. 60); 125, 260 (310, Rn. 191); BVerwG, NVwZ 2018, 731 (733, Rn. 25). Siehe insbes. auch BVerfGE 115, 320 (347, Rn. 95).

[117] BVerfGE 65, 1 (46, 54). Siehe weiter BVerfGE 100, 313 (359 f.); 110, 33 (53); 120, 274 (315 ff., Rn. 208 ff.); 133, 277 (323 ff., Rn. 113 ff.); 141, 220 (324 ff., Rn. 276 ff.).

[118] Zum Parlamentsvorbehalt beim Recht auf informationelle Selbstbestimmung siehe nur *T. Rademacher/L. Perkowski*, Staatliche Überwachung, neue Technologien und die Grundrechte, JuS 2020, S. 713 (719); *Barczak*, in: Dreier, GG, Bd. I, 4. Aufl., i. E., Art. 2 Abs. 1 Rn. 104.

[119] BVerfGE 152, 152 (190, Rn. 86 f.).

auf einem Gebiet, in dem nationale und europäische Gerichte traditionell strenge Kontrollmaßstäbe anlegen und die gesetzgeberischen Vorgaben kleinteilig nachprüfen.[120]

bb) Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

In seiner Entscheidung zur Online-Durchsuchung von 2007 hat sich der Erste Senat des Bundesverfassungsgerichts nicht darauf beschränkt, die Rechtfertigungslast für heimliche hoheitliche Maßnahmen, die im Zuge der Erhebung personenbezogener Daten zugleich die Integrität und Vertraulichkeit von IT-Systemen kompromittieren, zu erhöhen.[121] Vielmehr hat es in Reaktion auf die als gänzlich „neu" bewertete Bedrohungslage[122] das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als eigenständige tatbestandliche Ausprägung des allgemeinen Persönlichkeitsrechts geschaffen.[123]

Nach einer ersten, in der Tendenz eher kritischen Rezeption, die sich unter anderem daran stieß, dass hier „das System" zum Grundrechtsträger stilisiert würde,[124] wurde es bald still um das sogenannte „IT-Grundrecht".[125] Teilweise

---

[120] Siehe etwa BVerfGE 115, 320 (360 ff., Rn. 133 ff.); 120, 274 (321 ff., Rn. 226 ff.); 125, 260 (327 ff., Rn. 225 ff.; 334 ff., Rn. 238 ff.; 340 ff., Rn. 254 ff.); 141, 220 (264 ff., Rn. 90 ff.); 150, 244 (278 ff., Rn. 81 ff.); 150, 309 (335 ff., Rn. 70 ff.); entsprechend für Art. 10 GG BVerfGE 154, 152 (237 ff., Rn. 136 ff.). Ob darin eine Überreizung der verfassungsgerichtlichen Kontrollfunktion liegt, wird kontrovers diskutiert. Kritisch etwa *Groß*, in: Friauf/Höfling, GG, Art. 10 (2016) Rn. 71; vgl. auch das Sondervotum *Eichberger* zu BVerfGE 141, 220 (353 ff., Rn. 1 ff.). Positiver hingegen *Bäcker*, Sicherheitsverfassungsrecht, in: Herdegen/Masing et al. (Hrsg.), HVerfR, 2021, § 28 Rn. 184 ff.

[121] BVerfGE 120, 274 (302 ff., Rn. 165 ff.).

[122] BVerfGE 120, 274 (313, Rn. 200).

[123] Siehe insbesondere *W. Hoffmann-Riem*, Schutz der Vertraulichkeit und Integrität, JZ 63 (2008), S. 1009 (1014, 1022). Vgl. weiter nur *G. Britz*, Vertraulichkeit und Integrität informationstechnischer Systeme, DÖV 2008, S. 411 (412); *M. Hauser*, Das IT-Grundrecht, 2015, S. 48 m. w. N. Zur Semantik des „Neuen" und zum Topos der Grundrechtsinnovation siehe die Nachweise oben in § 3 Fn. 65.

[124] Alarmistisch *O. Lepsius*, Das Computer-Grundrecht, in: Roggan (Hrsg.), Online-Durchsuchungen, 2008, S. 21 (32 ff.). Offensichtlich wollte das Gericht jedoch IT-Systeme nicht um ihrer selbst willen schützen. Vielmehr wird – analog zu Art. 13 GG – der Schutz des Persönlichkeitsrechts vorverlagert und auf die Integrität von unter Privatheitsaspekten besonders sensiblen IT-Systemen erstreckt: *Hoffmann-Riem*, Schutz der Vertraulichkeit und Integrität, JZ 63 (2008), S. 1009 (1012). Nachvollziehbare Skepsis bei *M. Eifert*, Informationelle Selbstbestimmung im Internet, NVwZ 2008, S. 521 (522). Zu Recht hingegen auf die parallele Konstruktion der Art. 10 GG und Art. 13 GG verweisend, die in ähnlicher Form den Vertraulichkeitsschutz an „objektive" Strukturen knüpfen, *Hauser,* Das IT-Grundrecht, 2015, S. 64 f.

[125] Als „IT-Grundrecht" bezeichnet unter anderem bei *M. Bäcker*, Das IT-Grundrecht, in: Uerpmann-Wittzack (Hrsg.), Das neue Computergrundrecht, 2009, S. 1 ff.; *M. Albers*, Grundrechtsschutz der Privatheit, DVBl. 2010, S. 1061 (1068); *Hauser*, Das IT-Grundrecht,

galt es gar als „vergessen".[126] Mit dem wachsenden Bewusstsein um die Bedeutung sicherer IT-Systeme für das Gelingen von Staat und Gesellschaft hat sich das Interesse an dieser Grundrechtsausprägung jüngst jedoch wieder verstärkt.[127] Dass die im Urteil von 2008 erörterten Eingriffsformen nach wie vor von Bedeutung sind, hat der dem Urteil des BVerfG vom 20. April 2016 zum BKA-Gesetz zu Grunde liegende Sachverhalt gezeigt.[128] Die Diskussion ist seither nicht abgerissen.[129]

Unabhängig von diesen konjunkturellen Erwägungen stellt sich die Frage, ob die Anerkennung eines eigenständigen „Grundrechts" aus Sicht der Betroffenen tatsächlich einen Zugewinn an Schutz bewirkt hat. Das BVerfG hat sein rechtsschöpferisches Tätigwerden in erster Linie damit begründet, dass verwandte Grundrechte, namentlich das Recht auf informationelle Selbstbestimmung sowie die Freiheitsgewährleistungen der Art. 10 und Art. 13 GG, in den maßgeblichen Konstellationen keinen oder nicht hinreichend Schutz gewähren.[130] Für Art. 10 GG überzeugt dies, beschränkt sich dessen Schutz doch auf Kommunikations(-umstands-)daten; dieser beginnt erst mit dem Aus-der-Hand-Geben einer Mitteilung durch den Absender und endet, sobald die Mitteilung im (alleinigen) Herrschaftsbereich des Empfängers ange-

2015, S. 46 ff.; *Heinemann*, Schutz informationstechnischer Systeme, 2015, S. 179 ff. Kritisch zu diesem Begriff *H. Gersdorf*, in: Gersdorf/Paal, BeckOK Informations- und Medienrecht, 37. Ed. 1.7.2022, Art. 2 GG Rn. 22. Verdinglichende Fehlassoziationen kann der Begriff des „Computer-Grundrechts" wecken, der allerdings weit verbreitet ist, vgl. etwa *Lepsius*, Das Computer-Grundrecht, in: Roggan (Hrsg.), Online-Durchsuchungen, 2008, S. 21 ff.; R. Uerpmann-Wittzack (Hrsg.), Das neue Computergrundrecht, 2009; *S. Rixen*, in: Sachs, GG, 9. Aufl. 2021, Art. 2 Rn. 73c f.; *H. Hofmann* in: Schmidt-Bleibtreu/Hofmann/Henneke, GG, 15. Auf. 2022, Art. 2 Rn. 17. Der Begriffsvorschlag im gleichnamigen Beitrag von *A. Tschentscher*, Das Grundrecht auf Computerschutz, AJP/PJA 2008, S. 383 ff., hat sich, obschon in der Sache präzise, nicht durchgesetzt.

[126] *G. Baum/C. Kurz/P. Schantz*, Das vergessene Grundrecht, F.A.Z., 26.2.2013; *G. Baum*, Freiheit: Ein Appell, 2021, S. 63.

[127] Monographisch insbes. *Hauser*, Das IT-Grundrecht, 2015; *Heinemann*, Schutz informationstechnischer Systeme, 2015. Gerade im Vergleich zum Recht auf informationelle Selbstbestimmung bleibt die literarische Befassung jedoch dünn. In den etablierten Grundgesetz-Kommentaren finden sich ganz überwiegend nur kursorische Analysen, teils fehlen sogar diese, vgl. etwa *Ch. Starck*, in: v. Mangoldt/Klein/Starck, GG, 7. Aufl. 2018, Art. 2 Rn. 184a; *M. Pagenkopf*, in: Sachs, GG, 9. Aufl. 2021, Art. 10 Rn. 10a; *Ph. Kunig/J. A. Kämmerer*, in: von Münch/Kunig, GG, 7. Aufl. 2021, Rn. 81, 82; *D. Lorenz*, in: BK GG, Art. 2 (2008), Rn. 287 ff.; *H. Hofmann,* in: Schmidt-Bleibtreu/Hofmann/Henneke, GG, 15. Aufl. 2022, Art. 2 Rn. 17, 40 f. Ausführlichere Darstellungen finden sich vor allem bei *Barczak*, in: Dreier, GG, Bd. I, 4. Aufl., i. E., Art. 2 Abs. 1 Rn. 93 ff.; *Gersdorf*, in: Gersdorf/Paal, BeckOK Informations- und Medienrecht, 37. Ed. 1.8.2022, Art. 2 GG Rn. 22 ff.

[128] BVerfGE 141, 220 (224 ff., Rn. 2 ff.).

[129] Vertiefend dazu unten § 7.

[130] BVerfGE 120, 274 (303 ff., 168 ff.). Zum Folgenden ausführlich insbes. *Gersdorf*, in: Gersdorf/Paal, BeckOK Informations- und Medienrecht, 37. Ed. 1.8.2022, Art. 2 GG Rn. 23.

kommen ist.[131] Nur in diesem Zeitraum sind Daten den besonderen Risiken der telekommunikationstechnischen Übertragung ausgesetzt.[132] Hingegen realisiert sich bei Erhebungen vor Beginn und nach Abschluss des Übermittlungsvorgangs kein spezifisches Übertragungsrisiko. Dringen staatliche Stellen also in IT-Systeme ein, um dort ruhende Kommunikationsdaten oder sonstige personenbezogene Daten (etwa tagebuchähnliche Aufzeichnungen) zu extrahieren, vermittelt Art. 10 GG keinen Schutz. Die Grenze zwischen „laufenden" und „ruhenden" Kommunikationsdaten ist zwar nicht immer leicht zu ziehen. Kontrovers diskutiert wurde insbesondere die Zwischen- oder auch dauerhafte Speicherung von Kommunikationsdaten auf Servern, etwa bei der E-Mail-Übertragung und der Nutzung sozialer Netzwerke oder sonstiger Messaging-Dienste. Nach mittlerweile herrschender Meinung endet der Schutz des Art. 10 GG in diesen Fällen erst dann, wenn die Nachricht im alleinigen Herrschaftsbereich des Empfängers angekommen ist; solange die Kommunikationsdaten auf dem Server des Providers gespeichert sind, besteht hingegen noch ein spezifisches Übertragungsrisiko, vor dem Art. 10 GG schützen will.[133] In solchen Fällen hätte es daher keines zusätzlichen Schutzes bedurft. Ähnliche Abgrenzungsprobleme stellen sich auch bei der sog. Quellen-TKÜ.[134] Trotz dieser zeitlichen Ausweitung der Schutzgewähr bleibt es dabei, dass Art. 10 GG die Problematik staatlicher Manipulationen der IT-Sicherheit gewiss nicht abschließend erfasst.

Gleiches gilt auch für Art. 13 GG. Dessen Schutz greift ohnehin nur dann, wenn sich das angegriffene IT-System in einer „Wohnung" befindet, also in einem zum Aufenthalt von Menschen bestimmten Schutzraum, der ein Mindestmaß an Abgrenzung nach außen gewährleistet, um den physischen Zutritt und den Zugriff auf Informationen über dort befindliche Personen und Objekte zu

[131] BVerfGE 120, 274 (307 f., Rn. 185). Dazu weiter BVerfGE 115, 166 (183 ff., Rn. 72 ff.); 124, 43 (56, Rn. 48); BVerfG (K), NJW 2016, 3508 (3510, Rn. 40).

[132] Zur für die vorliegende Konstellation regelmäßig nicht relevanten Ausnahme der nach Abschluss des Übertragungsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten *Verbindungs*daten, für die der Nutzer nicht selbsttätig Schutzvorkehrungen treffen kann und die daher nach wie vor mit dem übermittlungsspezifischen Vertraulichkeitsrisiko belastet und somit von Art. 10 GG geschützt sind, siehe BVerfGE 107, 299 (313 f., Rn. 50 f.); 115, 166 (183 f., Rn. 70 f.); *T. Schwabenbauer*, Kommunikationsschutz durch Art. 10 GG, AöR 137 (2012), S. 1 (12 ff.); *von zur Mühlen*, Zugriffe auf elektronische Kommunikation, 2019, S. 86; *Schneider*, Fernmeldegeheimnis und Fernmeldeaufklärung, 2020, S. 31 f., 77.

[133] Siehe dazu BVerfGE 124, 43 (54 ff., Rn. 45 ff.); vgl. weiter auch *D. Neuhöfer*, Der Zugriff auf serverbasiert gespeicherte E-Mails beim Provider, 2011, S. 15 ff.; *Schwabenbauer*, Kommunikationsschutz durch Art. 10 GG, AöR 137 (2012), S. 1 (14); *S. Bauer*, Soziale Netzwerke und strafprozessuale Ermittlungen, 2018, S. 220 ff.; *von zur Mühlen*, Zugriffe auf elektronische Kommunikation, 2019, S. 103 ff. Zum Folgeproblem, auf welcher strafprozessualen Grundlage ein Zugriff erfolgen kann, BGH, NJW 2021, 1252 (1254, Rn. 13 ff.).

[134] Vertiefend unten § 7.

beschränken.[135] Mobile IT-Systeme außerhalb von Wohnungen werden daher nicht von Art. 13 GG erfasst. Aber auch bei vernetzten IT-Systemen, die sich innerhalb einer „Wohnung" im verfassungsrechtlichen Sinne befinden, begründet nicht jeder staatliche Zugriff einen Eingriff in Art. 13 GG. Für einen Eingriff in Art. 13 GG ist vielmehr erforderlich, dass durch staatliches Handeln die spezifische räumliche Abschirmung der Wohnung überwunden wird. Die Telekommunikationsüberwachung wird nicht dadurch zur Wohnraumüberwachung, dass sich der Nutzer des abgehörten Mobiltelefons in eine Wohnung begibt.[136] Hinzu kommt, dass die Privatheitserwartungen der Nutzer in Bezug auf ihre IT-Systeme kaum davon abhängen dürften, ob sich die Geräte innerhalb oder außerhalb ihrer Wohnung befinden. Allerdings sind Konstellationen denkbar, in denen sich Manipulationen der IT-Sicherheit am Wohnungsgrundrecht messen lassen müssen. Dies gilt insbesondere dann, wenn – wie erwähnt – staatliche Akteure durch Art. 13 Abs. 1 GG geschützte Räume (heimlich) betreten, um die dortigen IT-Systeme zu manipulieren, oder wenn mittels des manipulierten Systems – etwa über die Kamera oder das Mikrofon des Laptops – die Wohnung aus der Ferne überwacht werden soll.[137] Die parallele Anwendbarkeit der Grundrechte beschränkt sich jedoch auf Einzelfälle.

Zweifelhaft ist allerdings, wenn das BVerfG auch das Recht auf informationelle Selbstbestimmung im Umgang mit der skizzierten Gefährdungslage für überfordert hält, weil es nur Schutz vor dem Zugriff auf einzelne Daten oder Kommunikationsvorgänge garantiere, während sich der Staat durch Maßnahmen wie die Online-Durchsuchung einen „potentiell äußerst großen und aussagekräftigen Datenbestand" beschaffen könne, „ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein".[138] Dass die Eingriffsintensität der vom BVerfG mit dem IT-Grundrecht assoziierten Maßnahmen hoch ist, ist unbestreitbar.[139] Allerdings überzeugt es nicht,

---

[135] Maßgeblich ist der formale Aspekt der physischen Abgrenzung, vgl. *Albers*, Grundrechtsschutz der Privatheit, DVBl. 2010, S. 1061 (1064). Stärker nutzungs- bzw. funktionsbezogen der Wohnungsbegriff bei *Hermes*, in: Dreier, GG, Bd. I, 3. Aufl. 2012, Art. 13 Rn. 16; *Berkemann*, in: Denninger et al., AK-GG, 3. Aufl. 2001, Art. 13 Rn. 31; *Kühne*, in: Sachs, GG, 9. Aufl. 2021, Art. 13 Rn. 1.

[136] BVerfGE 120, 274 (310 f., Rn. 194). Kritisch hierzu *Hauck*, Heimliche Strafverfolgung und Schutz der Privatheit, 2014, S. 420 f.

[137] Zur Datenerhebung aus dem „Smart Home": *Löffelmann*, Datenerhebung aus dem „Smart Home" im Sicherheitsrecht, GSZ 2020, S. 244 ff.; *Frau*, Der nachrichtendienstliche Zugriff auf Smarthome-Geräte, GSZ 2020, S. 149 ff.; *Müller/Schwabenbauer*, Verfassungs-, unions- und konventionsrechtliche Vorgaben, in: Lisken/Denninger, HdbPolR, 7. Aufl. 2021, Kap. G, Rn. 1339 f.

[138] BVerfGE 120, 274 (312 f., Rn. 200 f.).

[139] Vgl. *L. Michael/M. Morlok*, Grundrechte, 8. Aufl. 2023, Rn. 429 („qualitativer Sprung"). Ähnlich auch *Hoffmann-Riem*, Schutz der Vertraulichkeit und Integrität, JZ 63 (2008), S. 1009 (1015 ff.); *M. Bäcker*, Vertraulichkeit der Internetkommunikation, in: Rensen/Brink (Hrsg.), Linien der Rechtsprechung, 2009, S. 99 (119 ff.).

punktuelle Datenerhebungen grundsätzlich als weniger intensiven Eingriff zu qualifizieren, wie bereits das Beispiel der Wohnraumüberwachung oder der Durchsuchung zeigt.[140] Zudem hat sich das Recht auf informationelle Selbstbestimmung auch sonst als leistungsfähig erwiesen, um großflächige oder eingriffsintensive staatliche Maßnahmen in den Griff zu bekommen.[141] Wie *Gabriele Britz* angemerkt hat, hat der Senat hier in seinem Bemühen, das „neue" Grundrecht zu rechtfertigen, der informationellen Selbstbestimmung „mutwillig die Flügel gestutzt, um ihr dann die erforderliche Flughöhe absprechen […] zu können".[142]

Jedenfalls was den Schutz der *Vertraulichkeit* des IT-Systems betrifft – bzw. in den Worten des Gerichts das vom neuen Grundrecht geschützte Interesse daran, „dass die von einem vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben" –, ist ein Mehrwert gegenüber dem Recht auf informationelle Selbstbestimmung nicht erkennbar.[143] Auf den ersten Blick anders verhält sich dies mit dem Schutz der *Integrität*. Auch wenn das Gericht mit diesem Aspekt, wie erwähnt, nicht das System um seiner selbst willen schützen will, findet doch eine Neuakzentuierung statt. So lässt sich staatliches Handeln nunmehr bereits dann als Eingriff qualifizieren, „wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können"; auf die Frage, ob dabei personenbezogene Daten verarbeitet werden, kommt es nicht an, soweit „die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen" ist.[144] Das IT-Grundrecht verlagert also den Schutz der Ver-

[140] *Gersdorf*, in: Gersdorf/Paal, BeckOK Informations- und Medienrecht, 37. Ed. 1.8.2022, Art. 2 GG Rn. 25.

[141] Hierzu und zum Folgenden insbes. *Britz*, Vertraulichkeit und Integrität informationstechnischer Systeme, DÖV 2008, S. 411 (413 f.); *Eifert*, Informationelle Selbstbestimmung im Internet, NVwZ 2008, S. 521 f.; *G. Hornung*, Ein neues Grundrecht, CR 2008, S. 299 (301 f). *Barczak*, in: Dreier, GG, Bd. I, 4. Aufl., i. E., Art. 2 Abs. 1 Rn. 96, weist darauf hin, dass schon BVerfGE 65, 1 (42), das Recht auf informationelle Selbstbestimmung mit Blick auf das Risiko entwickelt hat, dass personenbezogene Daten „zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden", was sich von der von BVerfGE 120, 274 (305, Rn. 178) perhorreszierten „Profilbildung" nicht wesentlich unterscheidet.

[142] *Britz*, Vertraulichkeit und Integrität informationstechnischer Systeme, DÖV 2008, S. 411 (413).

[143] Entsprechend *Barczak*, in: Dreier, GG, Bd. I, 4. Aufl., i. E., Art. 2 Abs. 1 Rn. 93. Subtile Differenzen zwischen den Schutzbereichen identifiziert *Hauser*, Das IT-Grundrecht, 2015, S. 113 f.

[144] BVerfGE 120, 274 (314, Rn. 204). Dass das Gericht den Aspekt der Integrität im Unterschied zum Vertraulichkeitsschutz nicht schon auf Schutzbereichs-, sondern erst auf Eingriffsebene thematisiert, ist verschiedentlich bemerkt worden, vgl. *Hauser*, Das IT-Grundrecht, 2015, S. 117.

traulichkeitserwartungen bzw. des allgemeinen Persönlichkeitsrechts auch im Verhältnis zum Recht auf informationelle Selbstbestimmung nochmals vor.[145] Allerdings fängt das Gericht diesen Vorstoß sogleich wieder ein: Denn derartige Integritätsbeeinträchtigungen werden nur bei solchen IT-Systemen beanstandet, die „allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten".[146, 147] Angesichts des Fortschritts (intelligenter) Analysetechniken, die selbst aus den Daten von Stromzählern aussagekräftige Persönlichkeitsbilder ableiten können,[148] überzeugt es allerdings schon aus technischen Gründen nur bedingt, zwischen „normalen" IT-Systemen, die nach ihrer „technischen Konstruktion lediglich Daten mit punktuellem Bezug zu einem bestimmten Lebensbereich des Betroffenen" enthalten und die daher „nur" vom Recht auf informationelle Selbstbestim-

[145] Vgl. *Rixen*, in: Sachs, GG, 9. Aufl. 2021, Art. 2 Rn. 73d, zur Bedeutung des Integritätsschutzes als eines grundrechtlichen „Schutzzaunes" gegen Maßnahmen, „die eine Ausspähung, Überwachung oder Manipulation des Systems ermöglichen, also einen späteren Informationseingriff nur vorbereiten"; Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 ergänze „insoweit den insb. von Art. 13 I geschützten real-räumlichen um einen virtuell-informationstechnischen Bereich freier Persönlichkeitsentfaltung".

[146] BVerfGE 120, 274 (314); dazu, dass es auf die technische Disposition des Systems ankommt („enthalten *können*"), nicht auf die tatsächliche Speicherung besonders persönlichkeitsrelevanter Daten, näher *Hauser*, Das IT-Grundrecht, 2015, S. 80. Vgl. weiter auch *Bäcker*, Das IT-Grundrecht, in: Uerpmann-Wittzack (Hrsg.), Das neue Computergrundrecht, 2009, S. 1 (11); *Bäcker*, Vertraulichkeit der Internetkommunikation, in: Rensen/Brink (Hrsg.), Linien der Rechtsprechung, 2009, S. 99 (125 f.).

[147] Wenn BVerfGE 120, 274 (315), fordert, der Betroffene müsse das IT-System „als eigenes" nutzen, nur dann sei ihm eine besondere Vertraulichkeitserwartung zuzugestehen, bildet dies nur bedingt die Erscheinungsformen der heutigen (privaten) IT-Nutzung ab; inwieweit sich aus der Formulierung des Gerichts, die Nutzung eines geschützten Systems könne einem Nutzer auch „zusammen mit anderen zur Nutzung berechtigten Personen" zustehen (ebd.), eine Öffnungsperspektive insbesondere für die Verlagerung von Daten in Cloud-Dienste, also – vereinfacht und typisierend – in eine von Dritten mitbeherrschte Sphäre, entnehmen lässt, bleibt in der Entscheidung offen. Kritisch dazu bereits *Hornung*, Ein neues Grundrecht, CR 2008, S. 299 (303). Weitergehend für die Einbeziehung von (bestimmten) Cloud-Speicherdiensten *W. Hoffmann-Riem*, Grundrechts- und Funktionsschutz für elektronisch vernetzte Kommunikation, AöR 134:4 (2009), S. 513 (531); noch weiter *Gersdorf*, in: Gersdorf/Paal, BeckOK Informations- und Medienrecht, 37. Ed. 1.8.2022, Art. 2 GG Rn. 26 („Nur wenn der Einzelne überhaupt keine Verfügungsgewalt über ein informationstechnisches System mit seinen Daten hat, gelangt das Grundrecht nicht zur Anwendung"); großzügig auch *Hauser*, Das IT-Grundrecht, 2015, S. 94 f., 112; nur andeutungsweise hierzu *Heinemann*, Schutz informationstechnischer Systeme, 2015, S. 155, 170. Siehe auch BVerfGE 141, 220 (304, Rn. 210).

[148] Vgl. die berechtigte Kritik von *Gersdorf*, in: Gersdorf/Paal, BeckOK Informations- und Medienrecht, 37. Ed. 1.8.2022, Art. 2 GG Rn. 25, an dem von BVerfGE 120, 274 (313) als Beispiel für ein „triviales" IT-System angeführten Fall der elektronischen Steuerungsanlage für die Haustechnik.

mung geschützt werden, und jenen sensiblen, *auch* vom IT-Grundrecht geschützten Systemen, die einen „äußerst großen und aussagekräftigen Datenbestand" vorhalten und deren Manipulation daher Einblicke in „wesentliche Teile der Lebensgestaltung einer Person" ermöglichen, zu differenzieren.[149] Dass das Gericht dann die persönlichkeitsrechtliche Relevanz des Systems wiederum rein abstrakt mit Blick auf dessen technische Disposition bestimmen will und wohl pauschal allen Desktopcomputern, Smartphones etc. zugesteht,[150] erleichtert zwar die Handhabung des Grundrechts, lockert jedoch wieder den Zusammenhang zwischen System- und Persönlichkeitsschutz.

Das Changieren des Gerichts zwischen Formalisierung und Vorverlagerung des Grundrechtsschutzes einerseits und enger Rückbindung an das allgemeine Persönlichkeitsrecht andererseits erscheint nur im Ergebnis und auch insoweit nur teilweise überzeugend. Kritikern ist zuzugeben, dass das Gericht seine Ziele ebenso gut durch eine Fortentwicklung des Rechts auf informationelle Selbstbestimmung hätte erreichen können.[151] Als die eigentliche, bisher nur selten gesehene Schwäche des „neuen" Grundrechts erweist sich jedoch weniger die fehlende Balance als die Verengung, die die Diskussion um die grundrechtliche Relevanz von IT-Sicherheit durch ihre Verortung im allgemeinen Persönlichkeitsrecht erfahren hat.

Bevor gleich unter 3. auf diesen Punkt näher einzugehen ist, sollen zuvor noch die für die Rechtfertigung eines (heimlichen[152]) Eingriffs in das IT-Grundrecht geltenden Maßstäbe berichtet werden. Insofern bereits die Manipulation bzw. Infiltration des Zielsystems ein gegenüber der anschließenden (etwa: Kommunikations-)Überwachung eigenständiger Grundrechtseingriff ist, bedarf es hierfür nach allgemeinen Grundsätzen einer eigenen, normenklaren, verhältnismäßigen etc. Befugnisnorm.[153] Angesichts der bereits durch den

[149] BVerfGE 120, 274 (313 f.).

[150] Siehe gerade in § 5 Fn. 146. Vgl. die Beispiele bei BVerfGE 120, 274 (314).

[151] *Eifert*, Informationelle Selbstbestimmung im Internet, NVwZ 2008, S. 521 (522); vgl. ausführlich auch *Gersdorf*, in: Gersdorf/Paal, BeckOK Informations- und Medienrecht, 37. Ed. 1.8.2022, Art. 2 GG Rn. 23, der darauf verweist, dass der EuGH in einer jüngeren Entscheidung (EuGH, C-673/17 v. 1.10.2019, Rn. 69 – Planet49) einen strukturanalogen Sachverhalt – das Setzen von Cookies ohne Wissen der Nutzer, das für sich noch nicht zur Erhebung personenbezogener Daten führt, aber die Integrität des Endgeräts des Nutzers beeinträchtigt – als „Eingriff in die Privatsphäre" gewertet und somit am Grundrecht auf Datenschutz gemessen hat, ohne über die Schaffung eines „neuen" Grundrechts nachzudenken.

[152] Die in BVerfGE 120, 274 entwickelten Maßstäbe beziehen sich nur auf heimliche Maßnahmen; ob Heimlichkeit Tatbestandvoraussetzung ist oder ob sich ein offener Zugriff auf ein IT-System, etwa dessen Durchsicht nach Beschlagnahmung, am IT-Grundrecht messen lassen muss (vgl. *Hornung*, Ein neues Grundrecht, CR 2008, S. 299 [303]; *Gersdorf*, in: Gersdorf/Paal, BeckOK Informations- und Medienrecht, 37. Ed. 1.8.2022, Art. 2 GG Rn. 27), lässt die Entscheidung ebenso wie die Frage nach den dann geltenden Maßstäben offen.

[153] Die Frage, ob sich diese Eingriffe in die Integrität des IT-Systems auf die tradierten einfachrechtlichen Befugnisnormen zur Telekommunikationsüberwachung stützen lassen

Grundrechtstatbestand geforderten hohen Persönlichkeitsrelevanz des Systems ist es nur konsequent, wenn das BVerfG auch im Rahmen der Verhältnismäßigkeitsprüfung eine hohe Eingriffsschwelle definiert und verlangt, dass „tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut vorliegen".[154] Ferner muss der Kernbereichsschutz sichergestellt werden.[155] Der heimliche Zugriff muss zudem grundsätzlich vorab von einem Richter genehmigt werden.[156]

3. Informationssicherheit als übergreifendes Grundrechtsproblem

Die Anerkennung der Bedeutung, die die IT-Sicherheit für das allgemeine Persönlichkeitsrecht hat und der das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme auf seine Weise Rechnung tragen will, darf nicht den Blick darauf verstellen, dass Informationssicherheit nicht exklusiv ein Problem des Privatheitsschutzes, sondern eine „Querschnittsbedingung für die Grundrechtsausübung" ist.[157] Auch wenn diese Beobachtung nicht ganz neu ist, hat sie in der verfassungsgerichtlichen Rechtsprechung bisher kaum Niederschlag gefunden. Zwar hat das BVerfG jüngst in einem Senatsbeschluss den Fokus verbreitert und konstatiert:

„Die Umstellung ehemals analoger Vorgänge auf digitale Prozesse und nicht zuletzt die immer breitere mobile Nutzung informationstechnischer Systeme erhöhen die Abhängigkeit von Informationstechnologie ständig weiter. Die Einzelnen können von *ihren grundrechtlichen Freiheiten* ohne die Nutzung informationstechnischer Systeme immer weniger Gebrauch machen und können sich auch den Gefahren der Nutzung informationstechnischer Systeme immer weniger dadurch entziehen, dass sie auf diese Nutzung verzichten."[158]

Dennoch bleibt der Senat auch hier letztlich der Engführung von Informationssicherheit und allgemeinem Persönlichkeitsrecht verhaftet. Hierfür dürfte auch der typisch „sicherheitsrechtliche" Anlass des Beschlusses – eine Regelung des baden-württembergischen Polizeigesetzes zum Umgang von Polizei-

(§§ 100a I 1; 100g I StPO) oder ob es neuer eigenständiger Ermächtigungsgrundlagen bedarf, ist aus der Dogmatik des Art. 10 GG bekannt, vgl. dazu *Wischmeyer*, in: Dreier, GG, Bd. I, 4. Aufl., i. E., Art. 10 Rn. 102 ff.

[154] BVerfGE 120, 274 (328, Rn. 247); 141, 220 (305, Rn. 212).

[155] Dazu die Nachweise oben in § 5 Fn. 59. Speziell für das IT-Grundrecht *M. Warntjen*, Der Kernbereichsschutz nach dem Online-Durchsuchungsurteil, in: F. Roggan (Hrsg.), Online-Durchsuchungen, 2008, S. 57 ff.

[156] BVerfGE 120, 274 (331 f., Rn. 257 ff.); 141, 220 (306, Rn. 216).

[157] *Heckmann*, Staatliche Schutz- und Förderpflichten zur Gewährleistung von IT-Sicherheit, in: Rüßmann (Hrsg.), FS Käfer, 2009, S. 129 (135).

[158] BVerfG, NVwZ 2021, 1361, Rn. 33 – Hervorhebung T.W.

behörden mit IT-Sicherheitslücken im Kontext der Quellen-TKÜ – verantwortlich sein.

Allerdings sind staatliche Manipulationen der IT-Sicherheit keineswegs nur denkbar, wo es um das Eindringen in IT-Systeme geht, die für „[t]agebuchartige Aufzeichnungen, intime Erklärungen oder sonstige schriftliche Verkörperungen des höchstpersönlichen Erlebens" genutzt werden.[159] Vielmehr ist mit *Poscher* und *Lassahn* zu konstatieren, dass es von der Funktion des manipulierten IT-Systems abhängt, welches Grundrecht durch entsprechende Manipulationen betroffen ist: „IT-Sicherheit geht es um den Schutz von IT-Systemen – nicht als Selbstzweck, sondern als Mittel, um diejenigen Belange zu schützen, denen das bestimmungsgemäße Funktionieren des jeweiligen IT-Systems dient und die durch Lücken in der IT-Sicherheit Schaden zu nehmen drohen."[160] Das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme erfasst somit nur einen kleinen Ausschnitt der möglichen Gefährdungskonstellationen und ist aufgrund seiner Verortung im allgemeinen Persönlichkeitsrecht kein allgemein gültiger Maßstab für aktive staatliche Interventionen im Cyberraum. Wenn etwa das Bundeskriminalamt, wie 2021 geschehen, aktiv Software auf fremde Server einbringt, die zur Abschaltung der für die Verbreitung und Steuerung der Malware Emotet genutzten Infrastruktur führt, hat dies die Integrität von IT-Systemen beeinträchtigt. Doch geschah dies gerade nicht, um einen „äußerst großen und aussagekräftigen Datenbestand" abzuschöpfen.[161] Auch stand die Auswahl der Server in keinem näheren Zusammenhang mit der Persönlichkeit oder den Vertraulichkeitsinteressen der jeweiligen Betreiber – sie zielte vielmehr allein auf die das Botnetz typischerweise gegen den Willen der Serverbetreiber steuernden Kriminellen.

In derartigen Konstellationen bietet das vom BVerfG als Ausprägung des allgemeinen Persönlichkeitsrechts entwickelte Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme wenig Orientierung. Verallgemeinern lässt sich, dass hier wie dort bereits der unautorisierte Zugriff auf das System als Grundrechtseingriff zu klassifizieren ist, auch wenn das staatliche Handeln eigentlich erst im anschließenden Gebrauch des IT-Systems zulasten des Betroffenen liegt – und ungeachtet dessen, dass der Betroffene typischerweise erst in diesem Stadium die staatliche Intervention

[159] BVerfGE 141, 220 (304, Rn. 210).

[160] *Poscher/Lassahn*, Verfassungsrechtliche Dimensionen der IT-Sicherheit, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 7 Rn. 37.

[161] Zu den technischen Details der Operation und der Frage nach der Rechtsgrundlage siehe die Dokumentation der Anhörung des BKA-Präsidenten im Innenausschuss vom 10.2.2021, abrufbar unter https://netzpolitik.org/2021/schadsoftware-bereinigung-bka-nutzt-emotet-takedown-als-tueroeffner-fuer-mehr-befugnisse-und-neue-gesetze/#2021–02–10_Innenausschuss_Protokoll_TOP-14_Emotet. Siehe auch *S. Herpig/D.-K. Kipker*, Emotet-Takedown: Der Zweck heiligt nicht die Mittel, Netzpolitik.org, 18.2.2021.

„spürt". Hingegen ist es nicht zielführend, abseits des allgemeinen Persönlichkeitsrechts am in der Online-Durchsuchungs-Entscheidung eng definierten Begriff des IT-Systems festzuhalten. Besteht etwa im gerade genannten Fall der hoheitlichen Abschaltung einer Schadsoftware keinerlei Interesse an den auf dem Zielsystem gespeicherten personenbezogenen Daten, kann es nicht darauf ankommen, das Vorliegen eines Eingriffs davon abhängig zu machen, ob sich mit Hilfe des Systems Einblicke in „wesentliche Teile der Lebensgestaltung einer Person" gewinnen ließen.[162] Umgekehrt führt die Tatsache, dass vom staatlichen Handeln ein auch unter das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme fallendes System erfasst ist – angesichts der starken Formalisierung dieser Kategorie durch das Bundesverfassungsgericht fällt etwa jedes Smartphone darunter –, nicht dazu, dass die Maßnahme stets an Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG zu messen ist, ähnlich wie sich staatliche Maßnahmen, die „Menschen" betreffen, nicht stets an diesem Grundrecht messen lassen müssen. Vielmehr ist bei der Auswahl des durch die staatliche Manipulation betroffenen Grundrechts maßgeblich auf den Kontext und die Zielsetzung staatlichen Handelns abzustellen. Welche Grundrechte letztlich einschlägig sind, kann nicht abstrakt beantwortet werden, sondern hängt davon ab, in welchen Bereichen und mit welchen Zielen der Staat im Cyberraum aktiv-manipulierend tätig wird.[163] Im Kontext der Emotet-Abschaltung werden, je nach Art der betroffenen Systeme und der technischen Auswirkungen ihrer Trennung vom Botnetz, etwa Art. 2 Abs. 1 GG, Art. 12 GG oder auch Art. 14 GG einschlägig sein. Einer Mitbetroffenheit des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, die – erneut – angesichts des hohen Formalisierungsgrads des Grundrechtstatbestands durch das BVerfG vielfach vorliegen wird, ist auf Ebene der Grundrechtskonkurrenzen Rechnung zu tragen. Das Gericht selbst hat das Problem bereits im Verhältnis von Art. 10 GG und Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG adressiert und konstatiert, dass bei Manipulationen der IT-Sicherheit zum Zwecke der Überwachung laufender Telekommunikation allein Art. 10 GG einschlägig sein soll.[164] Gerade in dieser Konstellation kann die Bestimmung des Konkurrenzverhältnisses zwar nicht überzeugen, weil das staatliche Handeln hier eben auf eine Beeinträchtigung des Vertraulichkeitsinteresses zielt. Die einschlägigen Entscheidungen zeigen aber, dass auch nach Auffassung des Gerichts der Maßstab des IT-Grundrechts nicht unbesehen auf alle IT-sicherheitsbezogenen Eingriffskonstellationen übertragen werden darf.

[162] BVerfGE 120, 274 (313 f.).
[163] Hierzu ausführlich unten § 7.
[164] BVerfGE 120, 274 (309, Rn. 190); 141, 220 (309, Rn. 228).

In gleicher Weise ist das Schrankensystem des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme nicht für alle Eingriffsformen praktikabel. Zum einen ist das System zu sehr auf den heimlichen Eingriff in Vertraulichkeitsinteressen zugeschnitten und lässt sich daher nicht schlicht auf andere Eingriffsformen übertragen. Für die hier einschlägigen Sicherungsmechanismen, etwa den präventiven Richtervorbehalt, besteht bei offenen Manipulationen ein weit geringeres Bedürfnis. Umgekehrt muss an dieser Stelle auf eine empfindliche Lücke in der Rechtfertigungsprüfung des IT-Grundrechts hingewiesen werden. Wohl weil die den Urteilen zu Grunde liegenden Fallkonstellationen dem Gericht den Eindruck vermittelt haben, dass sich das Gefährdungspotential derartiger staatlicher Maßnahmen im Wesentlichen im Verhältnis zum konkret betroffenen, weil überwachten, Grundrechtsträger realisiert, wurden die mit den Manipulationen einhergehenden strukturellen Gefährdungen für die Vertraulichkeit und Integrität der Informationsinfrastrukturen, für die der Staat eine Gewährleistungsverantwortung trägt, nicht hinreichend herausgearbeitet und auch nicht – zumindest nicht nach außen hin sichtbar – in die Abwägung eingestellt. Gerade diese strukturellen Gefährdungen, die nicht unmittelbar zu Lasten des durch die einzelne Maßnahme betroffenen Grundrechtsträgers gehen, sondern die die Aufgabe des Staates zur Gewährleistung der IT-Sicherheit kompromittieren, begründen aber auch abseits des allgemeinen Persönlichkeitsrechts die besondere Sensibilität entsprechenden Staatshandelns.[165] Auf die hier einschlägige, ebenfalls grundrechtlich radizierte staatliche Gewährleistungsverantwortung für die IT-Sicherheit ist sogleich näher einzugehen.[166]

Festhalten lässt sich, dass das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme keineswegs alleiniger Maßstab zur Beurteilung aktiv-manipulativer staatlicher Maßnahmen im Cyberraum sein kann und sollte. Entsprechendes Staatshandeln ist auch dort grundrechtsrelevant, wo kein im Lichte der bisherigen Rechtsprechung hinreichend „vertrauliches" IT-System betroffen ist. Verallgemeinern lässt sich demgegenüber die in der Entscheidung zur Online-Durchsuchung etablierte Vorverlagerung der Eingriffsprüfung. Das Rechtfertigungsprogramm für derartige Maßnahmen muss dann je im Lichte der konkret betroffenen Grundrechte, der gegebenenfalls einschlägigen Schrankenregelungen und auch und vor allem der (objektiven) Folgewirkungen des Eingriffs adjustiert werden.

[165] Vgl. dazu allerdings instruktiv *Roggan*, Die strafprozessuale Quellen-TKÜ und Online-Durchsuchung, StV 2017, S. 821 (828 f.); *Martini*, in: v. Münch/Kunig, GG, 7. Aufl. 2021, Art. 10 Rn. 193.

[166] Siehe § 5 II. Vertiefend dann auch § 7.

II. Grundrechtliche Gewährleistungsverantwortung für die IT-Sicherheit

Die Grundrechte wirken auf das Feld der IT-Sicherheit nicht nur in der Form ein, dass sie staatlichen Eingriffen Grenzen ziehen. Ohnehin tritt keineswegs nur der deutsche Staat als Manipulator der IT-Sicherheit auf. Gefahren für die Integrität und Vertraulichkeit von IT-Systemen drohen vielmehr auch und vor allem durch private Dritte sowie zunehmend durch fremde Staaten. Direktionskraft entfalten die Grundrechte für das staatliche Handeln daher nicht nur, indem sie den Staat darauf verpflichten, bestimmte Aktivitäten zu unterlassen. Vielmehr kann die objektiv-rechtliche Funktion der Grundrechte den Staat zur Einrichtung von Verfahren zur Hebung des Sicherheitsniveaus oder zu sonstigen Schutzvorkehrungen zwingen, um die durch das Handeln Dritter Betroffenen zu schützen.[167]

Eine solche Verantwortung des Staates für die Risiken der Technik gehört seit geraumer Zeit zum gesicherten Bestand der Verfassungsdogmatik.[168] Auf welche normativen Grundlagen sich diese Verantwortung speziell im Falle der IT-Sicherheit stützt und welche konkreten Folgerungen hieraus zu ziehen sind, ist jedoch bisher nicht ausdiskutiert. Dass hier Klärungsbedarf besteht, ergibt sich nicht zuletzt aus dem gerade erwähnten Senatsbeschluss des BVerfG von 2021.[169] Das Gericht hat dort darauf hingewiesen, dass ein immer größerer Teil grundrechtlich relevanter Aktivitäten in den digitalen Raum verlegt wird, sodass die Möglichkeit ihrer Wahrnehmung zunehmend von der Stabilität und Integrität der Informationsinfrastrukturen abhängt. Auch hat es anerkannt, dass die Grundrechte den Staat zum Schutz der IT-Systeme Privater vor Angriffen durch Dritte verpflichten können. Die normativen Grundlagen der hier aufgerufenen Gewährleistungsverantwortung des Staates für die

[167] Eine verfassungsrechtliche Pflicht für staatliche Stellen zur Erhöhung des Informationssicherheitsniveaus kann sich unter Umständen auch aus Normen ergeben, die nicht zu den Grundrechten oder den grundrechtsgleichen Rechten zählen. Diskutiert wird etwa, ob sich ein Anspruch auf sichere Telekommunikation aus Art. 87f Abs. 1 GG ableiten lässt. Dies dürfte allerdings eine Überforderung des Konzepts der Grundversorgung sein, vgl. *Heinemann*, Schutz informationstechnischer Systeme, 2015, S. 211. Auch für die Verfassungsorgane liegt es, je nach Bedrohungslage, nahe, eine verfassungsrechtliche Pflicht zur Sicherung deren jeweiliger Informationsinfrastrukturen aus dem Grundsatz des Erhalts der Funktionsfähigkeit herzuleiten bzw. Ansprüche auf eine angemessene personelle und finanzielle Ausstattung für die damit verbundenen Aufgaben anzuerkennen. Diese Spezialfragen bleiben hier außer Betracht.

[168] Grundlegend BVerfGE 53, 30 (57 f.). Dazu ausführlich bereits oben § 3 II. 2. und § 4 I. 1. sowie die allgemeinen Nachweise zu grundrechtlichen Schutzpflichten oben in § 4 Fn. 18.

[169] BVerfG, NVwZ 2021, 1361.

IT-Sicherheit (1.) hat der Senat allerdings ebenso wenig geklärt wie die Frage, welche konkreten Konsequenzen dies für den Gesetzgeber hat (2.).[170]

1. Maßstäbe: Grundrechtsschutz durch Informationssicherheit

Auch aus objektiv-rechtlicher Sicht gilt, dass die Suche nach den grundrechtlichen Wurzeln der staatlichen Gewährleistungsverantwortung nicht vorschnell auf bestimmte Grundrechte hin verengt werden oder, umgekehrt, losgelöst von konkreten Grundrechtsgarantien operieren darf. Eine allgemeine Pflicht zur Gewährleistung *der* Informationssicherheit existiert ebenso wenig wie eine allgemeine Pflicht zur Gewährleistung *der* technischen Sicherheit oder sonstiger Sicherheiten. Unbestreitbar dient staatliches Handeln, das der Förderung der Informationssicherheit gilt, in aller Regel der Erfüllung des allgemeinen staatlichen Auftrags der Sicherheitsgewährleistung.[171] Hieraus ergibt sich jedoch zunächst nicht mehr, als dass Maßnahmen zur Stärkung der IT-Sicherheit einen legitimen Zweck darstellen und damit Einschränkungen von (Abwehr-)Rechten grundsätzlich rechtfertigen können. Eine Verpflichtung des Staatshandelns auf konkrete Ziele oder Maßnahmen folgt hieraus jedoch noch nicht. Eine solche normative Verdichtung muss vielmehr stets aus einer konkret einschlägigen Grundrechtsgarantie heraus begründet werden.[172] Auch aus objektiv-rechtlicher Sicht ist dabei, wie bereits zur abwehrrechtlichen Seite ausgeführt, die Querschnittsnatur der IT-Sicherheitsfrage zu beachten.

Die frühesten Ansätze zu einem objektiv-rechtlichen Argument für mehr Informationssicherheit finden sich im Zusammenhang mit dem Recht auf informationelle Selbstbestimmung. Wie berichtet, hat die datenschutzrechtliche Literatur seit den 1970er-Jahren betont, dass die vom Gesetzgeber zum Schutz personenbezogener Daten zu treffenden Vorkehrungen auch Informationssi-

---

[170] Zur Schutzdimension der Grundrechte in diesem Zusammenhang näher *Heckmann*, Staatliche Schutz- und Förderpflichten zur Gewährleistung von IT-Sicherheit, in: Rüßmann (Hrsg.), FS Käfer, 2009, S. 129 ff.; *Möllers/Pflug*, Verfassungsrechtliche Rahmenbedingungen des Schutzes kritischer IT-Infrastrukturen, in: Kloepfer (Hrsg.), Schutz kritischer Infrastrukturen, 2010, S. 47 ff.; *Hauser*, Das IT-Grundrecht, 2015, S. 290 ff.; *Heinemann*, Schutz informationstechnischer Systeme, 2015, S. 209 ff.; *J. Stinner*, Staatliche Schutzpflichten im Rahmen informationstechnischer Systeme, 2018, S. 54 ff., 91 ff.; *Poscher/Lassahn*, Verfassungsrechtliche Dimensionen der IT-Sicherheit, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 7 Rn. 40 f.

[171] Siehe dazu oben § 4 I. 1.

[172] *W. Frenz*, Stärkerer staatlicher Schutz vor Cyberangriffen, DVBl. 2019, S. 1021 (1022); *I. Härtel*, Das europäische Datenschutzgrundrecht in der digitalen „Infosphäre", in: Nowak/Thiele (Hrsg.), Effektivität des Grundrechtsschutzes in der Europäischen Union, 2021, S. 103 (118 f.).

cherheitsrisiken abdecken müssen.[173] Da das Recht auf informationelle Selbstbestimmung auch durch Verletzungen der Verfügbarkeit, Integrität und Vertraulichkeit der verarbeiteten Daten tangiert wird, ist es naheliegend, dass der Staat insoweit regulierend eingreift.[174] War die Gefährdungslage in der Frühzeit der Digitalisierung noch diffus, kann heute angesichts der umfassenden und erheblichen Bedrohungslage, der personenbezogene Daten ausgesetzt sind, kein Zweifel mehr daran bestehen, dass die zur Begründung einer grundrechtlichen Schutzpflicht erforderliche abstrakte Gefährdungslage vorliegt. Zwar müssen sich selbstverständlich auch Private für die Sicherheit ihrer IT und der ihnen anvertrauten Daten engagieren. Doch darf der Staat das Feld nicht ganz allein der privaten Vorsorge überlassen.

Prominent aufgegriffen hat das Bundesverfassungsgericht diese Argumentation im Urteil zur Vorratsdatenspeicherung, hier noch im Kontext einer staatlichen Eingriffsermächtigung. Das Gericht hat dabei mit Blick auf die Gefahren eines illegalen Zugriffs auf die bei den Privaten anfallenden Vorratsdaten verlangt, dass „ein besonders hoher Sicherheitsstandard, der über das allgemein verfassungsrechtlich gebotene Maß für die Aufbewahrung von Daten der Telekommunikation hinausgeht", gewährleistet ist.[175] Auch wenn das Grundgesetz „nicht detailgenau" vorgebe, welche Sicherheitsmaßnahmen im Einzelnen geboten seien, unterliege dies einer verfassungsgerichtlichen Nachprüfung. Der Gesetzgeber müsse etwa durch die Verpflichtung zur Orientierung am „Stand der Technik" und durch turnusmäßige Evaluations- und Anpassungspflichten sicherstellen, dass sich die speicherpflichtigen Unternehmen am „Entwicklungsstand der Fachdiskussion" orientieren und „neue Erkenntnisse und Einsichten fortlaufend aufnehmen".[176] Gestützt auf die im gerichtlichen Verfahren durch Anhörung von Sachverständigen gewonnenen Erkenntnisse definiert das Gericht ganz konkrete Minimalstandards: Verlangt werde „grundsätzlich eine getrennte Speicherung der Daten, eine anspruchsvolle Verschlüsselung, ein gesichertes Zugriffsregime unter Nutzung etwa des Vier-Augen-Prinzips sowie eine revisionssichere Protokollierung".[177]

Das Beispiel des Gerichts hat Schule gemacht. Entsprechende Verpflichtungen werden mittlerweile auch aus den unions- und menschenrechtlichen Regeln zum Schutz der Privatheit in Art. 7 und 8 GRCh, Art. 8 EMRK, Art. 17 IPbpR und Art. 12 EMRK abgeleitet, wobei sich Argumentation und Ergeb-

[173] Dazu oben § 2 I. 2.

[174] Zu staatlichen Handlungspflichten im Datenschutzrecht siehe nur *Albers*, Informationelle Selbstbestimmung, 2005, S. 113 ff.; *Britz*, Informationelle Selbstbestimmung, in: Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, 2010, S. 561 ff.; *W. Hoffmann-Riem*, Freiheitsschutz in den globalen Kommunikationsinfrastrukturen, JZ 69 (2014), S. 53 (56 f.).

[175] BVerfGE 125, 260 (325, Rn. 222).

[176] BVerfGE 125, 260 (326, Rn. 224).

[177] BVerfGE 125, 260 (327, Rn. 224).

nis kaum von den hier für das Grundgesetz dargelegten Überlegungen unterscheiden.[178]

Die für das Recht auf informationelle Selbstbestimmung entwickelte Argumentation lässt sich auf alle Grundrechte übertragen, deren Inanspruchnahme auf sichere IT angewiesen ist. In der zitierten Passage aus der Vorratsdatenspeicherungsentscheidung scheint bereits auf, dass auch die aus Art. 10 GG folgende objektiv-grundrechtliche Pflicht, die Vertraulichkeit des Brief- und Telekommunikationsverkehrs vor Übergriffen privater oder fremdstaatlicher Dritter zu schützen,[179] eine IT-Sicherheitsdimension aufweist.[180] Dementsprechend ist der Staat nicht nur daran gehindert, Verschlüsselungstechnologien zu schwächen, die es den Kommunikationsteilnehmern erleichtern, sich vor Eingriffen Dritter zu schützen. Vielmehr muss er private Anbieter von Telekommunikationsdiensten und -netzen zur Einhaltung hinreichender Sicherheitsvorkehrungen für die Kunden verpflichten und darüber hinaus seinerseits die Entwicklung entsprechender Sicherheitspraktiken fördern.

Je nach Grad der digitalen Durchdringung des vom Grundrecht erfassten Sach- und Lebensbereichs gilt Entsprechendes auch für andere Grundrechte,

---

[178] Zum Unionsrecht siehe insbes. EuGH, C-293/12 u. a. v. 8.4.2014, Rn. 65 ff. – Digital Rights Ireland, wo die Gewährleistung der Datensicherheit Art. 8 GRCh zugeordnet wird; vgl. demgegenüber zur Herleitung aus Art. 7 GRCh *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 220. Zur menschenrechtlichen Dimension der Informationssicherheit siehe *M. Dunn Cavelty/C. Kavanagh*, Cybersecurity and Human Rights, in: Wagner/Kettemann/Vieth (Hrsg.), Research Handbook on Human Rights and Digital Technology, 2019, S. 73 ff.; *M. Kettemann*, This is not a drill, in: Wagner/Kettemann/Vieth (Hrsg.), Research Handbook on Human Rights and Digital Technology, 2019, S. 113 ff.; *I. Kilovaty*, An Extraterritorial Human Right to Cybersecurity, Notre Dame J. Int'l & Comp. Law 10 (2020), S. 35 (52 ff.); *Martini*, in: Paal/Pauly (Hrsg.), DS-GVO, 3. Aufl. 2021, Art. 32 Rn. 17i. Von den zuständigen menschenrechtlichen Spruchkörpern ist das Argument allerdings bisher kaum aufgegriffen worden. Allein der EGMR hat als Sicherungsmechanismus bei staatlichen Eingriffen in das Recht aus Art. 8 EMRK verlangt, dass die auf diese Weise erhobenen Daten besonders gegen Zugriff durch Dritte gesichert werden müssen, vgl. EGMR, 24029/07 v. 13.11.2012, Rn. 195 – M. M./UK. Dort wird weitgehend analog zu BVerfGE 125, 260 (325 ff.) festgestellt, dass eine verhältnismäßige Ausgestaltung der Vorratsdatenspeicherung verlangt, dass die Sicherheit der gesammelten Daten gewährleistet ist. Nicht näher thematisiert wird dieser Aspekt allerdings dann in EGMR, 58170/13 u. a. v. 25.5.2021, Rn. 400 ff. – Big Brother Watch/UK.

[179] Dazu allgemein: BVerfGE 106, 28 (37, Rn. 21); BVerfG, NVwZ 2021, 1361, Rn. 32. Entsprechend für Art. 8 EMRK: EGMR, 1874/13 v. 17.10.2019, Rn. 110 ff. – Ribalda. Speziell mit Blick auf den Schutz vor dem Handeln ausländischer Stellen siehe *F. Becker*, Grundrechtliche Grenzen staatlicher Überwachung zur Gefahrenabwehr, NVwZ 2015, S. 1335 (1340); *C. Neubert*, Grundrechtliche Schutzpflicht des Staates gegen grundrechtsbeeinträchtigende Maßnahmen fremder Staaten, AöR 141 (2015), S. 267 (275 f.); *Guckelberger*, in: Schmidt-Bleibtreu/Hofmann/Henneke, GG, 15. Aufl. 2022, Art. 10 Rn. 31.

[180] Vgl. BVerfG, NVwZ 2021, 1361, Rn. 30 ff.; *Groß*, in: Friauf/Höfling, GG, Art. 10 (2016), Rn. 71; *Poscher/Lassahn*, Verfassungsrechtliche Dimensionen der IT-Sicherheit, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 7 Rn. 40 ff.

etwa das Recht auf körperliche Unversehrtheit[181] oder das Eigentum[182]. Die Justizgrundrechte verpflichten den Staat, zum Schutz der Arbeitsfähigkeit der Gerichte entsprechende Maßnahmen zur Sicherung der eigenen IT zu ergreifen; andernfalls leidet der Justizgewährleistungsanspruch.[183] Es bestätigt sich also, dass unter den Bedingungen der Digitalisierung sichere und funktionierende Informationstechnik als allgemeine Wirksamkeitsvoraussetzung der Grundrechte verstanden werden muss.[184]

Neben diese Garantien – nicht an ihre Stelle – tritt schließlich die aus dem allgemeinen Persönlichkeitsrecht abgeleitete Pflicht des Staates, die Vertraulichkeit und Integrität besonders sensibler informationstechnischer Systeme vor Angriffen Dritter zu schützen.[185] Dritte sind dabei neben privaten Akteuren auch Agenten ausländischer Staaten, etwa ausländische Nachrichtendienste.[186] Schon weil die aus dem IT-Grundrecht folgende Schutzgarantie auf besonders persönlichkeitsrelevante IT-Systeme beschränkt ist, lässt sich in ihr eine umfassende staatliche Verantwortung für die Risiken der Informationstechnik nicht verorten. Bemerkenswert ist insoweit, dass das Bundesverfassungsgericht im erwähnten Senatsbeschluss von 2021 bei der Rekonstruktion der objektiv-rechtlichen Dimension des IT-Grundrechts auf den in der Entscheidung zur Online-Durchsuchung geprägten engen Grundrechtstatbestand gar nicht eingeht; stattdessen führt das Gericht aus, dass sich gerade durch die „immer breitere mobile Nutzung informationstechnischer Systeme" die individuelle Abhängigkeit von der Technik gesteigert habe, wodurch es immer schwerer werde, sich den mit ihrer Nutzung verbundenen Gefahren zu

[181] Vgl. das Beispiel bei *Poscher/Lassahn*, Verfassungsrechtliche Dimensionen der IT-Sicherheit, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 7 Rn. 41.

[182] Zu eigentumsrechtlichen Positionen im digitalen Kontext siehe nur *Wischmeyer/Herzog*, Daten für alle?, NJW 2020, S. 288 ff. m. w. N.

[183] Vgl. zum Wirken des Emotet-Virus am Berliner Kammergericht das Gutachten von T-Systems v. 23.12.2019, abrufbar unter https://www.berlin.de/sen/justva/presse/pressemitteilungen/2020/pressemitteilung.887323.php.

[184] Allgemein zu den „Wirksamkeitsvoraussetzungen" des Verfassungsrechts und der Grundrechte *Isensee*, Grundrechtsvoraussetzungen und Verfassungserwartungen, in: Isensee/Kirchhof (Hrsg.), HStR, Bd. IX, 3. Aufl. 2011, § 190.

[185] Zu dieser objektiv-rechtlichen Dimension des IT-Grundrechts siehe BVerfGE 120, 274 (306); *Hoffmann-Riem*, Schutz der Vertraulichkeit und Integrität, JZ 63 (2008), S. 1009 (1019); *M. Sachs/T. Krings*, Das neue „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme", JuS 2008, S. 481 (486); *Heckmann*, Staatliche Schutz- und Förderpflichten zur Gewährleistung von IT-Sicherheit, in: Rüßmann (Hrsg.), FS Käfer, 2009, S. 129 (133 ff.); *Heinemann*, Schutz informationstechnischer Systeme, 2015, S. 209 ff.; *Leuschner*, Sicherheit als Grundsatz, 2018, S. 205 f.; *Derin/Golla*, Der Staat als Manipulant und Saboteur der IT-Sicherheit?, NJW 2019, S. 1111 (1115); *Gersdorf*, in: Gersdorf/Paal, BeckOK Informations- und Medienrecht, 37. Ed. 1.8.2022, Art. 2 GG Rn. 29. Jetzt auch ausdrücklich BVerfG, NVwZ 2021, 1361, Rn. 33.

[186] Speziell zu letzterem *P. Brunst*, Cyberabwehr, in: Dietrich/Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017, S. 817 Rn. 22 f.

entziehen.[187] Ob darin, jedenfalls für die objektiv-rechtliche Grundrechtsdimension, eine Abkehr von der – wie gezeigt wenig überzeugenden – Differenzierung zwischen sensiblen und nicht-sensiblen IT-Systemen liegt, wird in der Entscheidung nicht weiter ausgeführt.[188] Mit Blick auf die weiteren einschlägigen objektiv-rechtlichen Grundrechtsgehalte, die ohnehin eingreifen, erscheint eine entsprechende Fortbildung der Dogmatik des IT-Grundrechts unter dem Gesichtspunkt der Grundrechtseffektivität allerdings auch nicht zwingend geboten.

2. Pflicht zur risikobasierten Regulierung

Die aus der objektiv-rechtlichen Dimension der Grundrechte erwachsenden Handlungspflichten des Gesetzgebers übersetzen sich nicht unmittelbar in ein konkretes Aktionsprogramm. Wie der Gesetzgeber den ihm aus allgemeinen verfassungsrechtlichen Erwägungen zustehenden Einschätzungs-, Wertungs- und Gestaltungsspielraum weiter ausfüllt, liegt zwar – wie das BVerfG formuliert – „nicht außerhalb verfassungsgerichtlicher Kontrolle", kann also durchaus unter Rückgriff auf die verfassungsrechtlichen Wertentscheidungen konkretisiert werden.[189] Im Allgemeinen genügt es jedoch, wenn der Gesetzgeber den Vorwurf entkräften kann, er habe gar keine oder nur solche Schutzvorkehrungen getroffen, die „offensichtlich ungeeignet oder völlig unzulänglich sind, das gebotene Schutzziel zu erreichen, oder [die] erheblich hinter dem Schutzziel zurückbleiben".[190] Wie noch zu zeigen sein wird, kann hiervon schon angesichts der vielfältigen gegenwärtigen Initiativen im Informationssicherheitsrecht letztlich keine Rede sein.[191] Zwar fügen sich die verschiedenen vom Gesetzgeber verfolgten Ansätze bisher nur bedingt zu einem ganzheitlichen „Schutzkonzept"[192]; doch dürfen die weiten Spielräume, die dem Gesetzgeber aus der Warte der grundrechtlichen Schutzpflichten zuzugestehen sind, nicht durch überspannte Kohärenzerwartungen unterminiert werden. Auch ist die Tatsache, dass der Gesetzgeber dort, wo er tätig geworden ist, die Ent-

[187] BVerfG, NVwZ 2021, 1361, Rn. 33.

[188] Angesichts der im Verfahren angegriffenen Maßnahmen – eine polizeirechtliche Befugnisnorm zur Infiltration von IT-Systemen mittels sogenannter Quellen-TKÜ bzw. das Fehlen von Begleitregelungen für ein Schwachstellen-Management zum Umgang mit Sicherheitslücken – konnte dies auch dahinstehen.

[189] BVerfGE 157, 30 (114, Rn. 152). Daran anknüpfend speziell für die IT-Sicherheit BVerfG, NVwZ 2021, 1361, Rn. 50.

[190] So die in st. Rspr. gebräuchliche Formulierung des Ersten Senats, vgl. aus jüngerer Zeit BVerfGE 142, 313 (337 f., Rn. 70); 157, 30 (114, Rn. 152) m. w. N.; BVerfG, NVwZ 2021, 1361, Rn. 50; BVerfG, NJW 2022, 380, Rn. 98.

[191] Zu diesem Prüfungsprogramm vgl. BVerfGE 92, 26 (46); 125, 39 (79 f.); 142, 313 (337 f., Rn. 70); 157, 30 (114, Rn. 152); stRspr.

[192] Zu dieser Begrifflichkeit siehe etwa BVerfGE 125, 39 (78); 157, 30 (114, Rn. 152).

wicklung konkreter Sicherheitsstandards weitgehend an die Verwaltung bzw. an die Prozesse der technischen Standardsetzung delegiert hat, nicht zu beanstanden, sondern kann im Sinne des Grundsatzes eines „dynamischen Grundrechtsschutzes" sogar geboten sein.[193] Hinzu kommt, dass in einer derart stark durch das unionale Recht überformten Materie die Rechtsetzung der europäischen Ebene – bzw. präziser die deutsche Beteiligung an dieser Rechtsetzung – bei der Beurteilung der Frage, ob hinreichende Schutzvorkehrungen getroffen wurden, berücksichtigt werden muss; andernfalls brächte die – verfassungsrechtlich gewünschte – europäische Integration den Gesetzgeber in Konflikt mit seiner grundrechtlichen Schutzverantwortung.[194] Schließlich muss beachtet werden, dass die dem Schutzziel Informationssicherheit dienende Regulierung ihrerseits Grundrechte beeinträchtigen kann;[195] die hieraus resultierende Notwendigkeit einer weiteren Abwägung steht der Ableitung ganz konkreter Schutzmaßnahmen unmittelbar aus dem Verfassungsrecht gleichfalls entgegen.

Dieser allgemeine Befund schließt allerdings nicht aus, dass sich im Einzelfall eine vom Gesetzgeber gewählte Gestaltung als so unzulänglich erweisen kann, dass von Verfassungs wegen mehr oder weniger bestimmte Maßnahmen zu ergreifen sind.

Dies ist zum einen dort der Fall, wo der Staat dafür verantwortlich ist, dass Private an sich gebotene IT-Sicherheitsstandards unterschreiten, oder wo er Private gar zur Schaffung von Gefährdungslagen für die IT-Sicherheit verpflichtet. Eine solche zwischen Abwehrrecht und Schutzpflicht angesiedelte Konstellation lag im Fall der Vorratsdatenspeicherung vor, bei der die Verpflichtung privater Telekommunikationsdiensteanbieter auf ein bestimmtes IT-Sicherheitsniveau das Gewicht des durch die Speicherpflicht eigentlich erstrebten staatlichen Zugriffs auf die Nutzerdaten kompensieren sollte.[196] In der Literatur wird darauf verwiesen, dass dem Staat eine besonders intensive Garantenstellung hinsichtlich integritätsverletzender Zugriffe Dritter zukomme, wenn er durch eigenes Handeln diesen Verletzungen gewissermaßen technisch „Tür und Tor" geöffnet hat.[197] Eine analoge Diskussion wird gegenwärtig zum staatlichen Umgang mit IT-Schwachstellen diskutiert; hierauf

[193] Grundlegend BVerfGE 49, 89 (137); dazu gleich unter § 5 III. 2. b) aa). Vgl. auch *Poscher/Lassahn*, Verfassungsrechtliche Dimensionen der IT-Sicherheit, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 7 Rn. 42, die auch auf die staatliche Forschungs- und Entwicklungspolitik als Baustein zur Erfüllung grundrechtlicher Schutzpflichten hinweisen.

[194] Zu den Unionskompetenzen sogleich unter § 5 III. 1. a) bb).

[195] Siehe oben § 5 I. 1. b).

[196] Siehe oben § 5 Fn. 175.

[197] *Thiel*, Die „Entgrenzung" der Gefahrenabwehr, 2011, S. 283. Plastisch die Formulierung vom „staatlich gelegten Kuckucksei" bei *Hoffmann-Riem*, Schutz der Vertraulichkeit und Integrität, JZ 63 (2008), S. 1009 (1018).

wird noch zurückzukommen sein.[198] Ganz allgemein lässt sich festhalten, dass sich die grundrechtliche Schutzpflicht immer mehr zu einem konkreten Handlungsgebot verengt, je dichter die fragliche Maßnahme in den Kontext staatlichen Eingriffshandelns eingebunden ist.

Eine entsprechende, allerdings weit weniger präzise Je-desto-Formel lässt sich zum anderen mit Blick auf das jeweils drohende Risiko formulieren. Im Detail ist die Qualifizierung und Quantifizierung von Informationssicherheitsrisiken zwar mit erheblichen Unsicherheiten belastet.[199] Auf einer allgemeineren Ebene lassen sich jedoch durchaus aus grundrechtlicher Sicht strukturell riskantere von strukturell weniger riskanten Konstellationen unterscheiden.[200] Ganz in diesem Sinne agiert der Gesetzgeber, wenn er etwa zwischen Pflichten für Betreiber kritischer Infrastrukturen und „Unternehmen im besonderen öffentlichen Interesse" einerseits und solchen für „normale" Unternehmen und Akteure andererseits differenziert.[201] Dieser risikoorientierte Ansatz findet sich auch auf der Ebene der Gesetzesanwendung, wenn etwa Art. 32 Abs. 1 DSGVO die zu treffenden technischen und organisatorischen Maßnahmen von der „unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos" abhängig macht.[202]

III. Zur Organisation hoheitlicher Interventionen in die Informationstechnik

1. Kompetenzrechtliche Determinanten für die Informationssicherheitsregulierung im Mehrebenensystem

a) Gesetzgebungskompetenzen

Jede Form der Regulierung, mit der der Staat seiner Gewährleistungsverantwortung nachkommen will, muss sich in das verfassungsrechtliche Kompetenzregime einfügen. Welche Herausforderungen dies für den zur effektiven Gewährleistung von Informationssicherheit geforderten All-Gefahren-Ansatz begründet, wurde bereits dargestellt.[203] Dennoch sieht sich die Politik in

---

[198] Hierzu BVerfG, NVwZ 2021, 1361, Rn. 50 ff. Vertiefend § 7.

[199] Siehe oben § 4 II. 3.

[200] Vgl. den regulatorischen Neuansatz der U.S. Cybersecurity and Infrastructure Security Agency (CISA), dokumentiert unter https://www.cisa.gov/blog/2021/01/14/risk-based-approach-national-cybersecurity.

[201] Siehe unten § 6 II. 5. c).

[202] Allgemein zum Risikogrundsatz im Datenschutzrecht *O. Lynskey*, The Foundations of EU Data Protection Law, 2015, S. 81 ff.; *R. Gellert*, The Risk-Based Approach to Data Protection, 2020, S. 9 ff.; ein Kurzüberblick bei *M. Schröder*, Der risikobasierte Ansatz in der DS-GVO, ZD 2019, S. 503 ff.

[203] Siehe oben § 4 I. 3. b) cc).

Deutschland und Europa auf die geltende Kompetenzordnung verwiesen, deren Grundzüge hier, soweit relevant, dargestellt werden sollen.[204]

aa) Grundgesetz

Trotz der hohen praktischen Bedeutung, die die Materie erlangt hat, sehen weder das Grundgesetz noch das Unionsprimärrecht gesonderte Kompetenztitel für die Informationssicherheit vor. Entsprechende Bemühungen um eine Hochzonung der Gesetzgebungskompetenzen im Bereich des Katastrophenschutzes und des Schutzes kritischer Infrastrukturen, die auch Folgen für die Regelung der Informationssicherheit hätten haben können, sind – wie berichtet – jedenfalls bisher gescheitert.[205] So ist der Bundesgesetzgeber darauf verwiesen, für seine Aktivitäten in diesem Bereich jeweils punktuell Annexkompetenzen zu sonstigen Kompetenztiteln zu nutzen. Zunächst hat sich der Bund hierzu vor allem auf die Ermächtigungen zur Regulierung einzelner Sektoren gestützt.[206] Je stärker sich die Informationssicherheitsgesetzgebung des Bundes allerdings vom sektoralen KRITIS-Modell in Richtung eines horizontalen, risikobasierten Regulierungsansatzes fortentwickelt, desto plausibler wird es, die im weiten Kompetenztitel des Art. 74 Abs. 1 Nr. 11 GG (Recht der Wirtschaft) enthaltene gefahrenabwehrrechtliche Annexkompetenz als (Haupt-)Kompetenztitel zu nutzen.[207] Soweit daneben zur Stärkung der Informationssicherheit (Eingriffs-)Befugnisse für die Sicherheitsbehörden des Bundes geschaffen werden sollen, muss dies auf die speziellen Titel der Art. 73 Abs. 1 Nr. 1, 9a und 10 gestützt werden.[208]

bb) Unionsrecht

Ähnliches gilt im Unionsrecht.[209] Mangels eines ausdrücklichen Kompetenztitels für die Cybersicherheit stützt die Europäische Union ihr Handeln in diesem Bereich bislang vorwiegend auf den Kompetenztitel des Art. 114 Abs. 1

[204] Vorgaben zur IT-Sicherheit im innerstaatlichen Bereich, vor allem im Bund-Länder-Verhältnis, werden hier ausgeklammert.

[205] Siehe oben § 4 I. 3. b) cc).

[206] Zu den Kompetenztiteln, auf die sich das IT-SiG 2015 gestützt hat, siehe oben § 4 Fn. 89.

[207] *Deutscher Bundestag*, Gesetzesentwurf der Bundesregierung zum IT-SiG 2.0, BT-Drs. 19/26106, S. 31 ff. Vgl. ebd. auch die überzeugenden Ausführungen zum Kriterium der Erforderlichkeit i. S. d. Art. 72 Abs. 2 GG. Fraglich ist, inwieweit sich hierauf auch operative Gefahrenabwehrbefugnisse des BSI stützen lassen, wie sie nun in §§ 7c und 7d BSIG vorgesehen sind; soweit der Gesetzgeber hier ebenfalls auf Art. 74 Abs. 1 Nr. 11 GG rekurriert (*Deutscher Bundestag*, Gesetzesentwurf der Bundesregierung zum IT-SiG 2.0, BT-Drs. 19/26106, S. 71), hätte ein Verweis auf Art. 73 Abs. 1 Nr. 7 GG im konkreten Fall näher gelegen.

[208] Zu den Grundzügen der föderalen Sicherheitsarchitektur siehe die Nachweise oben in § 4 Fn. 80.

[209] Zu den aktuellen Rechtsetzungsvorhaben der Union siehe oben § 1 Fn. 30.

S. 2 AEUV. Dieser wird bekanntermaßen weit verstanden.[210] Laut EuGH umfasst die Binnenmarktkompetenz explizit auch Regelungen zur Herstellung eines einheitlichen Schutzniveaus für die Netz- und Informationssicherheit.[211] Das hat es der Union ermöglicht, sich sowohl in der Gesetzgebung zur Zertifizierung von IT-Produkten als auch bei der Regulierung kritischer Infrastrukturen als regulatorischer Schrittmacher zu etablieren.[212] Auch die für den Aufbau von Vertrauensdiensten maßgebliche eIDAS-Verordnung nutzt diesen Kompetenztitel. Für die Gewährleistung der Sicherheit personenbezogener Daten (vgl. Art. 32 DSGVO) greift parallel Art. 16 Abs. 2 AEUV.[213]

Berühren regulatorische Maßnahmen allerdings Art. 4 Abs. 2 S. 2 EUV, also die „grundlegenden Funktionen des Staates, insbesondere die Wahrung der territorialen Unversehrtheit, die Aufrechterhaltung der öffentlichen Ordnung und den Schutz der nationalen Sicherheit", sind der Unionskompetenz Grenzen gezogen. Dies gilt, wie Art. 4 Abs. 2 S. 3 EUV hervorhebt, insbesondere für die nationale Sicherheit, die „weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten fällt". Auch wenn der EuGH diesen Vorbehalt eng fasst und eine Regelung jedenfalls dann nicht für kompetenzwidrig halten will, wenn sie (nur) mittelbare Auswirkungen auf die Tätigkeit der Nachrichtendienste hat,[214] beschränkt sich die Gestaltungsmacht der Union im Sicherheitsrecht bisher weitgehend darauf, die mitgliedstaatlichen Sicherheitsbehörden in ihrem Handeln zu unterstützen und eine grenzüberschreitende Koordinierung zu gewährleisten (vgl. Art. 67, 74 AEUV).[215] Vor diesem Hintergrund hat

[210] Vgl. im Kontext des Sicherheitsrechts insbes. die erste Entscheidung des EuGH zur Vorratsdatenspeicherung: EuGH, C-301/06 v. 10.2.2009, Rn. 60 ff. – Irland/Europäisches Parlament.

[211] EuGH, C-217/04 v. 2.5.2006, Rn. 48 ff. – ENISA.

[212] Hierauf stützen sich etwa der CSA, die NIS-Richtlinie und jetzt die NIS 2-RL. Kritisch zur Unionskompetenz für den CSA *M. Fischer/D.-K. Kipker/F. Voskamp*, Internationaler Rahmen, in: Kipker (Hrsg.), Cybersecurity, 2020, Kap. 16 Rn. 11 f.

[213] Für weitere sektoral einschlägige unionale Kompetenzgrundlagen, darunter etwa Art. 170 ff. AEUV, siehe *F. Deusch/T. Eggenhofer*, 50.1 IT-Sicherheit, in: Taeger/Pohle (Hrsg.), ComputerR-HdB, Stand: Februar 2021, 50.1, Rn. 249 ff.

[214] EuGH, C-203/15 v. 21.12.2016, Rn. 75 ff. – Tele2 Sverige; EuGH, C-207/16 v. 2.10.2018, Rn. 29 ff. – Ministerio Fiscal; EuGH, C-623/17 v. 6.10.2020, Rn. 44 ff. – Privacy International; EuGH, C-511/18 u. a. v. 6.10.2020, Rn. 99 ff. – La Quadrature du Net u. a. Kritisch dazu *M. Müller/T. Schwabenbauer*, Unionsgrundrechte und Datenverarbeitung durch nationale Sicherheitsbehörden, NJW 2021, S. 2079 (2080 f.). Großzügig auch zur Unionskompetenz im Bereich Cybersicherheit trotz Art. 4 Abs. 2 EUV *Calliess/Baumgarten*, Cybersecurity in the EU, German L. J. 21 (2020), S. 1149 (1164).

[215] Zu Sonderrolle des Grenzschutzes (Frontex) vgl. *A. Mrozek*, Grenzschutz als supranationale Aufgabe, 2013; *M. Lehnert*, Frontex und operative Maßnahmen an den europäischen Außengrenzen, 2014; *R. Bossong*, Der Ausbau von Frontex, in: van Ooyen/Möllers (Hrsg.), Jahrbuch Öffentliche Sicherheit 2020/2021, 2021, S. 707 ff. Zur Kontextualisierung dieser „operativen" Tätigkeiten siehe auch *B. Schöndorf-Haubold*, Auf dem Weg zum Sicherheitskooperationsrecht?, in: Dietrich/Gärditz et al. (Hrsg.), Nachrichtendienste in vernetzter Sicherheitsarchitektur, 2020, S. 3 (10, 12).

die Union umfangreiche legislative Aktivitäten zur Informationskooperation in Sachen IT-Sicherheit entwickelt.[216] Größere Hürden bestehen hingegen nach wie vor, was die Ausgestaltung der „operativen Zusammenarbeit" der Behörden der Mitgliedstaaten betrifft; im Fall der Polizeibehörden ist hier das Einstimmigkeitserfordernis des Art. 87 Abs. 3 S. 1 AEUV zu beachten.

Darüber hinaus verfolgt die Union zunehmend den Aufbau unionseigener Stellen (Agenturen) im Sicherheitsrecht.[217] Auf die für den Bereich Cybersicherheit maßgeblichen Institutionen ist gleich näher einzugehen.[218] Zuvor muss jedoch noch darauf hingewiesen werden, dass die Befugnisse, die die Union diesen Agenturen jenseits der (Informations-)Kooperation und Koordination einräumen kann, durch die Verträge begrenzt wird. Eigene Eingriffsbefugnisse und Zwangsmittel stehen ihnen daher regelmäßig nicht zur Verfügung. Ohnehin können unionseigene Stellen nur in Ausnahmefällen zu operativen Maßnahmen ermächtigt werden (vgl. Art. 88 Abs. 3 AEUV für Europol). Die Ausübung von Hoheitsbefugnissen durch supranationale Stellen erfolgt daher typischerweise nur in enger Zusammenarbeit mit und unter Zustimmungsvorbehalt der nationalen Behörden.[219] Bei aller Dynamik, die die sogenannte „Sicherheitsunion" mittlerweile entfaltet und die sich gerade auch mit dem Thema Cybersicherheit verbindet,[220] setzt die geltende Kompetenz-

[216] Ausführlich zum unionalen Sicherheitsrecht aus jüngster Zeit *K. Schober*, Europäische Polizeizusammenarbeit zwischen TREVI und Prüm, 2017; *F. Krämer*, Europäische Sicherheitsarchitektur, in: Brings-Wiesen/Ferreau (Hrsg.), 40 Jahre „Deutscher Herbst", 2019, S. 39 ff.; *H. Aden*, Europäische Rechtsgrundlagen und Institutionen des Polizeihandelns in: Lisken/Denninger, HdbPolR, 7. Aufl. 2021, Kap. M.; *B. Schöndorf-Haubold*, Europäisches Sicherheitsrecht, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht, Bd. 3, 4. Aufl. 2021, § 68; *dies.*, Europäisches Polizei- und Sicherheitsrecht, in: Terhechte (Hrsg.), Verwaltungsrecht der Europäischen Union, 2022, § 35; *R. Repasi*, Das Recht des Raums der Freiheit, der Sicherheit und des Rechts, in: Hatje/Müller-Graff (Hrsg.), Enzyklopädie Europarecht, Bd. 1, 2. Aufl. 2022, S. 469 ff.

[217] Hierzu im Überblick *Aden*, Europäische Rechtsgrundlagen und Institutionen des Polizeihandelns in: Lisken/Denninger, HdbPolR, 7. Aufl. 2021, Kap. M, Rn. 98 ff.; *Schöndorf-Haubold*, Europäisches Polizei- und Sicherheitsrecht, in: Terhechte (Hrsg.), Verwaltungsrecht der Europäischen Union, 2022, § 35 Rn. 52 ff. Ein weiterer Baustein, auf den hier nicht näher eingegangen wird, sind die auf Art. 83 Abs. 1 AEUV gestützten Mindestvorschriften für Straftaten u. a. im Bereich der Computerkriminalität. Dazu *M. Böse*, Kompetenzen der Union auf dem Gebiet des Straf- und Strafverfahrensrechts, in: ders. (Hrsg.), Enzyklopädie Europarecht, Bd. 11, 2. Aufl. 2021, S. 161 (164 ff.).

[218] Siehe § 5 III. 1. b). Die primär für Fragen der Cybersicherheit verantwortliche ENISA stützt ihr Handeln allerdings nicht auf Art. 67 ff. AEUV, sondern auf die Binnenmarktkompetenz, siehe § 5 Fn. 236.

[219] Zu dieser Organisationsform und – erneut – zum Sonderfall des Art. 42 der VO (EU) 2019/1896 (Frontex-VO) siehe *Schöndorf-Haubold*, Europäisches Polizei- und Sicherheitsrecht, in: Terhechte (Hrsg.), Verwaltungsrecht der Europäischen Union, 2022, § 35 Rn. 123 ff.

[220] Siehe oben § 1 II.

ordnung den Ambitionen der Union, als maßgeblicher Akteur in Sachen Sicherheit zu wirken, nach wie vor Grenzen.[221]

b) Verwaltungskompetenzen

aa) Grundgesetz

Aus der einheitlichen Aufgabe lässt sich weder auf die Befugnisse der an ihrer Umsetzung beteiligten Stellen noch auf eine „Funktionseinheit" des damit befassten Teils der Staatsverwaltung schließen. Die Verteilung der Verwaltungskompetenzen im Bereich Informationsfreiheit folgt daher – mit der Ausnahme des für den staatlichen Innenbereich geltenden Art. 91c GG – dem allgemeinen Schema der Kompetenzverteilung der Art. 83 ff. GG. Allerdings hat der Bund mit dem auf Grundlage des Art. 87 Abs. 3 S. 1 GG errichteten Bundesamts für Sicherheit in der Informationstechnik umfassende Kompetenzen an sich gezogen.[222] Der Landesverwaltung verbleibt daneben im Wesentlichen nur die Verantwortung für die Sicherheit der (landes-)eigenen und der kommunalen Informationstechnik, für die Beratung von Unternehmen und Bürgern sowie für operative Tätigkeiten im Rahmen der Länderzuständigkeit für die Gefahrenabwehr und Strafverfolgung.[223] Sollte sich die Überzeugung durchsetzen, dass die Länder auch mit dieser Restverantwortung überfordert sind und dass daher eine Überführung auch dieser Teilaufgaben in die exklusive Zuständigkeit der Verwaltung des Bundes erforderlich ist, müsste dies durch eine Verfassungsänderung abgesichert werden.[224]

Innerhalb der Bundesverwaltung kommt dem BSI zwar eine zentrale, jedoch keine konkurrenzlose Stellung zu. So hat der Bundesgesetzgeber auch anderen Bundesbehörden, allen voran der Bundesnetzagentur, meist ebenfalls auf Grundlage von Art. 87 Abs. 3 S. 1 GG Verwaltungsaufgaben im Bereich

---

[221] Vgl. auch die Einschätzung bei *Wessel*, Towards EU Cybersecurity Law, in: Tsagourias/Buchan (Hrsg.), Research Handbook on International Law and Cyberspace, 2015, S. 403 (425): „While the EU is usually able to find a connection to existing competences, allowing it to produce new legislation in many different fields, it suffers from the fact that it is not always easy (and sometimes even impossible) to combine the different cybersecurity dimensions in consistent or even connected policies." Positiver hingegen *Carrapico/Barrinha*, The EU as a Coherent (Cyber)Security Actor?, JCMS 55:6 (2017), S. 1254 ff.

[222] Zur fast unbegrenzten Möglichkeit des Bundes, über Art. 87 Abs. 3 S. 1 GG bundeseigene Oberbehörden auf- und auszubauen, näher *Wischmeyer*, Der Verfassungsschutzverbund, in: Dietrich/Gärditz et al. (Hrsg.), Nachrichtendienste in vernetzter Sicherheitsarchitektur, 2020, S. 35 (52 f.).

[223] Vgl. die umfassende Dokumentation der in Ländern und Kommunen mit Fragen der Informationssicherheit befassten Akteure bei *S. Herpig/C. Rupp*, Deutschlands staatliche Cybersicherheitsarchitektur, 8. Aufl. 2022, S. 152 ff., 215 ff.

[224] Zu entsprechenden Überlegungen siehe *H. Bubrowski*, Faeser will Grundgesetz für Cybersicherheit ändern, F.A.Z., 12.7.2022.

der Informationssicherheit zugewiesen.[225] Hinzu kommt, dass neben den für die „zivile Sicherheit"[226] zuständigen Fachbehörden auch die spezialisierten Sicherheitsbehörden (u. a. das BKA), Dienste (BfV und BND) und die Bundeswehr in ihren jeweiligen Zuständigkeitsbereichen Kompetenzen im Bereich IT-Sicherheit aufbauen.[227]

Hierdurch entstehen umfassende Koordinierungsnotwendigkeiten. Zu diesem Zweck wurde schon 2011 das – in dieser Arbeit bereits unter dem Aspekt der dort kombinierten „Sicherheitslogiken" betrachtete[228] – Nationale Cyber-Abwehrzentrum (NCAZ) durch interadministrative Kooperationsvereinbarungen auf der Basis eines Kabinettsbeschlusses als Informationsverbund geschaffen. Teilnehmer des derzeit vom BKA koordinierten NCAZ sind BSI, BBK, Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Sicherheitsbehörden (u. a. Bundespolizei und BKA), Dienste (BfV, MAD und BND) und die Bundeswehr.[229] Die Struktur des NCAZ orientiert sich an der des Gemeinsamen Terrorismusabwehrzentrums (GTAZ). Wie dort besteht die Funktion des NCAZ in der Erleichterung des Informationsaustauschs zwischen den beteiligten Behörden über technische Fragen der IT-Sicherheit (etwa Sicherheitslücken), abstrakte Gefährdungslagen und allgemeine IT-bezogene Risiken. Auf dieser Grundlage wird eine „nationale Cybersicherheitslage" aufbereitet. Mit Blick auf die Verwaltungskompetenzen des Bundes begegnet dieses informationelle Kooperationsformat keinen Bedenken. Insbesondere greift Art. 87 Abs. 3 S. 1 GG nicht. Unproblematisch ist daher auch, dass der Informationsverbund im Frühjahr 2021 auf die Länderebene ausgeweitet wurde; so können jetzt auch spezialisierte (Landes-)Staatsanwaltschaften und sonstige Landesbehörden am NCAZ mitwirken.

---

[225] Dazu vertiefend unten § 6 II. 3. c).

[226] Zu diesem Konzept oben § 4 I. 2. c).

[227] Vgl. die Dokumentation bei *Herpig/Rupp*, Deutschlands staatliche Cybersicherheitsarchitektur, 8. Aufl. 2022, S. 110 ff.

[228] Siehe oben § 4 II. 3.

[229] Siehe die Darstellung unter https://www.bka.de/DE/UnsereAufgaben/Kooperationen/NCAZ/ncaz_node.html. Zum NCAZ vgl. *M. Fremuth*, Wächst zusammen, was zusammengehört?, AöR 139 (2014), S. 32 (64 f.); *T. Linke*, Rechtsfragen der Einrichtung und des Betriebs eines Nationalen Cyber-Abwehrzentrums, DÖV 2015, S. 128 ff.; *Leisterer*, Internetsicherheit in Europa, 2018, S. 51 f., 275 ff.; *Herpig/Bredenbrock*, Cybersicherheitspolitik in Deutschland – Akteure, Aufgaben und Zuständigkeiten. Im Fokus: Das Cyber-Abwehrzentrum, April 2019; *Herpig/Rupp*, Deutschlands staatliche Cybersicherheitsarchitektur, 8. Aufl. 2022, S. 149. Zur Rolle der Bundeswehr im NCAZ *Spies-Otto*, Aufgaben und Befugnisse der Bundeswehr, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 19 Rn. 39 ff. Zum Kontext *W. Cremer*, Organisationen zum Schutz von Staat und Verfassung, in: Isensee/Kirchhof (Hrsg.), HStR, Bd. XII, 3. Aufl. 2014, § 278 Rn. 15; *K. Räuker/M. Dombert*, Am Beispiel der deutschen Sicherheitsarchitektur: Zum Grundrechtsschutz durch Organisation, DÖV 2014, S. 414 ff.

Die fehlende gesetzliche Grundlage führt jedoch dazu, dass dem Informationsaustausch im NCAZ enge Grenzen gezogen sind.[230] So kann im NCAZ keine dauerhafte analytische oder operative Zusammenarbeit erfolgen.[231] Das Zentrum darf insbesondere nicht selbst personenbezogene Daten sammeln, auswerten oder als Plattform für den Austausch personenbezogener Daten fungieren.[232] Besteht hierzu Anlass, müssen die beteiligten Stellen vielmehr auf die ihnen sonst durch Gesetz eingeräumten Möglichkeiten des Informationsaustauschs zurückgreifen. Die Grundrechte schlagen insoweit auf die Organisationsgestaltung durch. Sollte dies geändert werden und eine eigenständige Behörde mit entsprechenden außenrechtlichen Befugnissen geschaffen werden, bedürfte es nach allgemeinen Regeln eines Gesetzes.[233] Auf Basis der geltenden Rechtslage ist es durchaus konsequent, dass das NCAZ bisher nur ein geringes Maß an Aktivitäten entfaltet hat.[234]

---

[230] *M. Ladiges*, Der Cyberraum, NZWehrr 2017, S. 221 (232); *Spies-Otto*, Aufgaben und Befugnisse der Bundeswehr, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 19 Rn. 43.

[231] Vgl. die Antwort der Bundesregierung auf die Kleine Anfrage „Die Strategie der Bundesregierung zur Bekämpfung der Internetkriminalität – Das Nationale Cyber-Abwehrzentrum" v. 2.5.2011, BT-Drs. 17/5694, S. 3, wonach im NCAZ „keine dauerhaft analytische und keine operative Zusammenarbeit" stattfindet. Siehe auch *K. Graulich*, in: Schenke/Graulich/Ruthig, 2. Aufl. 2018, BKAG, § 2 Rn. 26.

[232] Vgl. *F. Rachor/F. Roggan*, Organisation der Sicherheitsbehörden und Geheimdienste in Deutschland, in: Lisken/Denninger, HdbPolR, 7. Aufl. 2021, Kap. C., Rn. 151.

[233] Der Streit um die Notwendigkeit einer Rechtsgrundlage für das NCAZ und für vergleichbare Zentren betrifft zum einen die Frage, wann die Organisationsstruktur hinreichend verfestigt ist, um den „institutionellen" Gesetzesvorbehalt auszulösen" – dies wird angesichts der zurückhaltenden Maßstäbe eher zu verneinen sein, vgl. *F. Kirchhof*, in: Dürig/Herzog/Scholz, GG, Art. 83 (2021), Art. 83 Rn. 45 –, und zum anderen die Frage, ob sich das NCAZ tatsächlich auf die Anbahnung der Informationsvermittlung beschränkt – letzteres hängt von der gelebten Praxis ab. Angesichts des weiten Verarbeitungsbegriffs und der im Zentrum nur begrenzt vorhandenen Analysekapazität dürfte ein eigenständiger Beitrag des Zentrums zur Datenverarbeitung allerdings nahe liegen, was nach den oben zum Recht auf informationelle Selbstbestimmung ausgeführten Grundsätzen eine gesetzliche Grundlage erforderlich machen würde. Zur Kontroverse siehe die Aufarbeitung durch *Deutscher Bundestag – Wissenschaftliche Dienste*, Sachstand: Gemeinsames Terrorismusabwehrzentrum (GTAZ). Rechtsgrundlagen und Vergleichbarkeit mit anderen Kooperationsplattformen, 19.12.2018, WD 3 – 3000 – 406/18, S. 15 f.; *N. Bergemann*, Nachrichtendienste und Polizei, in: Lisken/Denninger, HdbPolR, 7. Aufl. 2021, Kap. H., Rn. 168. Einen Verstoß des NCAZ gegen das sogenannte „Trennungsgebot" bzw. gegen das „informationelle Trennungsprinzip (BVerfGE 133, 277 [329]) diskutiert und verneint überzeugend *Leisterer*, Internetsicherheit in Europa, 2018, S. 275 ff.

[234] In einem vertraulichen Bericht hat der Bundesrechnungshof die Einrichtung des NCAZ aus diesem Grund scharf kritisiert, vgl. *Goetz/Leyendecker*, Das Problem mit der Wirklichkeit, S.Z., 7.6.2014, S. 5.

bb) Unionsrecht

Auch auf unionaler Ebene vermehrt sich die Zahl der für die Informationssicherheit zuständigen Einrichtungen stetig. Die Aktivitäten der Union reichen dabei von der bloßen Informationssammlung und Koordinierung horizontaler mitgliedstaatlicher Aktivitäten in diversen Netzwerken bis hin zur Institutionalisierung eigenständiger supranationaler Institutionen.[235]

Parallel zum BSI wurde durch VO (EG) Nr. 460/2004 auf der Grundlage der Binnenmarktkompetenz[236] ENISA als zentrale Behörde für Cybersicherheit eingerichtet. Die Behörde nahm im September 2005 als „European Network and Information Security Agency" ihren Dienst auf. Seit 2019 firmiert sie, unter Beibehaltung des alten Akronyms, als „European Union Agency for Cybersecurity". Seit Jahren hat ENISA einen ständigen Aufgabenzuwachs zu verzeichnen. Daneben existieren zahlreiche weitere Stellen, deren Aufgabenspektrum von der Forschungsförderung über die Bekämpfung der Cyberkriminalität bis hin zu Formaten der militärischen Zusammenarbeit reicht.[237] Jüngste Ergänzungen sind das auf die Kompetenzen der EU im Bereich der Technologieförderung (Art. 173 Abs. 3, 188 Abs. 1 AEUV) gestützte Europäische Kompetenzzentrum für Cybersicherheit und das daran angeschlossene Netz nationaler Koordinierungszentren, die gemeinsam zur Stärkung von Forschung und Entwicklung im Bereich der Informationssicherheit beitragen sollen.[238]

---

[235] Zu diesen Vertikalisierungs- und Zentralisierungstendenzen frühzeitig bereits *B. Schöndorf-Haubold*, Europäisches Sicherheitsverwaltungsrecht, 2010, S. 51 ff.; siehe dazu jetzt *dies.*, Europäisches Polizei- und Sicherheitsrecht, in: Terhechte (Hrsg.), Verwaltungsrecht der Europäischen Union, 2022, § 35.

[236] Zur seinerzeit streitigen Frage, inwieweit die Rechtsangleichungskompetenz des ex-Art. 95 EGV auch die Einrichtung von Unionsagenturen trägt, EuGH, C-217/04 v. 2.5.2006 – ENISA, Rn. 42 ff. Dazu vertiefend *J. Saurer*, Die Errichtung von Europäischen Agenturen, DÖV 2014, S. 549 ff. Jetzt wieder kritisch zur Frage, ob Art. 114 AEUV die durch Art. 7 CSA gestärkten operativen Befugnisse von ENISA tragen kann, *Fischer/Kipker/Voskamp*, Internationaler Rahmen, in: Kipker (Hrsg.), Cybersecurity, 2020, Kap. 16 Rn. 11 ff.

[237] Vgl. die Dokumentation bei *Europäischer Rechnungshof*, Herausforderungen für eine wirksame Cybersicherheitspolitik der EU, März 2019, S. 27 ff. und passim; *Herpig/Rupp*, Deutschlands staatliche Cybersicherheitsarchitektur, 8. Aufl. 2022, S. 62 ff. Zur Koordinierungsfunktion von Europol, die insbes. durch das Europäische Zentrum zur Bekämpfung von Cyberkriminalität (EC3) und die dortige Joint Cybercrime Action Taskforce wahrgenommen wird und die der des BKA nicht unähnlich ist, näher *M. Monroy*, Cybersecurity-Initiativen als Teil einer Technologieoffensive, Vorgänge 2015, S. 54 ff. Den Aufwuchs der europäischen Behördenlandschaft als Reaktion auf die Inhomogenität der mitgliedstaatlichen Cybersicherheitsstrategien erklärt *E. Moechel*, EU erhielt die zwölfte Cybersicherheitsorganisation, FM4, 4.7.2021.

[238] Vgl. Verordnung (EU) 2021/887 vom 20.5.2021 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren, ABl. L 202, S. 1. Dazu *C. Gräfin von Wintzingerode/D. Müllmann/I. Spiecker gen. Döhmann*, Ein Netzwerk für Europas Cybersicherheit, NVwZ 2021, S. 690 ff.

Unter den auf Grundlage der Art. 67 ff. AEUV errichteten, also dem Raum der Freiheit, der Sicherheit und des Rechts (RFSR) zuzuordnenden, unionseigenen Akteuren nehmen vor allem die Agenturen Europol, Eurojust und eu-LISA (Betreiberin der IT-Großsysteme im RFSR) Funktionen im Bereich der Cybersicherheitsgewährleistung wahr.[239] Weitere Aufgaben obliegen den Organen der Union selbst, allen voran der Europäischen Kommission[240] und dem Rat[241].

Auch hier wirft die Multiplizierung der Institutionen weniger verfassungsrechtliche als verwaltungspraktische Probleme der Koordinierung und Durchsetzung auf.[242] So ist etwa die Zuständigkeit zur Koordination bei länderübergreifenden Cybersicherheitsvorfällen auf eine derart große Zahl von Stellen und Netzwerken verteilt, dass eine konzertierte Antwort der Union im Krisenfall überaus unwahrscheinlich ist.[243] Um die Defizite des Status quo zu beheben, treibt die Kommission gegenwärtig den Aufbau einer Gemeinsamen Cyber-Einheit (Joint Cyber Unit – JCU) voran, die auf Unionsebene das Handeln der unionalen Stellen bündeln[244] und eine „koordinierte Reaktion der

---

[239] Vgl. *Herpig/Rupp*, Deutschlands staatliche Cybersicherheitsarchitektur, 8. Aufl. 2022, S. 62 ff.

[240] Innerhalb der Kommission verteilen sich die Zuständigkeiten für Cybersicherheitspolitik insbes. auf die Generaldirektionen CNECT (Cybersicherheit), HOME (Cyberkriminalität) und CONNECT (Zuständigkeit für ENISA), je nachdem, ob der digitale Binnenmarkt oder die Sicherheitsunion betroffen sind. Auch das CERT-EU ist direkt bei der Kommission angesiedelt.

[241] Näher dazu *Herpig/Rupp*, Deutschlands staatliche Cybersicherheitsarchitektur, 8. Aufl. 2022, S. 73, 78.

[242] Vgl. beispielhaft das ungeklärte Verhältnis von Europäischem Kompetenzzentrum und ENISA: *Gräfin von Wintzingerode/Müllmann/Spiecker gen. Döhmann*, Ein Netzwerk für Europas Cybersicherheit, NVwZ 2021, S. 690 (693).

[243] Siehe dazu die Empfehlung (EU) 2017/1584 der Kommission vom 13.9.2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen, ABl. L 239/36. Zur Umsetzung haben die Mitgliedstaaten 2020 das EU Cyber Crisis Liaison Organisation Network (EU CyCLONe) zur freiwilligen Koordinierung der Cyberkrisenmanagement-Institutionen der Mitgliedstaaten geschaffen. Die NIS 2-Richtlinie soll eine gesetzliche Basis für eine verstärkte Kooperation schaffen. Mit Aufgaben der Krisenbewältigung sind allerdings parallel, mit je leicht unterschiedlichem Fokus, betraut: das Europäische Zentrum zur Bekämpfung der Cyber-Kriminalität (EC3) mit seiner Joint Cybercrime Action Taskforce (J-CAT); Europol; die Kooperationsgruppe unter der NIS-Richtlinie (NIS Cooperation Group); das beim Europäischen Auswärtigen Dienst angesiedelte Zentrum für Informationsgewinnung und -analyse (INTCEN EU). Ebenfalls mit der Antwort auf Cyberkrisen befassen sich die Schlussfolgerungen des Rates zu einem Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten (Cyber Diplomacy Toolbox) vom 19.6.2017 (9916/17) und diverse Projekte im Rahmen der Ständigen Strukturierten Zusammenarbeit (PESCO); zu den Cyber-Aktivitäten im Rahmen von PESCO siehe *Miadzvetskaya/Wessel*, The Externalisation of the EU's Cybersecurity Regime, European Papers 7 (2022), S. 413 (425 ff.).

[244] Empfehlung (EU) 2021/1086 der Kommission vom 23.6.2021 zum Aufbau einer Gemeinsamen Cyber-Einheit, ABl. L 237/1. An der JCU beteiligt sind ENISA, Europol, CERT-EU, INTCEN EU, das CSIRTs Netzwerk, EU CyCLONe sowie diverse unterstützende Stellen.

EU auf Cybersicherheitsvorfälle und -krisen sowie eine koordinierte Folgenbewältigung gewährleisten" soll.[245] Anders als auf nationaler Ebene das NCAZ soll sich die JCU dabei laut der Kommissionsempfehlung nicht auf den Informationsaustausch und auf technische Unterstützung beschränken, sondern auch eine „operative" Ebene enthalten, deren Umfang und Details aus der Kommissionsempfehlung allerdings nicht hervorgehen.[246] Grundlage des operativen Tätigwerdens sollen die operativen Ressourcen von Europol (vgl. Art. 88 Abs. 3 AEUV) und ENISA (Art. 114 AEUV i. V. m. Art. 7 CSA) sein. Ob es hier zur Übertragung von Eingriffsbefugnissen an die JCU kommt und wie dies mit den Kompetenzschranken der Union im Sicherheitsrecht vereinbar wäre, lässt sich derzeit nicht sicher ausmachen. Unabhängig davon gilt es, im Rahmen der konkreten Ausgestaltung der JCU und der von ihr betriebenen Kooperationen mit den mitgliedstaatlichen Stellen den Grundsatz der Verantwortungsklarheit zu wahren.[247]

2. Demokratische Legitimation der Informationssicherheitsverwaltung

Die Organisation des staatlichen Handelns im Feld der Informationssicherheit muss sich nicht nur an den kompetenzrechtlichen Vorgaben für die Politikgestaltung im Mehrebenensystem messen lassen, sondern auch ein hinreichendes Legitimationsniveau gewährleisten. Schwierigkeiten bereitet es hier – jedenfalls aus Sicht des deutschen Verfassungsrechts –, wenn vorgeschlagen wird, nach unionalem Vorbild die Durchführung des Informationssicherheitsrechts einer vom ministeriellen Weisungszug entkoppelten unabhängigen Behörde anzuvertrauen (a.).[248] Legitimationsfragen wirft ferner die im Informationssicherheitsrecht – wie auch sonst im Technikrecht – anzutreffende Praxis auf, wonach sich der Gesetzgeber auf eine Grobsteuerung der Materie

[245] Empfehlung (EU) 2021/1086 der Kommission vom 23.6.2021 zum Aufbau einer Gemeinsamen Cyber-Einheit, ABl. L 237/1, Ziff. 4.

[246] Empfehlung (EU) 2021/1086 der Kommission vom 23.6.2021 zum Aufbau einer Gemeinsamen Cyber-Einheit, ABl. L 237/1, ErwGr 5, 9 und insbes. Ziff. 4: „Die operativen Teilnehmer sollten in der Lage sein, innerhalb der Gemeinsamen Cyber-Einheit rasch und effektiv operative Ressourcen für die gegenseitige Unterstützung zu mobilisieren."

[247] Zum Changieren des operativen Handelns unionaler Stellen zwischen dem Modus horizontaler Kooperation (Tätigkeit auf nationaler Rechtsgrundlage im Wege der Organleihe) und dem Modus vertikaler Kooperation (Tätigkeit in Ausübung supranationaler Befugnisse) und den daraus resultierenden Zurechnungsproblemen *Schöndorf-Haubold*, Europäisches Polizei- und Sicherheitsrecht, in: Terhechte (Hrsg.), Verwaltungsrecht der Europäischen Union, 2022, § 35 Rn. 134 ff.

[248] Für ENISA, die gemäß Art. 3 Abs. 3 CSA als unabhängige Agentur organisiert ist, stellt sich diese Frage aufgrund des insoweit permissiven Unionsverfassungsrechts (siehe § 5 Fn. 254) nicht, sodass sich die folgenden Ausführungen auf die deutsche (Verfassungs-) Rechtslage konzentrieren.

beschränkt und die Konkretisierung seiner Vorgaben Behörden oder gar Privaten überlässt (b.).

a) Unabhängige Behörden?

Nach geltender Rechtslage ist die für die deutsche Informationssicherheitsverwaltung zentrale Stelle, das Bundesamt für Sicherheit in der Informationstechnik (BSI), als Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern und für Heimat (BMI) organisiert, § 1 S. 1 BSIG. Dem Bundesamt ist heute eine Vielzahl unterschiedlicher Aufgaben anvertraut, die von der der Normsetzung bis hin zum operativen Tätigwerden reichen (vgl. § 3 BSIG). Die Behörde nimmt in erster Linie Aufgaben aus dem Bereich der „zivilen" Sicherheit wahr. Sie hat sich jedoch nie vollständig von ihren Ursprüngen im Reich der Nachrichtendienste gelöst[249] und übernimmt weiterhin einzelne Funktionen für die Sicherheitsbehörden[250]. In erster Linie auf diese Kooperationen zielt es, wenn immer wieder kritisiert wird, die Einordnung des BSI in den Geschäftsbereich des BMI kompromittiere den zivilen Sicherheitsauftrag der Behörde; um eine Verquickung mit den Interessen insbesondere der Gefahrenabwehrbehörden und Dienste – im Geschäftsbereich des BMI sind bekanntlich auch das Bundesamt für Verfassungsschutz und die Bundespolizei angesiedelt – zu vermeiden, sei das BSI in die Unabhängigkeit zu entlassen, also „ministerialfrei" zu stellen.[251] Während diese Forderung im

[249] Historisch hat sich das BSI aus der in den 1950er-Jahren geschaffenen „Zentralstelle für das Chiffrierwesen" entwickelt, die zunächst Zuarbeiten für Bundeskanzleramt und Bundesnachrichtendienst erledigte. Vgl. dazu bereits *A. Roßnagel/J. Bizer*, Sicherheit in der Informationstechnik, Kritische Justiz 23 (1990), S. 436 ff.; *A. Roßnagel/J. Bizer et al.*, Ein Bundesamt für die Sicherheit in der Informationstechnik, DuD 14 (1990), S. 178 ff.; *H. Neusel*, Aktivitäten der Bundesregierung zur IT-Sicherheit, RDV 1990, S. 161 ff.; zusammenfassend *E. Buchberger*, in: Schenke/Graulich/Ruthig, 2. Aufl. 2018, BSIG, § 1 Rn. 1. Nach kleineren Reformen in den späten 1980er-Jahren wurde die Stelle mit dem Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik vom 17.12.1990 (BSIG), BGBl. I S. 2834, in Kraft getreten am 1.1.1991, aus dem nachrichtendienstlichen Organisationszusammenhang gelöst. Das BSI verblieb jedoch als zivile Bundesoberbehörde im Geschäftsbereich des BMI.

[250] Vgl. §§ 3 Abs. 1 Nr. 13; 5 Abs. 5 und 6 BSIG. Zusammenfassend zu den Unterstützungsleistungen, die das BSI für die Nachrichtendienste, Strafverfolgungs- und Gefahrenabwehrbehörden erbringt, sowie zu den eigenen Befugnissen des BSI in Sachen Gefahrenabwehr *M. Bäcker/S. Golla*, Schutz der IT-Sicherheit durch Gefahrenabwehr, Strafverfolgung und nachrichtendienstliche Aufklärung, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 18 Rn. 33 ff. Immer wieder wird in diesem Zusammenhang auch an die Beteiligung des BSI an der Entwicklung des „Bundestrojaners" erinnert. Vgl. dazu die Dokumentation interner Schreiben des BMI unter https://netzpolitik.org/2015/geheime-kommunikation-bsi-programmierte-und-arbeitete-aktiv-am-staatstrojaner-streitet-aber-zusammenarbeit-ab/.

[251] Zu dieser Forderung vgl. die Nachweise bei *Wischmeyer*, Informationssicherheitsrecht, DV 50 (2017), S. 155 (166 f.). Siehe auch ausführlich *Leisterer*, Internetsicherheit in

internationalen Vergleich kaum exotisch anmutet, unabhängige Behörden dort vielmehr ein vertrautes Bild sind,[252] lassen sie sich mit dem tradierten deutschen Modell der Verwaltungslegitimation nicht leicht vereinbaren. Dieses verlangt für einen hinreichenden Legitimationszusammenhang über die Bindung der Verwaltung durch das Parlamentsgesetz hinaus typischerweise zusätzliche personell-organisatorische Rückkoppelungsmechanismen zur Verwaltungsspitze bzw. zur Regierung, zu denen auch die ministerielle Weisungsbefugnis zählt.[253] Entsprechende Überformungen, die die deutsche Rechtsordnung durch das dem Unabhängigkeitskonzept offener gegenüberstehende Unionsrecht (vgl. Art. 298 Abs. 1 AEUV)[254] zunächst im Regulierungs- und Datenschutzrecht[255] und jetzt im Recht der Finanzmarktregulie-

Europa, 2018, S. 280 ff. Zu den verschiedenen Dimensionen der Unabhängigkeit von Behörden – für das BSI wird eine sachlich-inhaltliche Unabhängigkeit gefordert – siehe *M. Ruffert*, Verselbständigte Verwaltungseinheiten, in: Trute/Groß et al. (Hrsg.), Allgemeines Verwaltungsrecht, 2008, S. 431 (447 ff.); *A.-K. Kaufhold/K. Langenbucher/P. Blank/J. Krahnen*, BaFin (in)dependence, März 2021, S. 6 ff.

[252] Vgl. aus der Literatur mit vergleichender Perspektive nur *G. Majone*, Regulatory State, West European Politics 22 (1999), S. 1 ff.; *M. Thatcher*, Regulation After Delegation, Journal of European Public Policy 9 (2002), S. 954 ff.; *F. Gilardi*, Delegation in the Regulatory State, 2008; J. Masing/G. Marcou (Hrsg.), Unabhängige Regulierungsbehörden, 2010; M. Kröger/A. Pilniok (Hrsg.), Unabhängiges Verwalten in der Europäischen Union, 2016; *A. Orator*, Möglichkeiten und Grenzen der Einrichtung von Unionsagenturen, 2017, S. 285 ff.; sowie die die Beiträge von *D. Halberstam*, *L. Sossin*, *M. Prado, J. Yeh*, *A. Thiruvengadam* und *M. Shapiro* in P. Lindseth/S. Rose-Ackerman (Hrsg.), Comparative Administrative Law, 2. Aufl. 2017.

[253] Vgl. aus der Literatur zur deutschen Verfassungsrechtslage nur *M. Jestaedt*, Demokratieprinzip und Kondominialverwaltung, 1993, S. 265 ff.; *E.-W. Böckenförde*, Demokratie als Verfassungsprinzip, in: Isensee/Kirchhof (Hrsg.), HStR, Bd. II, 3. Aufl. 2004, § 24 Rn. 11 ff.; *S. Bredt*, Die demokratische Legitimation unabhängiger Institutionen, 2006; *M. Ludwigs*, Die Bundesnetzagentur auf dem Weg zur Independent Agency?, DV 44 (2011), S. 41 (46 ff.); *H.-H. Trute*, Die demokratische Legitimation der Verwaltung, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 3. Aufl. 2022, § 9 Rn. 66 ff. Zu den Idealisierungen, mit denen das Modell gerade mit Blick auf das Weisungsrecht arbeitet, *T. Groß*, Verantwortung und Effizienz in der Mehrebenenverwaltung, in: VVDStRL 66 (2007), S. 152 (170 f.). Zur legitimationstheoretischen Funktion der Weisung vertiefend *J. Schemmel*, Die demokratische Weisung, in: Wagner et al. (Hrsg.), Pfadabhängigkeit hoheitlicher Ordnungsmodelle, 2016, S. 155 ff.; *J. Schemmel*, Europäische Finanzmarktverwaltung, 2018, S. 402 ff.

[254] Zum Unabhängigkeitsgedanken im Unionsverwaltungsrecht allgemein: *T. Groß*, Die Legitimation der polyzentralen EU-Verwaltung, 2015, S. 79 ff. Zur Rechtsstellung unabhängiger Behörden im Unionsrecht grundlegend bereits EuGH, C-9/56 v. 13.6.1958 – Meroni; siehe weiter auch *M. Ruffert*, Die neue Unabhängigkeit, in: Müller-Graff/Schmahl/Skouris (Hrsg.), FS Scheuing, 2011, S. 399 ff.; *K. Weißgärber*, Die Legitimation unabhängiger europäischer und nationaler Agenturen, 2016; *N. Simantiras*, Netzwerke im Europäischen Verwaltungsverbund, 2016, S. 70 ff.; *Orator*, Möglichkeiten und Grenzen der Einrichtung von Unionsagenturen, 2017, S. 333 ff.; *M. Kröger*, Unabhängigkeitsregime im europäischen Verwaltungsverbund, 2020.

[255] Zum Datenschutzrecht EuGH, C-518/07 v. 9.3.2010 – Kommission/Deutschland; EuGH, C-614/10 v. 16.10.2012 – Kommission/Republik Österreich. Siehe auch *H. P. Bull*, Die „völlig unabhängige" Aufsichtsbehörde, EuZW 2010, S. 488 ff.; *A. Dix*, Unabhängige

rung[256] erfahren hat, sind daher in der deutschen Verfassungsrechtswissenschaft auf kritische Resonanz gestoßen.[257] Gleichwohl sind auch nach hergebrachtem Verständnis weisungsfreie Verwaltungsräume[258] mit dem grundgesetzlichen Demokratieprinzip nicht unvereinbar.[259] Vielmehr haben Literatur und Rechtsprechung verschiedene Kriterien entwickelt, anhand derer entsprechende organisationsrechtliche Gestaltungen gemessen und die durch den Wegfall des Weisungsrechts verursachte Absenkung des demokratischen Legitimationsniveaus („Einflussknick"[260]) kompensiert werden können. In seiner Entscheidung zur *Europäischen Bankenunion* hat das BVerfG ausgeführt, dass die Übertragung von Aufgaben und Befugnissen auf unabhängige Institutionen „nur in begrenzten Ausnahmefällen" zulässig ist, wozu es einer „spezifischen Rechtfertigung" – also eines aus der Art der wahrzunehmenden Aufgabe herrührenden Sachgrunds – sowie „kompensatorischer" Kontroll- oder Rechenschaftspflichten – etwa parlamentarischer oder gerichtlicher Art – bedürfe.[261]

Nun liegt es auf den ersten Blick nicht nahe, dass das BSI etwa bei der Definition von IT-Sicherheitsstandards oder bei der Beratung von KRITIS-Betreibern von einer partiellen Abkoppelung vom politischen Prozess profitieren würde.[262] Auch ist das Handeln des BSI zwar in hohem Maße von technischer

---

Datenschutzkontrolle als vorgezogener Grundrechtsschutz, in: Kröger/Pilniok (Hrsg.), 2016, S. 121 ff. Zum Regulierungsrecht zuletzt EuGH, C-718/18 v. 2.9.2021 – Kommission/Deutschland. Siehe auch *M. Ruffert*, Grundfragen der Wirtschaftsregulierung, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht, Bd. 1, 4. Aufl. 2019, § 21 Rn. 27 ff.; *M. Eifert*, Telekommunikationsrecht, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht, Bd. 1, 4. Aufl. 2019, § 23 Rn. 140 ff.; *Kröger*, Unabhängigkeitsregime im europäischen Verwaltungsverbund, 2020, S. 279 ff.

[256] Dazu bereits *T. Groß*, Ist die Wirtschaftskrise ein Katalysator für das Entstehen unabhängiger Behörden?, DV 47 (2014), S. 197 ff.; *Kaufhold/Langenbucher/Blank/Krahnen*, BaFin (in)dependence, März 2021. Siehe insbes. auch BVerfGE 151, 202 (290 ff., Rn. 127 ff.).

[257] Vgl. etwa *K. F. Gärditz*, Europäisches Regulierungsverwaltungsrecht auf Abwegen, AöR 135 (2010), S. 251 (266 ff.); *E. Frenzel*, „Völlige Unabhängigkeit" im demokratischen Rechtsstaat, DÖV 2010, S. 925 (927 ff.); *J. Masing*, Herausforderungen des Datenschutzes, NJW 2012, S. 2305 (2311).

[258] *Jestaedt*, Demokratieprinzip und Kondominialverwaltung, 1993, S. 102 ff.

[259] Vgl. bereits BVerfGE 9, 268 (282). Zum Überblick über die Rechtslage in Deutschland siehe weiter nur *G. Hermes*, Abhängige und unabhängige Verwaltungsbehörden, in: Masing/Marcou (Hrsg.), Unabhängige Regulierungsbehörden, 2010, S. 53 ff.; *Kröger*, Unabhängigkeitsregime im europäischen Verwaltungsverbund, 2020, S. 113 ff.

[260] Zum Begriff des „Einflussknicks" siehe BVerfGE 151, 202 (LS 2), übernommen von *F. Wagener*, Typen der verselbständigten Erfüllung öffentlicher Aufgaben, in: ders. (Hrsg.), Verselbständigung von Verwaltungsträgern, 1976, S. 31 (40).

[261] BVerfGE 151, 202 (293, Rn. 134).

[262] Hierzu bereits *Wischmeyer*, Informationssicherheitsrecht, DV 50 (2017), S. 155 (167). Vgl. weiter auch *Leisterer*, Internetsicherheit in Europa, 2018, S. 284 ff. Dem trägt auch der durch das IT-SiG 2.0 eingefügte § 1 S. 3 BSIG Rechnung, wonach das BSI „auf Grundlage wissenschaftlich-technischer Erkenntnisse" handelt. Damit suchte der Gesetzgeber, den Be-

Fachkunde geprägt; dies erschwert die Ausübung des Weisungsrechts, reicht allein jedoch für die Anerkennung eines ministerialfreien Raums nicht aus, ist die Ausdifferenzierung der administrativen Wissensstrukturen doch gerade Zweck einer hierarchisch gegliederten Verwaltungsstruktur. Darüber hinaus ist das etwa für Zentralbanken oder Regulierungsbehörden im engeren Sinne in Stellung gebrachte Argument, die Anerkennung ministerialfreier Räume signalisiere eine rein sachorientierte Entscheidungspraxis und erhöhe die Akzeptanz der Behördenentscheidungen bei den Marktteilnehmern, im Falle des BSI nicht anwendbar. Im Gegenteil kann die Einbindung in die ministeriale Weisungsstruktur den behördlichen Entscheidungen besondere Wirksamkeit verleihen. Kritiker der „Versicherheitlichung" des Informationssicherheitsrechts verweisen jedoch darauf, dass die organisatorische Lösung aus der vom BMI überwölbten Sicherheitsverbundstruktur verloren gegangenes Vertrauen in den Willen und die Fähigkeit des Staates, jenseits von Überwachung als produktiver Gestalter des digitalen Raums wahrgenommen zu werden, zurückgewinnen könne. Dass dies für sich eine Modifikation der Grundstrukturen der Verwaltungslegitimation rechtfertigt, scheint jedoch nicht zwingend. Ein „struktureller Anreiz" der ministeriellen Führung, das BSI im eigenen politischen Interesse zu manipulieren – etwa durch eine Schwächung von IT-Sicherheitsstandards zugunsten nachrichtendienstlicher Aufklärungsmöglichkeiten – ist zwar denkbar.[263] Allerdings wäre die Entscheidung für die Priorisierung entsprechender Rechtsgüter zugleich von „hoher politischer Tragweite", was dafür spricht, dass die demokratisch verantwortlichen Instanzen die Verantwortung übernehmen müssen.[264] Sachgerecht dürfte daher sein, zur Stärkung des Vertrauens in das BSI als Akteur der zivilen Sicherheit zunächst etwaige Kooperationen des BSI mit den Sicherheitsbehörden und Diensten in operativen Fragen zu untersagen oder, wo doch erforderlich, gesetzlich engmaschig zu steuern.[265]

All das heißt nicht, dass die Integrationsgrenzen überschritten wären, sollte der Unionsgesetzgeber für die Organisation der mitgliedstaatlichen Informationssicherheitsverwaltung wie im Datenschutzrecht die Einrichtung unabhängiger Behörden verlangen. Sind die für die Einrichtung unabhängiger Behörden aus dem Unionsprimärrecht folgenden Maßstäbe eingehalten,[266] dürfte

fürwortern einer Unabhängigkeit des BSI entgegenzukommen, zieht die gesetzliche Regelung doch auch der Fachaufsicht Grenzen, vgl. *Keppeler/Schulte*, in: Ritter (Hrsg.), Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2022, § 1 BSIG Rn. 104.

[263] Näher zur Qualität, den dieser „Anreiz" haben muss, *Kaufhold/Langenbucher/Blank/Krahnen*, BaFin (in)dependence, März 2021, S. 17 f. Vgl. auch *J. Masing*, Unabhängige Behörden und ihr Aufgabenprofil, in: ders./Marcou (Hrsg.), Unabhängige Regulierungsbehörden, 2010, S. 181 (189 ff.).

[264] Zum Kriterium der politischen Tragweite BVerfGE 151, 202 (293, Rn. 133).

[265] So bereits *Wischmeyer*, Informationssicherheitsrecht, DV 50 (2017), S. 155 (167).

[266] Siehe oben § 5 Fn. 254 bis 256.

ein solches Vorgehen vielmehr aus Sicht des BVerfG jedenfalls dann „im Ergebnis noch hinnehmbar [sein], [wenn] die Einflussknicke durch besondere Vorkehrungen kompensiert werden, die der demokratischen Rückbindung ihres hier in Rede stehenden Handelns dienen", wenn also etwa hinreichende Rechtsschutzmöglichkeiten sowie parlamentarische Rechenschaftspflichten und Kontrollrechte vorgesehen sind.[267]

Verzichtet das Unionsrecht auf eine Festlegung und soll die Behörde zugleich noch stärker als bisher in die (konventionelle) Sicherheitsarchitektur des Bundes eingebunden werden – wofür das IT-SiG 2.0 einige Anzeichen gibt[268] –, ist allerdings eine Unabhängigkeit der Behörde der falsche Weg. Wenn und soweit dem BSI Aufgaben der „nicht-zivilen" Sicherheit übertragen werden, muss die Regierung dafür Verantwortung übernehmen.

Eine ganz andere Frage ist, ob die Herauslösung des BSI aus dem Weisungszusammenhang des BMI geboten sein könnte, um der Behörde ein gewaltenübergreifendes Tätigwerden zu ermöglichen. Bisher beschränkt sich der „staatsinterne" Aufgabenkreis des BSI auf die Hauptorgane der Exekutive des Bundes; die Kommunikationstechnik der Bundesgerichte (in Rechtsprechungsangelegenheiten), des Bundestages, des Bundesrates, des Bundespräsidenten und des Bundesrechnungshofes ist demgegenüber, soweit sie ausschließlich in deren eigener Zuständigkeit betrieben wird, dem BSI nicht zugänglich (§ 2 Abs. 3 BSIG).[269] Da Maßnahmen der Informationssicherheit durchaus den „Kernbereich" der einzelnen Gewalten, also deren „grundsätzlich nicht ausforschbaren Initiativ-, Beratungs- und Handlungsbereich",[270] berühren können – man denke etwa an die aus IT-Sicherheitsgründen gebotene Überwachung des gesamten internen Netzwerkverkehrs –, ist diese Beschränkung konsequent. Gleichzeitig haben Angriffe auf den Bundestag und auf verschiedene Gerichte den bei diesen Staatsorganen bestehenden Sicherheitsbedarf deutlich gemacht; hier fehlt es allerdings oft an Ressourcen, um hinreichenden Eigenschutz zu gewährleisten.[271] Soll das BSI hier umfassend als Sicherheitsdienstleister tätig werden, müsste es im Kräftefeld des Staatsorganisationsrechts auf eine neutrale Position rücken; dem käme es durch die Stellung als unabhängige Behörde nahe.

---

[267] BVerfGE 151, 202 (329 f., Rn. 212 ff.).

[268] Zu den Ambivalenzen des IT-SiG 2.0 siehe unten § 6 II. 6. a).

[269] Zum Verhältnis von „Gewalt" und „Organ" *T. Wischmeyer*, Gewaltenteilung und institutionelles Gleichgewicht, in: Kahl/Ludwigs, HVwR, Bd. 3, 2022, § 78 Rn. 11 m. w. N.

[270] So in st. Rspr. das BVerfG – erstmals BVerfGE 3, 225 (247). Vgl. zu Begriff und Konzept näher *Wischmeyer*, Gewaltenteilung und institutionelles Gleichgewicht, in: Kahl/Ludwigs, HVwR, Bd. 3, 2022, § 78 Rn. 39 m. w. N.

[271] Zur Überforderung der IT-Abteilung des Bundestages: *A. Biselli*, Wir veröffentlichen Dokumente zum Bundestagshack: Wie man die Abgeordneten im Unklaren ließ, Netzpolitik.org, 7.3.2016.

b) Grenzen der Delegation

Legitimationsfragen wirft auch die für das technische Sicherheitsrecht typische[272] Praxis des Gesetzgebers auf, auf materielle Vorgaben zu konkreten Sicherungsmaßnahmen weitgehend zu verzichten und stattdessen nur die Ziele sowie Organisation und Verfahren zu regeln, die dann durch die Exekutive und privaten technischen Sachverstand mit Leben gefüllt werden. Auf diesem Wege kann das Recht, so die Vorstellung, leichter mit der technischen Entwicklung mithalten. So halten auch die neueren Informationssicherheitsgesetze teils die Behörden zur Entwicklung eigener untergesetzlicher Standards an, vor allem aber wird die Ausarbeitung materieller Sicherheitsstandards privaten oder halb-staatlichen Gremien der technischen Standardsetzung überantwortet, typischerweise in Form des Verweises auf den in technischen Normen niedergelegten „Stand der Technik".[273]

aa) Indienstnahme privaten Sachverstands

Verfassungsrechtlich ist es zulässig, dass der Gesetzgeber bei der Technikregulierung auf eine eigenständige normative Feinsteuerung der Materie verzichtet und stattdessen den in der Technik – verstanden als soziales Ordnungssystem[274] – präsenten Sachverstand in den Prozess der Regelsetzung einbindet.[275] Dies gilt auch im Recht der Europäischen Union[276] und auch für das Recht der Informationssicherheit.[277] Allerdings darf der demokratische Gesetzgeber die Sache nicht ganz aus der Hand geben. Um den Legitimationsverlust, den das staatliche Recht durch den Verweis auf die private Normung erleidet, wenigstens teilweise zu kompensieren, muss der Staat auf Organisation und Verfahren der privaten Normsetzung einwirken; nötig ist eine „steuernde Rezeption" des technischen Sachverstands.[278] Dies gilt umso mehr, weil technische

[272] Siehe oben § 3 II. 3.

[273] Historisch lässt sich diese Regelungstechnik bis zum Preußischen Allgemeinen Landrecht zurückführen, vgl. *Vec*, Kurze Geschichte des Technikrechts, in: Schulte/Schröder (Hrsg.), Handbuch des Technikrechts, 2. Aufl. 2011, S. 3 (38); aus internationaler Sicht *Yates/Murphy*, Engineering Rules, 2019. Zu den Regelungen im Recht der Informationssicherheit im Detail siehe unten § 6 II. 5. a).

[274] Siehe oben § 3 I. 3.

[275] Vgl. BVerfGE 49, 89 (134), wonach es dem parlamentarischen Gesetzgeber „wegen der vielschichtigen und verzweigten Probleme technischer Fragen und Verfahren in der Regel nicht möglich [ist], sämtliche sicherheitstechnischen Anforderungen, denen die jeweiligen Anlagen oder Gegenstände genügen sollen, bis ins einzelne festzulegen". Siehe auch *E. Denninger*, Verfassungsrechtliche Anforderungen an die Normsetzung im Umwelt- und Technikrecht, 1990, S. 13 ff.; *K.-H. Ladeur*, Das Umweltrecht der Wissensgesellschaft, 1995; *Ossenbühl*, Die Not des Gesetzgebers im naturwissenschaftlich-technischen Zeitalter, 2000.

[276] Dazu zuletzt EuGH, C-160/20 v. 22.2.2022, Rn. 44 – Stichting Rookpreventie Jeugd.

[277] Dazu im Detail unten § 6 II. 5.

[278] Vgl. *M. Schmidt-Preuß*, Verwaltung und Verwaltungsrecht zwischen gesellschaftlicher Selbstregulierung und staatlicher Steuerung, in: VVDStRL 56 (1997), S. 160 (203 ff.);

Standards kein „reines" Wissen repräsentieren, sondern immer auch Ausdruck bestimmter Präferenzen und Wertungen sind.[279] Die Notwendigkeit einer „Normierung der Normung", also der Pflicht zur Einhaltung demokratisch-rechtsstaatlicher Mindeststandards durch die Normungsorganisationen,[280] folgt also nicht nur daraus, dass der Staat nicht selbst entscheidet; vielmehr gilt es, eine „Kolonisierung der Politik durch technowissenschaftliche Normativität" zu verhindern.[281] Ferner ist zu berücksichtigen, dass die Annahme, die Gesellschaft würde zu Fragen der technischen Sicherheit stets unmittelbar Antworten entwickeln, die der Staat nur noch angemessen rezipieren müsse, jedenfalls in dieser Allgemeinheit nicht trägt. Oft genug reagiert die Gesellschaft von sich aus nicht oder nicht schnell genug auf Herausforderungen. Auch unter funktionalen Gesichtspunkten kann sich der Staat daher nicht schlicht auf privat organisierte Lösungsprozesse verlassen.[282]

---

ders., Private technische Regelwerke, in: Kloepfer (Hrsg.), Selbst-Beherrschung, 1998, S. 89 (95 ff.). Siehe auch *K.-H. Ladeur*, Recht – Wissen – Kultur, 2016, S. 38, im Anschluss an *E. Wenger*, Communities of Practice, 1999.

[279] Zu den damit verbundenen „Kosten" technischer Standards siehe unten § 6 II. 5. b).

[280] Vgl. neben den oben in § 3 Fn. 63 genannten Werken insbes. auch *Battis/Gusy*, Technische Normen im Baurecht, 1988, S. 220 ff.; *C. Gusy*, Techniksteuerung durch Recht: Aufgaben und Grenzen, in: Donner (Hrsg.), Umweltschutz zwischen Staat und Markt, 1989, S. 241 ff.; *Denninger*, Verfassungsrechtliche Anforderungen an die Normsetzung im Umwelt- und Technikrecht, 1990, S. 118 ff.; *G. Lübbe-Wolff*, Verfassungsrechtliche Fragen der Normsetzung und Normkonkretisierung im Umweltrecht, ZG 6 (1991), S. 219 (232 ff.); *C. Gusy*, Probleme der Verrechtlichung, NVwZ 1995, S. 105 ff.; *Schmidt-Preuß*, Verwaltung und Verwaltungsrecht zwischen gesellschaftlicher Selbstregulierung und staatlicher Steuerung, in: VVDStRL 56 (1997), S. 160 (170 ff.); kritischer *U. Di Fabio*, Verwaltung und Verwaltungsrecht zwischen gesellschaftlicher Selbstregulierung und staatlicher Steuerung, in: VVDStRL 56 (1997), S. 235 (245); *M. Schwab*, Rechtsfragen der Politikberatung im Spannungsfeld zwischen Wissenschaftsfreiheit und Unternehmensschutz, 1999, S. 191 ff., 220 ff.; *Trute*, Wirtschaft und Technik, in: Isensee/Kirchhof (Hrsg.), HStR, Bd. IV, 2006, § 88 Rn. 46 ff.; *Kloepfer*, Instrumente des Technikrechts, in: Schulte/Schröder (Hrsg.), Handbuch des Technikrechts, 2. Aufl. 2011, S. 151 (178 ff.); *R. Schröder*, Verfassungsrechtliche Rahmenbedingungen, in: Schulte/Schröder (Hrsg.), Handbuch des Technikrechts, 2011, S. 237 (239 ff.). Nach *M. Eifert*, „Sachverständiges Recht" am Beispiel des Technikrechts, in: Bumke/Röthel (Hrsg.), Privates Recht, 2012, S. 79 (80), hat die Debatte einen „Zustand weitgehender Sättigung erreicht, indem zwar keine Einigkeit besteht, aber die Positionen ausführlich ausgemalt sind"; dies hat sich seither nicht geändert. Eine allgemeine Perspektive noch bei *F. Becker*, Kooperative und konsensuale Strukturen in der Normsetzung, 2005, S. 479 ff. Zur politischen Relevanz globaler Standards im Technologiebereich siehe schließlich auch *D. Grewal*, Network Power, 2008, S. 193 ff.

[281] Vgl. *A. Bora*, Im Schatten von Normen und Fakten, Zeitschrift für Rechtssoziologie 27 (2006), S. 31 ff. Vgl. auch *ders.*, Ökologie der Kontrolle, in: Engel/Halfmann/Schulte (Hrsg.), Wissen, Nichtwissen, unsicheres Wissen, 2002, S. 253 ff.

[282] Dazu weiter unten § 6 II. 5. b). Skeptische Anfragen an das Normungswesen (u. a. mit Blick auf dessen Langsamkeit) schon bei *Schulze-Fielitz*, Technik und Umweltrecht, in: Schulte/Schröder (Hrsg.), Handbuch des Technikrechts, 2011, S. 455 (462 f.) m. w. N.; *Eifert*, „Sachverständiges Recht" am Beispiel des Technikrechts, in: Bumke/Röthel (Hrsg.), Privates Recht, 2012, S. 79 (88 ff.).

Aus diesen Maßgaben lassen sich allerdings nur begrenzt operationalisierbare Maßstäbe ableiten. Hinzu kommt, dass der Steuerungsanspruch des grundgesetzlichen Demokratieprinzips an territoriale Grenzen stößt, werden technische Normen doch heute weitgehend auf europäischer oder sogar internationaler Ebene gesetzt. Allerdings hat sich auch der europäische Gesetzgeber der Thematik angenommen und insbesondere im Produktsicherheitsrecht Rahmenregelungen getroffen, die die Repräsentativität der Organisation und die Responsivität der Verfahren der wesentlichen technischen Normgeber sicherzustellen suchen.[283] Wie sich bei der Analyse der konkreten Vorschriften des Informationssicherheitsrechts zeigen wird, hat der Gesetzgeber hier zudem weitere, differenzierte Modi der Inbezugnahme privater Normen entwickelt, die davon zeugen, dass sich der Gesetzgeber der legitimatorischen Relevanz und der begrenzten Funktionalität privater Normsetzung durchaus bewusst ist.[284] Wo der Versuch zur Erhöhung der Legitimation und Funktionalität dieser Normungsprozesse wie im Fall der Internetsicherheit an faktische Grenzen stößt,[285] muss der Gesetzgeber bei der Rezeption besondere Sensibilität walten lassen.

bb) Ermächtigung der Exekutive

Als Alternative zur Delegation an private Normungsinstanzen wählt der Gesetzgeber auch im Informationssicherheitsrecht regelmäßig die Delegation auf die Exekutive, der die Ausarbeitung detaillierter Standards überlassen wird. Auch diese Entwicklung – die Verschiebung der materiellen Steuerungshoheit vom Parlament zur Exekutive und mittelbar zur Judikative – ist im techni-

[283] Siehe unten § 6 II. 6. Zur internationalen Perspektive allgemein nur *H. C. Röhl*, Internationale Standardsetzung, in: Möllers/Voßkuhle/Walter (Hrsg.), Internationales Verwaltungsrecht, 2007, S. 319 ff.; *O. Lepsius*, Standardsetzung und Legitimation, in: Möllers/Voßkuhle/Walter (Hrsg.), Internationales Verwaltungsrecht, 2007, S. 345 ff.

[284] Vgl. unten § 6 II. 5.

[285] Hierzu weiter unter § 6 II. 1. b) cc). Zwar finden sich in der Literatur auch positive Einschätzungen zur Legitimität der maßgeblichen Entscheidungsprozesse im IETF, vgl. *Kettemann*, The Normative Order of the Internet, 2020, S. 246 (unter Rückgriff auf *T. Vesting*, Instituierte und konstituierte Normativität, in: Sheplyakova (Hrsg.), Prozeduralisierung des Rechts, 2018, S. 101 ff.). Angesichts der (fehlenden) Repräsentativität und Responsivität der Normsetzungsverfahren im IETF (vgl. *Calliess/Zumbansen*, Rough Consensus and Running Code, 2012, S. 135 f.; *Kettemann*, The Normative Order of the Internet, 2020, S. 153 f.; sowie die Nachweise unten in § 6 Fn. 92) muss jedoch vor Idealisierungen gewarnt werden. Zu ICANN vgl. *Viellechner*, Transnationalisierung des Rechts, 2013, S. 128 ff. Allgemein zur Debatte um die Legitimität der existierenden Internet Governance-Strukturen, die sich teilweise mit der Frage nach der Rechtsqualität der dort erzeugten transnationalen Normen mischt (zu letzterer bereits oben § 2 Fn. 73), siehe aus der ausufernden Literatur nur: W. Benedek/V. Bauer/M. Kettemann (Hrsg.), Internet Governance and the Information Society, 2008; *R. Weber*, Shaping Internet Governance: Regulatory Challenges, 2009; R. Radu/J.-M. Chenou/R. Weber (Hrsg.), The Evolution of Global Internet Governance, 2014; I. Borucki/W. Schünemann (Hrsg.), Internet und Staat, 2. Aufl. 2019.

schen Kontext keineswegs neu.[286] Rechtsprechung und Lehre haben eine derartige Gewichtsverlagerung grundsätzlich akzeptiert; durch eine Schärfung der Wesentlichkeitslehre und des Gesetzesvorbehalts sowie der Statuierung einer Pflicht zum legislatorischen Nachsteuern werden ihr allerdings auch Grenzen gezogen.[287]

Diese Arbeitsteilung von Gesetzgeber und Verwaltung ist bewährt und bedarf im Grundsatz keiner Revision. Allerdings setzt sie erneut voraus, dass wenigstens in der Verwaltung die beim Gesetzgeber vermisste Expertise vorhanden ist. Dies ist in Sachen Informationssicherheit jedoch nur bedingt der Fall. Während Forsthoff noch die Verdrängung des Juristen durch den technischen Fachmann fürchtete, muss heute die Sorge eher dem Mangel an (informations-)technischem Sachverstand in den Behörden gelten. In dieser Situation fällt die Verantwortung für die Steuerung der technischen Entwicklung im Bereich Informationssicherheit an den Gesetzgeber zurück. Sie wandelt sich zur Verpflichtung, erst einmal die Bedingungen dafür zu schaffen, dass eine Delegation von Sachentscheidungen an die Verwaltung möglich und sinnvoll ist. Dazu gehört die Bereitstellung hinreichender Ressourcen, d. h. von Organisation, Personal und Finanzen, um die Reaktionsfähigkeit des Rechts auf die dynamische Technikentwicklung zu sichern, sowie den Aufbau einer tragfähigen regulatorischen Kommunikations- und Wissensinfrastruktur in der Verwaltung. Die hierzu auf Unions- und nationaler Ebene unternommenen Schritte werden im folgenden Kapitel zu untersuchen sein.[288]

IV. Folgerungen

Die Querschnittsnatur der Materie und die Vielfalt möglicher regulatorischer Zugriffe verlangen aus verfassungsrechtlicher Sicht einen breiten Zugriff. Die hier ausgewählten, auf die im vorangegangenen Kapitel identifizierten Aufmerksamkeitsfelder abgestimmten Maßstäbe bilden die wesentlichen verfassungsrechtlichen Rahmenbedingungen ab. Je nach Ausgestaltung der Regulierung sind darüber hinaus jedoch weitere verfassungsrechtliche Garantien heranzuziehen. Würden etwa den privaten CERTs[289] hoheitsrechtliche Befugnisse übertragen, die faktische Privatisierung der Abwehr von Informationssicherheitsrisiken also auch rechtlich sanktioniert, müsste dies an Art. 33 Abs. 4 GG

[286] Siehe dazu bereits *Plischka*, Technisches Sicherheitsrecht, 1969, S. 80 ff.; *Breuer*, Direkte und indirekte Rezeption technischer Regeln durch die Rechtsordnung, AöR 101 (1976), S. 46 ff.

[287] Vgl. erneut BVerfGE 49, 89 (LS 1–3); 53, 30 (57 ff.); 56, 54 (78). Umfassend *Schröder*, Verfassungsrechtliche Rahmenbedingungen, in: Schulte/Schröder (Hrsg.), Handbuch des Technikrechts, 2011, S. 237 (239 ff.).

[288] Siehe unten § 6 II. 3.

[289] Siehe oben § 4 Fn. 111.

gemessen werden. In dem hier ausgeklammerten Bereich der IT-Sicherheit im E-Government stellen sich zudem weitergehende Fragen der föderalen Kompetenzverteilung und der Gewaltenteilung. Sollen sich Einheiten der Bundeswehr an der Bekämpfung von Gefährdungen des „Cyberraumes" beteiligen, sind die wehrverfassungsrechtlichen Bestimmungen der Art. 35 Abs. 2 und 3 GG und Art. 87a Abs. 2 und 4 GG zu beachten.[290]

Gerade was die im folgenden Kapitel zu analysierenden rechtlichen Vorgaben zur Erhöhung des Informationssicherheitsniveaus betrifft, beschränkt sich der Einfluss des Verfassungsrechts jedoch, wie gesehen, auf Rahmenvorgaben. Dies ist angemessen, existieren doch keine Blaupausen für erfolgreiche Regulierung in diesem Bereich. Der Gesetzgeber muss Freiräume haben, auch Irrtümer zu begehen. Regulierung hat in diesem Sinne immer auch einen experimentellen Charakter.[291]

[290] Dazu *S. Spies-Otto*, Die verfassungsrechtliche Dimension staatlichen Verhaltens im Cyber-Raum, NZWehrr 2016, S. 133 ff.; *Marxsen*, Verfassungsrechtliche Regeln für Cyberoperationen der Bundeswehr, JZ 72 (2017), S. 543 ff.; *Ladiges*, Der Cyberraum, NZWehrr 2017, S. 221 ff.; *R. Schmidt-Radefeldt*, Rechtsdurchsetzung mit militärischen Mitteln (Landesbericht Deutschland), in: Kischel/Graf von Kielmansegg (Hrsg.), Rechtsdurchsetzung mit militärischen Mitteln, 2018, S. 1 (26 f.).

[291] Vgl. oben § 2 Fn. 83 m. w. N.

§ 6 Gewährleistung von Informationssicherheit: Ein regulatorisches Schutzkonzept

> „Cybersecurity comes into being through an interactive, non-hierarchical, multi-layered assemblage of people, objects, technologies and ideas, is thus co-produced between a wide range of users, institutions, laws, materials, protocols, etc."[1]

I. Zur Ordnung komplexer Regulierungsregime

Die Akteure im Feld der Informationssicherheit sind mit unterschiedlichen Verhaltenserwartungen konfrontiert. Neben rechtlichen Regelungen verlangen technische Standards, Regeln des Marktes sowie soziale Konventionen Beachtung und erzeugen Pfadabhängigkeiten für künftige Entscheidungen. Die einzelnen Regelsysteme interagieren miteinander, oft ohne dass aus Sicht der Betroffenen eine klare Hierarchie zwischen den jeweiligen Ordnungsansprüchen besteht.[2]

Rechtsnormen sind jedoch nicht ein Steuerungsmedium unter anderen. Vielmehr erhebt das Recht einen Anspruch auf Gestaltung, der im besten Falle demokratisch rückgebunden ist, rechtsstaatlichen Anforderungen genügt und Individualrechte schützt.[3] Auch im globalen Kontext verbinden sich mit dem Medium des Rechts Erwartungen, die über ein funktionales Verständnis als besonders effektive Sozialtechnik hinausgehen.[4] Um diesem Anspruch gerecht

---

[1] *Egloff/Dunn Cavelty*, Attribution and Knowledge Creation Assemblages in Cybersecurity Politics, Journal of Cybersecurity 7:1 (2021), S. 1 (3). Ähnlich: *Stevens*, Cybersecurity and the Politics of Time, 2016, S. 3; *J. Collier*, Cybersecurity Assemblages, Politics and Governance 6:2 (2018), S. 13.

[2] Dazu allgemein *Baldwin/Cave/Lodge*, Understanding Regulation, 2. Aufl. 2012, S. 37.

[3] Zum Gestaltungsanspruch und -auftrag des Rechts siehe oben § 2 IV. 1.

[4] Dazu *Kingsbury*, The Concept of 'Law' in GAL, EJIL 20 (2009), S. 23 ff., der allerdings in methodisch angreifbarer Weise die Frage nach der moralischen Signifikanz einer Regel bzw. nach ihrer Legitimierbarkeit mit der Frage nach ihrer rechtlichen Geltung verknüpft und daher die Beachtung der „general principles of public law" – Rechtmäßigkeit, Rationalität, Verhältnismäßigkeit, rule of law und Menschenrechte – zu Bedingungen der „rule of recognition" des globalen Rechts erklärt. Dazu näher § 2 Fn. 69.

zu werden, muss sich das Recht im Gewirr der Normen Gehör verschaffen, indem es überzeugt, anleitet, in Dienst nimmt und nötigenfalls zwingt.

Bedingung für all das ist, dass klar erkennbar ist, was von Rechts wegen geboten ist.[5] Die Rechtsmaterie, die den Schutzzielen der Verfügbarkeit, Integrität und Vertraulichkeit von Informationen dient (vgl. § 2 Abs. 2 S. 4 BSIG[6]), ist allerdings äußerst unübersichtlich. Das Informationssicherheitsrecht kennt kein „systemprägendes" Gesetz und – jenseits der allseits konsentierten Ziele – keine allgemeingültigen Prinzipien. Rechtsnormen, die zur Erreichung der Schutzziele beitragen, gehören teils dem Privatrecht, teils dem Strafrecht, teils verschiedenen Segmenten des öffentlichen Rechts an. Sie regulieren meist nur einzelne Teilbereiche der Gesamtaufgabe, adressieren also entweder nur die Komponentensicherheit oder den Systemschutz. Und sie decken oft nur einzelne Phasen des Informationssicherheitszyklus ab, der aus technischer Sicht von der Prävention über die Detektion bis hin zur Reaktion reicht.[7] Die Varianz der eingesetzten rechtlichen Instrumente[8] und der verwendeten Organisations- und Verfahrensformen ist ebenfalls groß. Divers ist ferner der Adressatenkreis, der Verbraucher ebenso wie Unternehmen und staatliche Stellen bis hin zu den Betreibern kritischer Infrastrukturen umfasst. Neben Querschnittsregeln, die für alle gesellschaftlichen Bereiche Geltung beanspruchen, finden sich zahlreiche sektorale Vorgaben. Schließlich werden relevante Regelungen nicht nur durch den Nationalstaat, sondern auch in Europa und auf der Ebene des Völkerrechts gesetzt.[9] Erweitert und ergänzt wird das Normenpanorama durch privatrechtliche Abreden und technische Standards, die oft eine hohe faktische Bindungswirkung haben und teils auch unmittelbar vom staatlichen Recht rezipiert werden.

In der Literatur ist daher plastisch vom Informationssicherheitsrecht als einem regulatorischen „patchwork of confusion" die Rede.[10] Mit ähnlicher

---

[5] Vgl. auch die Funktionsbestimmung des Technikrechts bei *J. Halfmann*, Technikrecht aus der Sicht der Soziologie in: Schulte/Schröder (Hrsg.), Handbuch des Technikrechts, 2. Aufl. 2011, S. 93 (99): „Stabilisierung der kognitiven und normativen Erwartungen von Personen und Organisationen gegenüber Technik".

[6] Zu den Schutzzielen siehe gleich näher unter § 6 II. 1. a.

[7] *Bundesregierung*, Cyber-Sicherheitsstrategie für Deutschland, 2016, S. 8 f.

[8] Mit dem Begriff des „Instruments" werden hier und im Folgenden vertypte regulatorische Handlungsoptionen bezeichnet, deren Spektrum von gesetzlichen Verboten über Anreizstrukturen bis hin zum individualisierten Informationshandeln (Auskunft etc.) reicht. Siehe dazu auch gleich § 6 Fn. 19.

[9] Zu den aktuellen Rechtsetzungsvorhaben der Union, die das ohnehin schon vielfältige Normenpanorama nochmals deutlich komplexer machen, siehe oben § 1 Fn. 30.

[10] *T. Chaudhary/J. Jordan et al.*, Patchwork of Confusion. The Cybersecurity Coordination Problem, Journal of Cybersecurity 4:1 (2018). S. 1 ff. Zum IT-SiG 2.0 siehe die Diagnose bei *G. Hornung*, Das IT-Sicherheitsgesetz 2.0, NJW 2021, S. 1985. Passend wäre auch der von *Hoffmann-Riem*, Freiheitsschutz in den globalen Kommunikationsinfrastrukturen, JZ 69 (2014), S. 53 (63), in anderem Kontext eingeführte Begriff des „Regulierungsmosaiks".

Stoßrichtung ließe sich von einer „pluralistisch" strukturierten Rechtsmaterie[11] oder von einem „Regimekomplex"[12] sprechen.

All das erschwert eine strukturierte Aufbereitung des Rechtsstoffs.[13] Dennoch soll im Folgenden der Versuch unternommen werden, jene Normen, mit denen der Staat seiner Verantwortung für die Informationssicherheit nachzukommen versucht, zu ordnen und charakteristische Regelungsstrukturen herauszuarbeiten (II.). Dabei wird das heterogene Normgewebe nicht als „holistic approach" (*Ingolf Pernice*) verstanden, in dem die beteiligten Stellen Hand in Hand auf die Erreichung eines gemeinsamen Ziels hinarbeiten und dabei ihre Instrumente auf eine möglichst rationale Art und Weise miteinander kombinieren.[14] Auch die nachstehend eingeforderte „integrative Regulierungsperspektive" (III.) zielt nicht auf starke Kohärenz und Systematik, sondern will Strategien für den Umgang mit der Heterogenität, den Lücken und Bruchlinien, den das Informationssicherheitsrecht dauerhaft aufweisen wird, entwerfen.

Der auf Kontingenz gestellte Ordnungsanspruch der vorliegenden Untersuchung trägt der differenzierten Aufgabenstellung und der komplexen Kompetenzordnung Rechnung, in die sich die Querschnittsmaterie Informations-

[11] Zu verschiedenen Konzepten des Rechtspluralismus im Überblick *B. Tamanaha*, A Non-Essentialist Version of Legal Pluralism, Journal of Law and Society 27:2 (2000), S. 296 ff.; *P. Schiff Berman*, Global Legal Pluralism, 2012; *ders.*, Understanding Global Legal Pluralism, in: ders. (Hrsg.), The Oxford Handbook of Global Legal Pluralism, 2020, S. 1 ff. Zur Anwendung des Konzepts auf die Regulierung von Informationstechnologien siehe insbes. *J. Daskal*, The Overlapping Web of Data, Territoriality, and Sovereignty, in: a. a. O., S. 955 ff.; *M. Land*, The Problem of Platform Law, in: a. a. O., S. 975 ff.

[12] Zum Begriff des Regimekomplexes ausführlich *P. Pfister*, Regimekomplexe, 2012. Siehe weiter *T. Gehring/B. Faude*, Dynamics of Regime Complexes, Global Governance 19 (2013), S. 119 ff.; *S. Hameiri/L. Jones*, Governing Borderless Threats, 2015; *R. Keohane/D. Victor*, The Regime Complex for Climate Change, Perspectives on Politics 9 (2011), S. 7 ff.; *S. Oberthür/T. Gehring*, Institutional Interaction, in: Oberthür/Stokke (Hrsg.), Managing Institutional Complexity, 2011, S. 25 ff.; *A. Orsini/J.-F. Morin/O. Young*, Regime Complexes, Global Governance 19 (2013), S. 27 ff. Zum Regime-Begriff grundlegend S. Krasner (Hrsg.), International Regimes, 1983; zur Kollision regulatorischer Regime *A. Fischer-Lescano/G. Teubner*, Regime-Kollisionen, 2006, S. 34 ff. Zu unterschiedlichen *Rechts*-Regimen *M. Burgi*, Rechtsregime, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 3. Aufl. 2022, § 18.

[13] Zu dieser Basisaufgabe (verwaltungs-)rechtlicher Forschung *A. Voßkuhle*, Die Reform des Verwaltungsrechts als Projekt der Wissenschaft, DV 32 (1999), S. 545 (547 ff.); *Bumke*, Die Entwicklung der verwaltungsrechtswissenschaftlichen Methodik in der Bundesrepublik Deutschland, in: Schmidt-Aßmann/Hoffmann-Riem (Hrsg.), Methoden der Verwaltungsrechtswissenschaft, 2004, S. 73 (115 ff.); *Schmidt-Aßmann*, Das allgemeine Verwaltungsrecht als Ordnungsidee, 2. Aufl. 2006, 1/32.

[14] Vgl. *Pernice*, Global Cybersecurity Governance, Global Constitutionalism (2018), S. 112 (122). Allgemein zu den Möglichkeiten und Grenzen entsprechender Kohärenz- und Systemerwartungen *P. Dieterich*, Systemgerechtigkeit und Kohärenz, 2014; *P. Hilbert*, Systemdenken in Verwaltungsrecht und Verwaltungsrechtswissenschaft, 2015.

sicherheitsrecht nicht bruchlos einfügen lässt.[15] Er erkennt ferner an, dass der regulatorische Prozess kein Verfahren ist, in dem die beteiligten Stellen stets den zur Zielerreichung optimalen „Instrumentenmix" suchen und eine umfassend informierte und strukturierte Abwägung zwischen allen möglichen Regulierungsvarianten vornehmen.[16] Stattdessen spielen historische Pfadabhängigkeiten, politische Präferenzen und aktuelle Moden bei der Instrumentenwahl oft die bestimmende Rolle.[17] Auch wirken empirisch kaum validierbare staats- und verfassungstheoretische Annahmen zum Verhältnis von Staat, Recht, Verwaltung, Markt, Gesellschaft und Individuum auf die Wahl der Regulierungsarrangements ein: Welchen Akteuren wird die Lösung eines gesellschaftlichen Problems am ehesten zugetraut – dem Staat oder Privaten? Erwartet man Effizienzgewinne durch Kooperation oder fürchtet man regulatory capture? Welcher Wert wird der individuellen Verantwortung zuerkannt? Schließlich sind die Lücken und Widersprüche des Informationssicherheitsrechts auch für die hier allgemein interessierende Frage aufschlussreich, in welchem Maße technische Materien durch hoheitliche Regulierung gestaltbar sind. Im Informationssicherheitsrecht lässt sich gewissermaßen in Echtzeit beobachten, wie sich das Recht ein neues technisches Risiko aneignet, wie Gesetzgeber und Verwaltung zu diesem Zweck ihren Instrumentenkasten durchmustern und in einem von Versuch und Irrtum geprägten Verfahren mehr oder weniger taugliche Regelungsstrukturen identifizieren, überprüfen und etablieren oder auch wieder verwerfen. Von der Rekonstruktion dieses alles andere als gradlinigen Suchprozesses lässt sich – so die These – mehr lernen als von dem Versuch, die Materie als dogmatisch festgefügtes „Rechtsgebiet" zu präsentieren.[18]

Die Kriterien, an denen sich die folgende Aufbereitung des Rechtsstoffs orientiert und die hier als dessen „Strukturen" firmieren sollen, sind auf einer mittleren Abstraktionsebene angesiedelt. Sie sind geschärft durch die Aufga-

---

[15] Dazu gleich näher unter § 6 II. 1.

[16] Vgl. nur *Binder*, Regulierungsinstrumente und Regulierungsstrategien, 2012, S. 46 ff.; *Hellgardt*, Regulierung und Privatrecht, 2016, S. 492 ff. Zur Zielvorstellung „guter Regulierung" *Eifert*, Regulierungsstrategien, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 3. Aufl. 2022, § 19 Rn. 154 ff. m. w. N. Siehe ferner nur *G. F. Schuppert*, Gute Gesetzgebung, 2003, S. 31 ff. Allgemein auch *L. Michael*, Formen- und Instrumentenmix, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 2, 3. Aufl. 2022, § 40.

[17] Zu den Kontingenzen bei der Entstehung von Politikfeldern siehe die Nachweise in § 2 Fn. 84.

[18] Zum wenig aussagekräftigen Begriff des „Rechtsgebiets" siehe § 4 Fn. 4. Optimistischer noch die Qualifikation des Informationssicherheitsrecht als „Rechtsgebiet im Werden" bei *Wischmeyer*, Informationssicherheitsrecht, DV 50 (2017), S. 155 (186). In diese Richtung auch *M. Schallbruch*, IT-Sicherheitsrecht (Teil 1), CR 2017, S. 648; skeptischer *Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022, Rn. 2. Aus der U.S.-Perspektive vgl. den Ansatz von *J. Kosseff*, Defining Cybersecurity Law, Iowa L. Rev. 103 (2018), S. 985 ff.; *ders.*, Hacking Cybersecurity Law, U. Ill. L. Rev. 2020, S. 811 ff.

benbeschreibung und orientieren sich an den maßgeblichen Rechtsakten zur Informationssicherheit, übernehmen jedoch nicht einfach deren Selbstbeschreibung. Schon angesichts der hohen technischen und legislativen Dynamik wäre der mit einer Kompilation der einschlägigen (technischen) Normen verbundene Erkenntnisgewinn begrenzt. Der Gang der Analyse folgt aber auch nicht den abstrakten Instrumenten-Kategorien, die die Regulierungstheorie entwickelt hat.[19] Stattdessen stehen hier die Charakteristika der konkreten Materie im Vordergrund. Auch die etablierte Form der Aufbereitung regulatorischer Maßnahmen nach Art und Umfang der Beteiligung Privater („Regulierungsstrategie") entfaltet daher nur begrenzt Orientierungswirkung für die folgende Darstellung.[20] Zu berücksichtigen ist insoweit, dass das Zusammen-

[19] Zum Kanon regulatorischer Grundformen jüngst ausführlich und instruktiv *Hellgardt*, Regulierung und Privatrecht, 2016, S. 449 ff., der *direkt* wirkende Instrumente – durch oder aufgrund eines Gesetzes erlassene Gebote, Verbote und Unwirksamkeitsgründe, Sanktionsnormen (etwa Schadensersatzpflichten, Geldbußen oder Strafen), Anreizregelungen (Lenkungssteuern und Subventionen) sowie Erscheinungsformen der Qualitäts- und Preisregulierung – und *indirekte* Regulierungsinstrumente – Informations- und Offenlegungspflichten, die Möglichkeiten zur Indienstnahme Dritter, Zurechnungsnormen, Formen des Soft Law und der regulierten Selbstregulierung sowie das sog. Naming and Shaming – unterscheidet. Aus der jüngeren privatrechtlichen Literatur, in der regulierungstheoretische Ansätze seit einiger Zeit Konjunktur haben, vgl. ferner auch *Binder*, Regulierungsinstrumente und Regulierungsstrategien, 2012, S. 24 ff.; speziell zur privaten Selbstregulierung siehe auch *Bachmann*, Private Ordnung, 2006, S. 74 ff. Zum Begriff der Regulierung sowie den Grundlagen und methodischen Implikationen der Regulierungstheorie siehe ausführlich bereits oben § 2 IV.

[20] Zu den insoweit als typisch identifizierten „Regulierungsstrategien" staatlich-imperativer Regulierung (auch: hoheitliche Regulierung), (hoheitlich) regulierter gesellschaftlicher Selbstregulierung und gesellschaftlicher Selbstregulierung, die jeweils durch die Art der hoheitlichen Verantwortungsübernahme, die Form der Aufgabenerledigung, typische Anwendungsfelder und Instrumente sowie prägende Organisations- und Verfahrensprinzipien charakterisiert sind, grundlegend *W. Hoffmann-Riem*, Systematisierung und Entwicklungsperspektiven, in: Hoffmann-Riem/Schmidt-Aßmann (Hrsg.), Öffentliches Recht und Privatrecht, 1996, S. 261 (300 ff.); zum Begriff der „Regulierungsstrategie" siehe insbes. auch *Eifert*, Regulierungsstrategien, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 3. Aufl. 2022, § 19 Rn. 1 ff. Deutlich weiter dagegen das Begriffsverständnis bei *Binder*, Regulierungsinstrumente und Regulierungsstrategien, 2012, S. 46 ff., der darunter allgemein die Zuordnung von Regulierungsinstrumenten (bestimmte vertypte Handlungsoptionen) zu „einem oder mehreren Regulierungszweck(en)" verstehen will.

Aus der uferlosen Literatur zur „regulierten Selbstregulierung" – jener intermediären Strategie, der naturgemäß die besondere Aufmerksamkeit der Literatur gilt – vgl. nur *Schmidt-Preuß*, Verwaltung und Verwaltungsrecht zwischen gesellschaftlicher Selbstregulierung und staatlicher Steuerung, in: VVDStRL 56 (1997), S. 160 ff.; *Di Fabio*, Verwaltung und Verwaltungsrecht zwischen gesellschaftlicher Selbstregulierung und staatlicher Steuerung, in: VVDStRL 56 (1997), S. 235 ff.; *Augsberg*, Rechtsetzung zwischen Staat und Gesellschaft, 2003; sowie die Beiträge in DV Beiheft 4 „Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates", insbes. *E. Schmidt-Aßmann*, Regulierte Selbstregulierung und verwaltungsrechtliche Systembildung, DV Beiheft 4 (2001), S. 253 ff.; *A. Voßkuhle*, „Regulierte Selbstregulierung" – Zur Karriere eines Schlüsselbegriffs, DV Beiheft 4 (2001), S. 197 ff.

wirken von hoheitlichen und privaten Stellen zwar ein zentrales Thema des Informationssicherheitsrechts ist; allerdings weist die Materie keine Privatisierungsgeschichte auf, sondern ist durch das allmähliche Vordringen der staatlichen Rechtsordnung in einen zuvor genuin privat geordneten Bereich geprägt.[21] Gleichwohl liefern die bekannten Modelle und Kategorien der Regulierungstheorie wichtige Orientierungspunkte für die folgende Analyse des Informationssicherheitsrechts. An geeigneter Stelle, etwa wenn es um das Zusammenspiel privater technischer Standards mit staatlichen Normen, also um eine typische Erscheinungsform hoheitlich regulierter gesellschaftlicher Selbstregulierung geht, wird daher auf sie zurückzugreifen sein.

II. Strukturen des Informationssicherheitsrechts

1. Primat der Aufgabe: Ziele und sachlicher Umfang der Regulierung

a) Von den Schutzzielen zur Aufgabe Informationssicherheit …

Bevor Informationssicherheit zur gesellschaftlichen Großaufgabe und zum Gegenstand intensiver regulatorischer Bemühungen wurde, befasste sich nur ein überschaubarer Kreis von Ingenieuren und Informatikern intensiver mit der Thematik.[22] In dieser Diskursgemeinschaft hat jene teleologische Definition von Informationssicherheit ihren Ursprung, die bis heute sowohl den technischen als auch den rechtlichen Zugriff auf die Materie prägt. So definiert § 2 Abs. 2 S. 4 BSIG im Einklang mit zahlreichen technischen Normen Sicherheit in der Informationstechnik als die „Einhaltung bestimmter Sicherheits-

[21] Die Situation weist daher Ähnlichkeiten mit dem ausgehenden 19. Jahrhundert auf, als die regulierte Selbstregulierung – als Phänomen, nicht als Begriff – ihre erste Blüte erlebt hat, vgl. dazu die umfangreichen Forschungen des Frankfurter Max-Planck-Instituts, die insbes. von *Peter Collin* getragen wurden, v. a. P. Collin/G. Bender et al. (Hrsg.), Selbstregulierung im 19. Jahrhundert – zwischen Autonomie und staatlichen Steuerungsansprüchen, 2011; dies. (Hrsg.), Regulierte Selbstregulierung im frühen Interventions- und Sozialstaat, 2012; dies. (Hrsg.), Regulierte Selbstregulierung in der westlichen Welt des späten 19. und frühen 20. Jahrhunderts, 2014. Synthetisierend *P. Collin*, Privat-staatliche Regelungsstrukturen im frühen Industrie- und Sozialstaat, 2016; *ders.*, The Legitimation of Self-Regulation and Co-Regulation in Corporatist Concepts of Legal Scholars in the Weimar Republic, Politics and Governance 5:1 (2017), S. 15 ff.; *ders.*, Regulierte Selbstregulierung in rechtshistorischer Perspektive. Studien und Materialien, 2018.

[22] Zur Entwicklung der Disziplin siehe *S. Lipner*, The Birth and Death of the Orange Book, IEEEA 37:2 (2015), S. 19 ff.; *M. Warner*, Notes on the Evolution of Computer Security Policy in the US Government 1965–2003, IEEEA 37:2 (2015), S. 8 ff. (zur Rolle staatlicher Institutionen); *J. Yost*, The Origin and Early History of the Computer Security Software Products Industry, IEEEA 37:2 (2015), S. 46 ff. (zu den Entwicklungen in der Privatwirtschaft). Zu ersten sicherheitsspezifischen Überlegungen innerhalb der IETF ab Mitte der 1980er-Jahre siehe *DeNardis*, The Internet Design Tension between Surveillance and Security, IEEEA 37:2 (2015), S. 72 (74).

standards, die die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen betreffen", in und bei der Anwendung von „informationstechnischen Systemen, Komponenten oder Prozessen".

Über Art und Inhalt dieser drei Teilziele Verfügbarkeit, Integrität oder Vertraulichkeit besteht im technischen Diskurs zwar kein allgemeiner Konsens, aber doch ein hohes Maß an Übereinstimmung.[23] Für die hiesigen Zwecke ist eine in jeder Hinsicht präzise Definition der Ziele verzichtbar.[24] Es reicht aus zu wissen, dass das Schutzziel der „Vertraulichkeit" (confidentiality) verfehlt ist, wenn die Regeln für den autorisierten Zugang zu IT-Systemen, für die Weitergabe von Informationen auf IT-Systemen oder für die Kommunikation zwischen IT-Systemen verletzt werden können. Besonders sensibel sind insoweit Systeme, die personenbezogene oder proprietäre Daten verarbeiten; aber auch sonstige Dateien, etwa Konfigurationsdateien, sind unter Vertraulichkeitsgesichtspunkten alles andere als „belanglos", wenn ihre Kenntnis dazu dienen kann, Zugriff auf ein IT-System zu erlangen.[25] Die „Integrität" (integrity) eines Datenbestandes ist gewahrt, soweit dieser vollständig und korrekt, d. h. unverändert, ist; teilweise wird darüber hinaus noch gefordert, dass die Daten den von ihnen abgebildeten Werten korrespondieren und, soweit die Daten in Datenbanken gespeichert werden, diese Abbildung in sich konsistent ist. Die Integrität von Daten ist jedenfalls dann verletzt, wenn die Daten unerlaubt oder nicht nachvollziehbar verändert wurden. Wenn von der Integrität eines IT-Systems die Rede ist, wird gefordert, dass sich dieses logisch korrekt verhält. Die „Verfügbarkeit" (availability) eines System ist schließlich gewährleistet, wenn es zu keinen ungeplanten Systemausfällen kommt und wenn der Zugriff auf dessen Daten für autorisierte Benutzer in angemessener Zeit möglich ist. Zusammengefasst und stark vereinfacht müssen „sichere" IT-Systeme also verhindern, dass Informationen gestohlen werden (Vertraulichkeit), dass Aufgaben inkorrekt ausgeführt werden (Integrität) und dass Funktionalitäten des Systems beeinträchtigt sind (Verfügbarkeit). Neben den im BSIG kodifizierten Zielen finden sich im technischen Normungswesen und in anderen Rechtsakten teils noch weitere Zielbestimmungen, die auf spezielle Anwen-

[23] Vgl. insbes. ISO/IEC 27000:2018, 3.28, dessen aktuelle Version „information security" definiert als „preservation of confidentiality (3.10), integrity (3.36) and availability (3.7) of information". Ausführlich zu den einzelnen Unterbegriffen sowie zu alternativen Ansätzen *L. Feiler*, Information Security Law, 2012, S. 4 ff. Überblicksartig auch *Finnemore/Hollis*, Constructing Norms for Global Cybersecurity, AJIL 110 (2016), S. 425 (433).

[24] Die folgenden Ausführungen orientieren sich teils wörtlich an den Definitionen des ISO/IEC 27000:2018-Standards sowie am Glossar des BSI, abrufbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html.

[25] Vgl. demgegenüber die (zu) enge Bestimmung sensibler IT-Systeme durch BVerfGE 120, 274 (314); dazu bereits oben § 5 I. 2. c) bb).

dungsszenarien fokussiert sind.[26] So ergänzt Art. 4 Nr. 2 NIS-RL (entsprechend Art. 6 Abs. 2 NIS 2-RL[27]) die Ziel-Trias des BSIG um das Merkmal der „Authentizität" (authenticity) von Informationen. Darunter wird verstanden, dass die von einem System verarbeiteten Daten tatsächlich aus den angegebenen Quellen stammen, was Vertrauen in die Kommunikationspartner und die Übermittlungswege und somit etwaige Authentifizierungsmaßnahmen voraussetzt. Die Literatur kennt ferner das Schutzziel der „Nachweisbarkeit" oder „Nichtabstreitbarkeit" (non-repudiation), wonach zu jedem Zeitpunkt Klarheit über die Identität der Kommunikationspartner bestehen muss, weder Sender noch Empfänger also ihre Aktivitäten glaubhaft bestreiten können dürfen. Letzteres hat primär für kommerzielle Transaktionen im Internet Bedeutung.

Aus Sicht des Rechtssystems hat die Entscheidung des Gesetzgebers, die Definition von Informationssicherheit mit den etablierten technischen Zielbestimmungen zu synchronisieren, ihre Vorzüge. Sie erleichtert die Kommunikation zwischen Recht und Technik. Die Definition ist zudem nicht an einen einmal fixierten Stand der Technik gebunden, sondern zukunftsoffen. Technische Innovationen können daher ohne Zeitverluste im Recht rezipiert werden. Ganz offen bleibt allerdings, auf welche Weise die Ziele erreicht werden sollen, welche *Mittel* also praktisch zur Erledigung der Aufgabe Informationssicherheit herangezogen werden können.[28] Der Blick ins BSIG, in die NIS-RL oder in andere Normen des Informationssicherheitsrechts hilft hier nicht weiter. Denn die Aufgabenadäquanz dieser Regelungen steht ja gerade auf dem Prüfstand. Es bedarf somit der in der Einleitung angekündigten Bestandsaufnahme des Realbereichs, die sich von dessen bereits erfolgter rechtlicher Einhegung lösen muss, ohne die Regulierungsperspektive aus dem Blick zu verlieren. Auf die damit verbundenen methodischen Herausforderungen wurde bereits hingewiesen.[29]

Um zu bestimmen, wie weit Regulierung in *sachlicher* Hinsicht ausgreifen muss, um das Informationssicherheitsproblem einzuhegen, müssen zunächst die technischen Grundlagen der Informationssicherheit geklärt werden. Ferner ist darauf einzugehen, welche Akteure einen Beitrag dazu leisten können, die einzelnen Problemfacetten anzugehen, was für den *personellen* Zuschnitt der Regulierung von entscheidender Bedeutung ist.[30]

---

[26] Vgl. ISO/IEC 27000:2018, 3.28.: „In addition, other properties, such as authenticity (3.6), accountability, non-repudiation (3.48), and reliability (3.55) can also be involved."

[27] Die NIS 2-Richtlinie wird hier in der endgültigen Fassung vom 14.12.2022 (Unterzeichnung durch den Präsidenten des EP und den Präsidenten des Rates) zitiert.

[28] Vgl. hierzu bereits die Kritik unter § 4 II. 1. a).

[29] Siehe § 2 IV.

[30] Hier liegt ein wesentlicher Unterschied zur Art der Aufbereitung, wie sie in der informations*straf*rechtlichen Literatur begegnet. Deren Interesse gilt primär den Akteuren, die

Die technischen Strukturen weisen offensichtlich eine derart hohe Komplexität und Varianz auf, dass sie sich hier nur in elementaren Grundzügen darstellen lassen. Der technische Fortschritt führt zudem dazu, dass ständig neue Gefährdungsszenarien entstehen. Ziel ist daher nicht, bald überholte Details zu präsentieren. Stattdessen sollen die technischen Strukturen so beschrieben werden, dass erkennbar wird, an welchen Stellen Regulierung ansetzen kann bzw. sollte.

b) … Aufgabe Informationssicherheit: Ein Schichtenmodell …

Die folgende Analyse unterscheidet drei Schichten des Informationssicherheitsproblems.[31] Dieses Schichtenmodell soll hier vorab skizziert und anschließend näher entfaltet werden.[32] Klassischer Regulierungsvektor des IT-Sicherheitsrechts ist der System- und Netzwerkschutz. Informationssicherheit setzt an, indem die Nutzer und Betreiber informationstechnischer Systeme und Netzwerke zu Schutzmaßnahmen verpflichtet werden (aa.). Zweitens muss Komponentensicherheit gewährleistet sein. Denn die Systembetreiber sind regelmäßig auf sichere Software und Hardware angewiesen; deren Hersteller sind somit in den Pflichtenkreis des Informationssicherheitsrechts ein-

---

die Sicherheit der Informationsordnung bedrohen, und nur sekundär jenen, die die Sicherheit gewährleisten können. Dementsprechend ordnet die strafrechtliche Literatur den Phänomenbereich typischerweise nach den Erscheinungsformen von Cyberkriminalität (Hacking, Malware, Botnetze, Phishing etc.), vgl. beispielhaft *D. Kochheim*, Cybercrime und Strafrecht, 2. Aufl. 2018.

[31] Schichtenmodelle haben sich allgemein bei der Untersuchung des Verhältnisses von Recht und Informationstechnik bewährt. Sie reduzieren die Komplexität der vernetzten Technik erheblich, was es erleichtert, Ansatzpunkte für (rechtliche) Regulierung zu identifizieren. Vgl. etwa das prominente Drei-Schichten-Modell der Internet-Regulierung, das zwischen physischer Infrastruktur-Schicht (*physical infrastructure layer*), die aus Kabel, Routern etc. besteht, der logischen Schicht (*logical layer*), die aus Software besteht, und der Inhaltsschicht (*content layer*), die die Kommunikationsinhalte enthält, unterscheidet: *Y. Benkler*, From Consumers to Users, Fed. Comm. L. J. 52 (2000), S. 561 (562); übernommen etwa von *L. Lessig*, The Architecture of Innovation, Duke L. J. 51 (2002), S. 1738 (1786). Weitere Beispiele für die Verwendung von Schichtenmodellen zur Kartierung von Regulierungsfragen *L. Solum/M. Chung*, The Layers Principle, Notre Dame L. Rev. 79 (2004), S. 815 (816 ff.); *Libicki*, Cyberdeterrence and Cyberwar, 2009, S. 12; *J. Zittrain*, The Future of the Internet, 2008, S. 67; *N. Choucri*, Cyberpolitics in International Relations, 2012; *V. Cerf/P. Ryan/M. Senges*, Internet Governance is our Shared Responsibility, I/S: A Journal of Law and Policy for the Information Society 10 (2014), S. 1 ff. (zur Internet Governance).

[32] Für eine alternative Rekonstruktion, die zwischen den Themenbereichen „Gerät", „Netzwerk", „System", „Daten", „Anwendungen" und „Nutzer" differenziert, siehe *A. van der Wees/D. Stefanatou/P. Pathania*, Work Package 4: Policy and the European Dimension Deliverable D4.2, 2020, S. 23 ff. (vgl. allerdings auch a. a. O., S. 88, die Diagnose, dass diese Art der Gliederung für rechtliche Analysen kaum anschlussfähig ist). Siehe zum Folgenden auch die instruktive Studie von *Bannelier/Christakis*, Cyber-Attacks – Prevention-Reactions, 2017.

zubeziehen, wenn die Vorgaben für die Systembetreiber nicht leerlaufen sollen (bb.). Schließlich müssen jene Kommunikationsarchitekturen gesichert werden, die den Rahmen für die den Austausch von Informationen zwischen Netzwerken setzen, d. h. vor allem das Internet. Gegenüber anderen Netzwerkverbünden zeichnet sich das Internet unter anderem dadurch aus, dass es nicht einheitlich verwaltet ist, Sicherheit also nicht zentral implementiert werden kann. Als „Netzwerk der Netzwerke" ist das Internet nicht nur selbst gefährdet; die Schwächen seiner Architektur können vielmehr auch für Angriffe auf alle daran angeschlossenen Systeme genutzt werden. Dies wirft eigenständige Regulierungsfragen auf (cc.). Der Gesetzgeber darf die einzelnen Schichten nicht je für sich isoliert betrachten. Jeder Ansatz zur technischen oder rechtlichen Regulierung muss vielmehr eine schichtenübergreifende Perspektive einnehmen (c.).

aa) System- und Netzwerksicherheit

Werden einzelne Software- und Hardware-Komponenten in Form der sogenannten von Neumann-Architektur kombiniert,[33] entsteht ein Computer bzw. – sollen die Fähigkeiten des Computers zur Informationsverarbeitung hervorgehoben werden – ein informationstechnisches System (IT-System). Unter diesen Begriff fallen nicht nur Personalcomputer, Peripheriegeräte, Kommunikationsgeräte, Datenbanken oder Server. Auch industrielle Steuerungsanlagen, Messsysteme oder die operative Technik für den Betrieb der Energienetzinfrastruktur (etwa Umspannstationen) integrieren bzw. sind IT-Systeme. Heutzutage werden IT-Systeme üblicherweise nicht isoliert betrieben, sondern sind Teil von mehr oder weniger großen Netzwerken.[34]

Systeme und Netzwerke können zahlreiche unterschiedliche Schwachstellen[35] aufweisen, wobei ihre Verletzlichkeit mit dem Grad ihrer technischen

[33] Zurückgeführt auf *J. von Neumann*, First Draft of a Report on the EDVAC (1945), S. 27 ff.

[34] Auch die Verbindung eines handelsüblichen PCs mit seinen Peripheriegeräten (Tastatur, Drucker etc.) ist bereits ein „Netzwerk" i. S. v. ISO/IEC 2382:2015–05 „Information technology – Vocabulary", wo „network" definiert wird als „arrangement of nodes and interconnecting branches". Sofern weiter zwischen System- und Netzwerksicherheit differenziert wird, werden mit letzterer vor allem die Sicherheit mittlerer und größerer Netzwerke in Verbindung gebracht, insbes. von sog. local area networks (LAN), die alle IT-Systeme innerhalb eines begrenzten räumlichen oder institutionellen Zusammenhangs (Unternehmen, Behörde etc.) umfassen, sowie von Metropolitan, Wide und Internet Area Networks. Angesichts der Tatsache, dass auch globale Netzwerke nur einen abgeschlossenen Nutzerkreis zulassen können (etwa im Fall von Virtual Private Networks), darf die Aussagekraft der geographischen Kategorien nicht überschätzt werden.

[35] Zum für den Diskurs zentralen Begriff der Schwachstelle, der auf alle drei hier unterschiedene Schichten Anwendung findet vgl. die technische Definition in *IETF*, Internet Security Glossary RFC 2828 (May 2000), https://datatracker.ietf.org/doc/html/rfc2828: „A flaw or weakness in a system's design, implementation, or operation and management that

Komplexität steigt.[36] Gefährdet sind keineswegs nur solche Systeme und Netzwerke, die der persönlichkeitsrechtsrelevanten Kommunikation dienen; auch vernetzte Industrieroboter, Kraftwerksturbinen oder Pipelines sind relevante Angriffsziele.[37] Gerade industrielle Anlagen haben oft gravierende Sicherheitslücken etwa in Gestalt ungesicherter Fernwartungszugänge.[38]

Die möglichen Angriffsvektoren sind zahlreich und reichen von gezielten Hacks über die massenhafte Versendung von Malware[39] bis hin zu Distributed

---

could be exploited to violate the system's security policy". Siehe auch § 2 Abs. 6 BSIG: „Sicherheitslücken im Sinne dieses Gesetzes sind Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen Systeme beeinflussen können." Entsprechend nun Art. 6 Abs. 15 NIS 2-RL, wonach unter Schwachstelle jede „Schwäche, Anfälligkeit oder Fehlfunktion eines IT-Produkts oder eines IT-Dienstes, die bei einer Cyberbedrohung ausgenutzt werden kann", verstanden wird.

[36] Welche Risiken der Betrieb eines IT-Systems begründet, lässt sich nicht abstrakt bestimmen, sondern hängt vom konkreten Aufbau ab. Einen Anhaltspunkt für typische Angriffspunkte geben die technischen Standards und Richtlinien zur sicheren Gestaltung von IT-Systemen und Netzwerken. So werden in der maßgeblichen Kategorie des IT-Grundschutz-Kataloges des BSI für IT-Systeme aktuell 22 IT-Systeme szenarienbasiert im Hinblick auf ihr individuelles Risikoprofil diskutiert. Typische Schwächen sind etwa ungenügendes oder fehlerhaftes Rechtemanagement, Ausnutzen von Fehlern beim Zusammenspiel von Betriebssystem- und Software-Komponenten, fehlerhafte Konfiguration von Hardware oder Software sowie ein unzureichendes Hardware- oder Software-Management während des Betriebs des IT-Systems. Zur Netzwerksicherheit gehören ferner etwa die Einrichtung von Firewalls (gesicherte Schnittstellen). Vgl. den Baustein „SYS: IT-Systeme" des IT-Grundschutz-Kompendiums sowie die Analysen für industriell genutzte IT-Systeme im Baustein „IND: Industrielle IT". Abrufbar je unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grund schutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html (Stand: 2022). Siehe konkret etwa auch *BSI*, SYS. 1.1: Allgemeiner Server, Februar 2021.

[37] Dies gilt insbesondere seit Kriminelle vermehrt sog. „Ransomware" für Erpressungszwecke nutzen, vgl. *BSI*, Die Lage der IT-Sicherheit in Deutschland 2020, 2020, S. 11 ff., 15 ff., 29 ff.; *BSI*, Lage der IT-Sicherheit in Deutschland 2021, 2021, S. 12 f.

[38] *BSI*, Industrial Control System Security: Top 10 Bedrohungen und Gegenmaßnahmen v1.3, 27.2.2019.

[39] Zur Terminologie: Üblicherweise wird bei Malware zunächst zwischen sogenannten „Viren" (hängen sich an Programme oder Dateien an und bedürfen zur Weiterverbreitung im Ziel-IT-System und/oder Netzwerk der Mitwirkung des Nutzers etwa durch Öffnen von Programm oder Datei) und „Würmern" (verbreiten sich ohne Mitwirkung des Nutzers im Zielsystem und nutzen dazu Schwächen in der Netzwerk- oder der Anwendungssoftware) unterschieden. Weiter existieren „trojanische Pferde", scheinbar harmlose Programme, die der Nutzer oft selbst installiert, die aber zugleich ihm verborgene schädliche Funktionen enthalten. Viren, Würmer und trojanische Pferde können genutzt werden, um Software auf Rechnern zu installieren, die sogenannte „Backdoors" öffnet und damit Unbefugten in Zukunft erleichterten Zugang zum Ziel-IT-System verschafft. Von „Rootkits" spricht man, wenn die eingebrachte Software das IT-System auf einer tiefen Ebene infiltriert, sich etwa Administratorrechte verschafft oder durch Einbringung ins Betriebssystem herkömmlicher Antiviren-Software entgeht. Möglich ist schließlich auch, dass Nutzer durch den Besuch einer vorher präparierten Internetseite unwissentlich den Download einer Software bewirken,

Denial of Service (DDoS)-Angriffen und Formen des Social Engineering[40].[41] Angriffe auf Netzwerke nutzen neben Schwächen der konkreten System- und Netzwerkkonfiguration auch Schwachstellen der Hard- und Software der physischen Netzwerkinfrastrukturen, der involvierten IT-Systeme sowie auch der menschlichen Nutzer aus.[42] Netzwerksicherheit schließt daher immer auch Systemsicherheit und Komponentensicherheit (auch, aber nicht nur von spezifischen Netzwerkkomponenten) ein.

Angreifer können, wie beschrieben, von ganz unterschiedlichen Motiven getrieben sein und sich einer Entdeckung oft effektiv entziehen.[43] Dies erschwert die Abwehr. Während die Manipulation eines unvernetzten IT-Systems regelmäßig verlangt, dass der Angreifer physische Nähe zum IT-System herstellt, etwa indem er sich selbst Zugang zum System verschafft, oder Mitarbeiter manipuliert, genügt bei vernetzten Systemen der Zugriff auf einen Netzwerkknoten (z. B. ein in das Netzwerk eingebundenes IT-System) oder auf eine Verbindung (z. B. ein Kabel), um unautorisierten Zugriff auf das Netzwerk, die darin eingebundenen Systeme und die dort verfügbaren Informationen zu erlangen und weitergehende Schädigungshandlungen in Form des Löschens, Unterdrückens, Unbrauchbarmachens oder Veränderns der im Netzwerk gespeicherten Daten vorzunehmen.[44] Die Anbindung von Syste-

---

die dann unter Ausnutzung der Sicherheitslücken des Browsers eine der Schadprogrammarten installiert (sog. Drive-by-Infection). Standardvarianten für alle derartigen Schadprogramme sind im Internet weit verbreitet; für avancierte Versionen, die etwa noch unbekannte Sicherheitslücken ausnutzen (sog. Zero-Day-Exploits), besteht ein lukrativer Markt.

[40] Beim „Social Engineering" verleiten Angreifer Personen, die im Rahmen ihrer Tätigkeit als Mitarbeiter Insider-Zugriff auf das Netz des Opfers haben – idealerweise IT-Personal mit Administrator-Rechten –, dazu, Dritten Zugriff zu verschaffen. Klassisch geschieht dies, indem Schadsoftware mittels Spam-Mails großflächig verbreitet wird. In jüngerer Zeit bedienen sich Angreifer vermehrt gezielterer Taktiken („Spear-Phishing"). Auch unzufriedene Mitarbeiter oder Whistleblower können Angreifern die Türen öffnen.

[41] Der Darstellung dieser Praktiken und ihrer rechtlichen Konsequenzen widmet sich eine umfassende informationstechnische und informationsstrafrechtliche Literatur, auf die an dieser Stelle verwiesen werden kann, vgl. bspw.: *Singer/Friedman*, Cybersecurity and Cyberwar, 2014; H.-J. Lange/A. Bötticher (Hrsg.), Cyber-Sicherheit, 2015; *F. Groom/K. Groom/S. Jones*, Network and Data Security, 2016; *Kochheim*, Cybercrime und Strafrecht, 2. Aufl. 2018. Zum aktuellen Stand vgl. *BSI*, Die Lage der IT-Sicherheit in Deutschland 2020, 2020, S. 15 ff., 29 ff.; *BSI*, Lage der IT-Sicherheit in Deutschland 2021, 2021, S. 10 ff.

[42] Üblicherweise werden passive (Antennen, Kabel etc.) und aktive (wie Router, Switch etc.) Komponenten unterschieden; teilweise kann die Funktion einzelner Komponenten auch durch Software erbracht werden. Siehe beispielhaft zu den erheblichen Defiziten der Software von Breitband-Routern *BSI*, Die Lage der IT-Sicherheit in Deutschland 2016, 2016, S. 12.

[43] Siehe oben § 4 II. 2.

[44] Für eine differenzierte Darstellung der Formen, die derartige Angriffe annehmen können, vgl. die Kommentarliteratur zu §§ 202a ff., 303a ff. StGB sowie im Überblick insbes. *Haase*, Computerkriminalität im Europäischen Strafrecht, 2017, S. 71 ff.; *Kochheim*, Cybercrime und Strafrecht, 2. Aufl. 2018, S. 227 ff.

men an globale Netzwerke wie das Internet ermöglicht Angreifern, weitgehend ortsungebunden agieren. Aus diesem Grund wird teilweise „Entnetzung" – also die Abkopplung bestimmter sensitiver IT-Systeme insbesondere vom Internet – als Strategie zur Reduktion von Informationssicherheitsrisiken empfohlen.[45] Allerdings schützt auch eine solche Entnetzung nicht umfassend. Möglich bleiben insbesondere der unautorisierte physische Zugriff sowie das Social Engineering. Zudem kann die Entnetzung unter Umständen dadurch unterlaufen werden, dass die verwendete Hard- oder Software bereits beim Einbau mit sogenannten „back doors" versehen wird. Und selbst dort, wo eine physische Trennung erfolgt, also ein sogenannter „air gap" installiert wird, sind Angriffe nicht ausgeschlossen, wie die Fälle „Stuxnet" und „agent.btz" gezeigt haben.[46]

Die Erhöhung der System- und Netzwerksicherheit ist in erster Linie den Betreibern möglich, die entsprechende Abwehrmaßnahmen ergreifen können, an denen sie regelmäßig auch ein hohes Eigeninteresse haben (sollten).[47] Die Betreiber sind dementsprechend traditionell die primären Adressaten informationssicherheitsspezifischer Pflichten in der technischen Normung und im Recht.[48] Soweit IT-Systeme im Rahmen größerer Organisationseinheiten eingesetzt werden, kann die Verantwortung intern weiter abgestuft werden.[49] Bei der Ausgestaltung des Pflichtenprogramms ist zudem, wie erwähnt, zu berücksichtigen, dass sich um jedes vernetzte System typischerweise ein Ökosystem von Drittanbietern lagert, einschließlich der für die Sicherheit der Netzwerkkomponenten verantwortlichen Hersteller. Ein exklusiver Fokus der IT-Sicherheitsgewährleistung auf die Betreiber von Systemen und Netzwerken wäre daher zu eng.

---

[45] Vgl. dazu aus Sicht des BSI *H.-T. Langwald/J. Sanders et al.*, Stand der Technik im Bereich der Kritischen Infrastrukturen, BSI Forum 27:6 (2019), S. 35 (38).

[46] Auch aus Anwendersicht ist es nur in wenigen Fällen möglich, einen air gap zu implementieren, vgl. *Joe*, Mind the (Air) Gap, 31.5.2021. Die IT-Sicherheitsforschung diskutiert im Übrigen zahlreiche Szenarien zur Überwindung des air gap, etwa durch Messung der elektromagnetischen Abstrahlung, des Stromverbrauchs, der Vibrationen oder der Thermik eines IT-Systems mittels Radiowellen, Laser-Technologie etc.

[47] *Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022, Rn. 2. Dazu, warum dies in der Praxis nicht immer der Fall ist, siehe unten § 6 Fn. 142.

[48] Bereits § 6 BDSG 1977 verpflichtete datenschutzrechtlich Verantwortliche zu einer entsprechenden Systemgestaltung. Vertiefend dazu § 6 II. 4 a).

[49] Die Bausteine des Grundschutz-Kompendiums des BSI ordnen sich nach Schichten (ORG: Organisation und Personal; APP: Anwendung; SYS: IT-Systeme; NET: Netze und Kommunikation; INF: Infrastruktur; etc.), denen dann jeweils besondere Primärzuständigkeiten innerhalb der Organisation zugeordnet werden (für APP: Anwendungsverantwortliche und-betreiber; für SYS: Zuständige für IT-Systeme; für NET: Netzadministratoren; für INF: Haustechnik; etc.). Dazu sowie zur organisationsinternen „Organisation des Sicherheitsprozesses" ausführlich *BSI*, BSI-Standard 200–2: IT-Grundschutz-Methodik, S. 36 ff., 137.

bb) Komponentensicherheit

Schon aus Sicht der System- und Netzwerksicherheit rückt also die Sicherheit von Hard- und Software in den Fokus der IT-Sicherheitsregulierung.[50] Viele zur System- und Netzwerksicherheit getroffene Feststellungen lassen sich auf die Komponentensicherheit übertragen. So ist erneut vor allem die Komplexität der technischen Komponenten ein Risikofaktor. Sowohl konkrete Kodierungsfehler als auch die Software- und Hardware-Gestaltung können die Anfälligkeit für Angriffe erhöhen. Von Schwachstellen freie Software existiert praktisch nicht.[51] Nicht alle Fehler sind dabei sicherheitstechnisch relevant, was die Bewertung des mit ihnen verbundenen Risikos erschwert.[52] Um eine Sicherheitslücke zu begründen, muss es vielmehr möglich sein, den Fehler so auszunutzen, dass Unbefugte Zugriff auf das die Software verwendende IT-System oder Netzwerk erlangen können (Exploit).[53] Ob und inwieweit Schwachstellen der Software ein Risiko für den Systemgebrauch begründen, hängt also von ihrer Art, der Qualität des Angriffs und den Sicherheitsmaßnahmen des Systems ab. Soweit Standardkomponenten verwendet werden – also kommerziell erhältliche Produkte, deren Integration keine individuelle

[50] Hardware bezeichnet die physischen Komponenten des Systems (Prozessoren, Speicherwerke, Input- und Output-Geräte etc.). Die Programme, die die Aktivitäten des IT-Systems steuern, sind dessen Software; im Unterschied zur Hardware ist Software nicht sinnvoll über physische Manifestationen definierbar, sondern besteht in einem bestimmten Zustand des Speichermediums bzw. in einer bestimmten Konfiguration der Schaltkreise. Die Unterscheidung von Hardware und Software ist analytisch hilfreich, praktisch aber nicht immer eindeutig. Denn erstens sind auch Hardwarekomponenten mit Steuerungsprogrammen (Firmware) ausgestattet, die untrennbar mit der Struktur der Hardware verwoben sein können. Zweitens können Funktionen innerhalb eines Rechensystems oft sowohl von darauf spezialisierter Hardware als auch von Software wahrgenommen werden. Drittens werden in jüngerer Zeit infolge der Nutzung von Cloud Computing, Virtualisierung etc., Funktionen vermehrt „nicht mehr statisch durch die eingesetzte Hardware definiert […], sondern dynamisch konfiguriert" (Software-defined Everything). Zur Entwicklung der Computer-Architektur instruktiv aus historischer Sicht *G. Dyson*, Turing's Cathedral, 2012, S. 77 ff., 278 ff.; aus technischer Sicht *L. Null/J. Lobur*, Computer Organization and Architecture, 5. Aufl. 2018.

[51] Vgl. zu dieser auch als „Assume-Breach-Paradigma" bezeichneten Diagnose auch BVerfG, NVwZ 2021, 1361, Rn. 38 m. w. N.

[52] Eine standardisierte Klassifikation bekannter Schwachstellen bietet das Common Weakness Enumeration System (CWE), abrufbar unter http://cwe.mitre.org/about/index.html. Konkrete Schwachstellen werden klassifiziert nach dem Common Vulnerabilities and Exposures System (CVE), abrufbar unter: https://www.cve.org. Die Schwere von Schwachstellen kann nach dem Common Vulnerability Scoring System bestimmt werden (CVSS), abrufbar unter https://www.first.org/cvss/. Speziell dazu *P. Mell/K. Scarfone/S. Romanosky*, A Complete Guide to the Common Vulnerability Scoring System, Version 2.0, 2007. Allgemein zum Problem der Risikobewertung im Bereich Informationssicherheit *D. Hubbard/R. Seiersen*, How to Measure Anything in Cybersecurity Risk, 2016; *R. Slayton*, Measuring Risk, IEEEA 37:2 (2015), S. 32. Überblicksartig auch *K. Sohr/T. Kemmerich*, Technische Grundlagen der Informationssicherheit, in: Kipker (Hrsg.), 2020, Kap. 2 Rn. 155 ff.

[53] Vgl. *BSI*, Die Lage der IT-Sicherheit in Deutschland 2020, 2020, S. 22 ff.

Anpassung verlangt und die dadurch regelmäßig kostengünstig und benutzerfreundlich sind –, sind entsprechende Fehler aufgrund der oft globalen Verbreitung dieser Produkte besonders folgenreich. Gleiches gilt für populäre Open-Source-Software. Hardware-Schwachstellen stehen oft weniger im Fokus als Software-Schwächen.[54] Allerdings sind auch hier vielfältige Manipulationen denkbar, etwa der mechanischen Komponenten[55] oder der in die Hardware integrierten Firmware[56]. Entsprechende Schwachstellen können zur physischen Beschädigung der Hardware selbst oder, bei cyber-physischen Systemen, zum Angriff auf ihre Umwelt genutzt werden.[57]

Typischerweise suchen Angreifer in Systemen und Netzwerken nach bekannten Schwachstellen. Das Auffinden und Ausnutzen komplexerer Sicherheitslücken verlangt dabei regelmäßig umfangreiche Planungen und Ressourcen. Dies gilt besonders dann, wenn Schwachstellen bereits in (Teil-)Komponenten implementiert oder Lieferketten kompromittiert werden sollen, wie dies etwa im Falle der Netzwerkmanagement-Software des Unternehmens SolarWinds der Fall war.[58] Zu berücksichtigen ist insofern, dass die Entwicklung von IT-Komponenten heute regelmäßig ein vielschichtiger, oft hochgradig arbeitsteiliger Prozess ist. Vielfach verwenden Hersteller „von Dritten entwickelte Technologien und Bestandteile wie Software-Module, Bibliotheken oder Programmierschnittstellen […] und sind von diesen abhängig".[59] Lange Lieferketten sind entsprechend verwundbar. Entsprechende Hintertüren (Backdoors) in der Software, der System-Hardware oder den Netzwerkkomponenten können dann beim Endnutzer per Internet aktiviert und zur Spionage oder zur Einbringung von weiterem Schadcode genutzt werden.

Wie im Fall der System- und Netzwerksicherheit bleiben Identität, Standort und Motivationslage der Angreifer oft unbekannt. Die Vermeidung und Behebung entsprechender Schwachstellen muss daher in erster Linie den Herstellern der jeweiligen Komponenten obliegen, die am ehesten Investitionen in die Sicherheit ihrer Produkte tätigen können. Zahlreiche technische Normen geben dabei in Sachen Fehlererkennung und -vermeidung Orientierung. Diese werden durch eine zunehmend ausdifferenzierte IT-Sicherheitsforschung kon-

---

[54] Vgl. *BSI*, Die Lage der IT-Sicherheit in Deutschland 2020, 2020, S. 26 ff.

[55] Vgl. die Darstellung der Schwachstellen „Spectre" und „Meltdown", die Prozessoren aller namhaften Hersteller betrafen, bei *BSI*, Die Lage der IT-Sicherheit in Deutschland 2018, 2018, S. 44 ff.

[56] Vgl. die Darstellung eines derartigen Angriffs und der damit verfolgten Ziele der sogenannten „Equation Group" *Kaspersky Lab*, Equation Group: The Crown Creator of Cyber-Espionage, 16.2.2015. Zur Bewertung durch das BSI siehe *C. Kurz*, Keine Antworten der Festplatten-Hersteller auf NSA-Infiltration, Netzpolitik.org, 13.5.2015.

[57] Für ein Beispiel aus dem Kontext des Ukraine-Krieges siehe *R. Santamarta*, SATCOM terminals under attack in Europe. A plausible analysis, 7.3.2022.

[58] Siehe oben § 1 Fn. 16.

[59] So die präzise Beschreibung in ErwGr 12 CSA. Dazu weiter unter § 6 II. 6.

kretisiert. Komponentensicherheit ist dabei ein Qualitätsmerkmal, für das jedenfalls bei kommerziell vertriebenen Software- und Hardware-Komponenten – wenn auch nur in Ansätzen – ein Markt etabliert ist.[60] Allerdings erweist sich die konkrete Verteilung von Verantwortung innerhalb der regelmäßig langen Lieferketten als kompliziert und wird auch vertraglich bislang selten je näher geregelt.[61] Existenz und Ausmaß sogenannter „Third-Party Cyber Risks" sind den Marktteilnehmern oft nicht hinreichend bewusst.[62] Hier stößt die Selbststeuerung an Grenzen. Für die Regulierung der Komponentensicherheit erweist es sich daher als besondere Herausforderung, das ganze Ökosystem der Software- bzw. Hardware-Entwicklung in den Blick zu nehmen.

cc) Internetsicherheit

Die Sicherheit des Internets bildet einen Sonderfall der Netzwerksicherheit, da sich das Sicherheitsproblem hier im globalen Maßstab stellt und zudem kein einheitlicher „Betreiber" oder sonst Letztverantwortlicher existiert. Gekoppelt mit der extremen Durchdringungstiefe des Internets, von dem heute nur noch einzelne besonders sensitive IT-Systeme mehr oder weniger effektiv getrennt sind, führt dies zur Brisanz der Thematik. Dabei muss zunächst unterschieden werden: Keine internetspezifischen IT-Sicherheitsrisiken liegen vor, wenn das Internet allein zur Verbreitung von Viren, Würmern etc. genutzt wird, die allein Schwachstellen der an das Internet angeschlossenen Netze und Systeme ausnutzen. Internetspezifische Risiken sind vielmehr solche, die Schwachstellen der spezifisch für die Kommunikation über das Internet erforderlichen Infrastrukturen, Komponenten, Protokolle oder Dienste ausnutzen, sei es um die das Internet tragenden Systeme selbst oder um die an das Internet angebundenen IT-Systeme zu beeinträchtigen. Einer bekannten Erzählung zufolge ist die dezentrale Architektur des Internets zwar darauf ausgelegt, möglichst widerständig gegenüber Angriffen zu sein; das gilt jedoch allenfalls für Angriffe auf seine physische Infrastruktur.[63]

---

[60] Zu dessen Limitationen § 6 II. 3 a).

[61] Dies galt jedenfalls lange Zeit, ist allerdings wohl überholt, sofern IT-Sicherheit zur Hauptleistungspflicht von Verträgen gemacht wird. Siehe dazu weiter § 6 Fn. 138 und 143 sowie § 6 II. 4 b).

[62] *J. Germano*, Whitepaper: Third-Party Cyber Risk & Corporate Responsibility, 2017.

[63] Zur Ursprungsgeschichte des ARPANET, des Vorläufers des heutigen Internets siehe *J. Abbate*, Inventing the Internet, 1999; *C. Moschovitis/H. Poole et al.*, History of the Internet, 1999; *S. Lukasik*, Why the Arpanet Was Built, IEEEA 33:3 (2011), S. 4 ff. Während umstritten ist, welche Bedeutung die militärische Komponente insgesamt für die Entwicklung hatte (vgl. *B. Leiner/V. Cerf et al.*, Brief History of the Internet, 2000, Fn. 5; siehe auch allgemein oben § 3 Fn. 105) – zumindest die Beiträge der RAND-Gruppe hatten eine distinkte Stoßrichtung hin zur Entwicklung belastbarer Kommunikationssysteme im Falle eines Nuklearangriffs, vgl. *P. Baran*, On Distributed Communications Networks, IEEE Transactions on Communications Systems 12:1 (1964), S. 1 ff. – ist weitgehend konsentiert, dass das im

Zur technischen Vertiefung: Als „Netzwerk der Netzwerke" dient das Internet zur Übermittlung von Informationen zwischen Sender und Empfänger über die Grenzen lokaler Netzwerke hinweg. Wie jedes Netzwerk baut das Internet auf einer *physischen Infrastruktur* auf. Im Fall des Internets sind die Netzwerkknoten selbst öffentliche und private Netzwerke unterschiedlicher Art und Größe, die untereinander durch Kabel oder Funk verbunden sind. Die Teilnetze werden auch als Autonome Systeme (AS) bezeichnet.[64] Diese „Hardware" des Internets wird durch *Software* gesteuert, die die Kommunikation zwischen allen angeschlossenen IT-Systemen, also über lokale Netzwerkgrenzen hinweg, erlaubt. Möglich wird dies, da die Software einem vorab definierten Set von technischen Standards bzw. *Protokollen* folgt, die die Bedingungen der Kommunikation zwischen den Netzwerken und den angeschlossenen IT-Systemen einheitlich regelt. Die für die Internetkommunikation entscheidenden Protokolle sind die der TCP/IP-Suite.[65] Infrastruktur und Protokolle werden schließlich dazu genutzt, um über das Internet *Dienste* anzubieten. Hierzu gehören insbesondere E-Mails, Datentransfers sowie das World Wide Web – jene bekannte, im Wege des Hypertext Transfer Protocol (HTTP) über Browser zugängliche Dokumentensammlung. Diese Dienste sind aus Sicht der Nutzer oft das Wesentliche, bilden jedoch aus technischer Sicht nur in Verbindung mit der Infrastruktur und den Protokollen „das Internet".

Das Internet besteht also nicht nur aus den miteinander verbundenen IT-Systemen der Sender und Empfänger bestimmter Kommunikationen, sondern ruht auf einer komplexen, durch gemeinsame Protokolle gesteuerten Infrastruktur aus Netzbetreibern, Betreibern von BGP- und DNS-Servern (hierzu gleich), Zertifikatstellen, Internet Service Providern, Hard- und Softwareentwicklern, Internetdiensten etc. Diese elaborierte Architektur ermöglicht Nutzern eine reibungslose Kommunikation, deren technische Details unter der Oberfläche verborgen bleiben. Hinter dem oft als eine Art sozialer Tatsache wahrgenommenen Internet steht aber tatsächlich eine komplexe Ma-

---

Ergebnis implementierte technische Design eine hohe Stabilität gegen Angriffe auf die physische Infrastruktur aufweist. Zu dessen theoretischen Grenzen vgl. *R. Cohen/K. Erez et al.*, Breakdown of the Internet, Physical Review Letters 86:16 (2001), S. 3682 ff. Allerdings ist das Internet nur aus technischer Sicht stark dezentral organisiert; aus ökonomisch-rechtlicher Sicht ist es heute ein hierarchisiertes Gebilde, vgl. *A. Mathew*, The Myth of the Decentralised Internet, Internet Policy Review 5:3 (2016); *Kettemann*, The Normative Order of the Internet, 2020, S. 27 ff.; dazu weiter auch gleich bei § 6 Fn. 70.

[64] Autonome Systeme (AS) sind solche Netzwerke oder Netzwerkverbünde, die selbständig und einheitlich regeln können, welchen Weg die Datenströme zwischen den je zu ihrem Netz gehörenden IT-Systemen nehmen sollen. Hierzu zählen etwa die Netze von Internet Service Providern (ISP), großen Unternehmen oder Universitäten, die je als AS organisiert sind. Die Teilnetze unterscheiden sich erheblich in Art und Größe. Das Internet kann als Summe der miteinander verbundenen, den etablierten Protokollen genügenden AS verstanden werden.

schinenarchitektur, deren Betrieb – und Sicherheit – durch das koordinierte Zusammenwirken verschiedenster Instanzen gewährleistet wird.

Dies sei hier am Beispiel des Internet Protocol (IP) illustriert.[66] Das IP legt die Grundlage für die Weiterleitung von IP-Datenpaketen (auch: Datagrammen) vom sendenden IT-System bis zum Empfänger – das sogenannte Routing – im gesamten globalen Netz, also über die Grenzen der einzelnen zum Internet zusammengeschlossenen Netzwerke hinweg. Das Protokoll definiert, wie die über das Internet versendeten Datenpakete aufgebaut sind und legt Regeln für ein Adresssystem fest, das ermöglicht, allen am Internet teilnehmenden IT-Systemen eine eindeutige Adresse zuzuweisen und sie logischen Einheiten (Subnetzen) zuzuordnen. Das Protokoll selbst trifft keine Regelungen dafür, wie gesichert wird, dass die Daten tatsächlich an den Empfänger gelangen; es legt nur fest, wie erkannt werden kann, woher die Daten

[65] Das TCP/IP-Referenzmodell definiert statt der sieben Schichten des Open Systems Interconnection Model (OSI/ISO-Modell) vier funktionale Schichten (Layer). Jede Schicht nimmt eine für den Austausch von Kommunikation wesentliche Funktion wahr und folgt bestimmten, vorab in Protokollen definierten Regeln. Beim Sender wird eine Information von der obersten zur untersten Ebene weitergereicht und auf diesem Weg für den Transport kodiert. Auf der untersten sog. Bitübertragungsschicht wird sie mittels Kabel oder Antenne in Form elektronischer Signale, Wellen (Funk) oder auf andere Weise an den Empfänger übermittelt. Dort wird sie aufgenommen und dann in protokollgemäßer Umkehrung der beim Sender vollzogenen Operationen wiederum an die je nächsthöhere Ebene weitergegeben. Konkret für die Datenübertragung über das Internet: (1) Die Protokolle der untersten sogenannte Netzzugangsschicht (Link Layer) regeln die Bitübertragung, legen also Standards für den Austausch von Daten zwischen miteinander per Kabel oder Funk verbundenen IT-Systemen fest. Die IEEE-Norm 802.3 definiert den entsprechenden Ethernet-Standard und die IEEE-Norm 802.11 definiert den Link Layer im WLAN. (2) Die Protokolle der zweiten sog. Internetschicht (Internet Layer) regeln die Vermittlung von Datenpaketen innerhalb des Internets über Routing; zentrales Protokoll dieser Schicht ist das durch RFC 791 (1981) und RFC 2460 (IPv6, 1998) definierte Internet Protocol. (3) Die Transportschicht (Transport Layer) enthält Protokolle (insbes. das Transmission Control Protocol [TCP]), die eine sog. Ende-zu-Ende-Kommunikation zwischen Sender und Empfänger ermöglichen und die Zuverlässigkeit des Datenstroms sichern. (4) Auf der obersten sog. Anwendungsschicht (Application Layer) operieren zahlreiche Protokolle (BGP, HTTP, SMTP, POP etc.), die u. a. sicherstellen, dass die Daten von weiteren Programmen der beteiligten IT-Systeme verarbeitet werden können (etwa: Webbrowser, E-Mail-Programme).

Werden über Kabel (Ethernet) Daten zwischen IT-Systemen über das Internet ausgetauscht, enthält ein vom IT-System des Senders ausgehendes sog. „Datenframe" folgende Bestandteile: Das (1) Ethernet-Frame (mit MAC-Adressen u. a.), das auf dem Link Layer die Kommunikation zwischen physisch verbundenen IT-Systemen initiiert; (2) das IP-Datagram (auch „Paket"), das in seinen Kopfdaten (header) Informationen über Quelle und Ziel der intendierten Internet-Kommunikation enthält; (3) das TCP-Segment (zugleich die „Nutzlast" [payload] des IP-Pakets), das seinerseits aus Kopfdaten (u. a. zur Sortierung und Sicherung der Integrität der folgenden Nutzlast) und aus eigener „Nutzlast", d. h. dem aus Sicht der Nutzer „eigentlich" zu übertragenden Datenstrom besteht; letzterer wird dann von Anwendungen wie Webbrowsern mittels Standards wie HTTP interpretiert.

[66] Das IP wird in einer als IPv4 bezeichneten Version seit 1981 eingesetzt. Die aktuelle sechste Version (IPv6) ist seit 2017 in RFC 8200 als „Internet Standard" definiert.

stammen und an welches Ziel sie gelangen sollen. Wie viele der das Internet tragenden Protokolle setzt das IP somit eine Verwaltungsinfrastruktur voraus, die das Protokoll implementiert.[67] Insbesondere ist die Vergabe der Adressen zu organisieren. Diese erfolgt durch ein hierarchisch geordnetes System von Stellen, das seine Spitze in der Internet Assigned Numbers Authority (IANA), einer Abteilung der seit 2016 rein privat organisierten Internet Corporation for Assigned Names and Numbers (ICANN), hat.[68] Die IANA, die sich als reines Register ohne jede Verantwortung für Inhalte versteht, weist bestimmte IP-Adressbereiche an fünf sogenannte Regional Internet Registries (RIRs) zu (für den europäischen Raum ist RIPE NCC mit Sitz in Amsterdam zuständig).[69] Diese verteilen die Adressbereiche ihrerseits blockweise weiter auf Local Internet Registries (LIR), häufig Internet Service Provider, die dann die Zuweisung der einzelnen IP-Adresse beim Endkunden vornehmen.

Die Komplexität der Internettechnologie schafft ein Spektrum an Gefährdungslagen, das entsprechend vielschichtige Abwehrmechanismen erfordert. Für die Sicherheit der Infrastrukturkomponenten des Internets, also insbesondere der Netzknotenpunkte, sind deren jeweilige Betreiber verantwortlich. Hier stellen sich analoge Probleme zur „normalen" Netzwerk- und Komponentensicherheit.[70] Besondere Schwierigkeiten bereiten darüber hinaus jene

[67] Dies betont auch *Kettemann*, The Normative Order of the Internet, 2020, S. 103, der unter Zitierung von *K. Auerbach*, Deconstructing Internet Governance, 26.2.2004, die mit dem Betrieb des Internets verbundenen minimalen Verwaltungsaufgaben wie folgt qualifiziert: „First, a system of IP address allocation […]. Second, a system of inter-carrier/inter-ISP traffic exchange […]. Third, a system to allocate protocol numbers and other similar identifiers […]. Fourth, the responsible and accountable operation of the upper layers of the DNS hierarchy including oversight, on behalf of the community of internet users, of a suite of Domain Name System (DNS) root servers. Fifth, the management of the DNS root zone file." Zu weiteren Verwaltungsaufgaben *Kettemann*, The Normative Order of the Internet, 2020, S. 103 ff.

[68] Seit 2000 ist die IANA als Teil von ICANN organisiert. Als solche nahm sie ihre Aufgabe zunächst auf der Grundlage eines Vertrags mit dem United States Department of Commerce (DOC) wahr, wobei dem DOC bestimmte Aufsichtsfunktionen verblieben und insbesondere Ergänzungen und Änderungen der sog. Rootzonendatei kontrolliert wurden. Dieser Vertrag lief am 30.9.2016 aus und die Verantwortung ging mit dem 1.10.2016 umfassend an ICANN, d. h. an eine rechtlich nach U.S.-Privatrecht organisierte, intern nach dem sogenannten Multistakeholder-Modell gegliederte Gesellschaft über. Zur Wahrnehmung der IANA-Funktionen und zur „transition" ausführlich *Kettemann*, The Normative Order of the Internet, 2020, S. 29 ff., 60 ff., 103 ff. Dazu, dass die regulatorische Kontrolle der USA über die IANA-Funktionen von ICANN auch vor 2016 eher theoretische Qualitäten hatte, siehe a. a. O., S. 31.

[69] Zu den Vertragsnetzwerken, auf deren Basis ICANN seine Funktionen ausübt, siehe *E. Weitzenboeck*, Hybrid Net, Int'l J. L. & Info. Tech. 22:1 (2014), S. 49 ff.

[70] Betrachtet man das Internet nicht aus technischer, sondern aus ökonomischer Sicht, zeigt sich, dass die Zahl der relevanten Betreiber der dezentralen Natur des Internets zum Trotz überschaubar ist. Heute konzentrieren einige wenige zentrale Anbieter große Teile der physischen Infrastruktur des Internets auf sich (insbes. die Glasfaserkabel) und unterhalten eine Vielzahl direkter physikalischer Verbindungen untereinander (sog. Tier-1-Provider).

Schwachstellen, die sich aus den zentralen Kommunikationsprotokollen bzw. den diese implementierenden Instanzen und Programmen ergeben. Dass die Internettechnologie hier leicht angreifbar ist, liegt auch daran, dass in der Designphase des Internets einseitig die Erleichterung von Kommunikation priorisiert wurde. Dementsprechend sorgen die für den Datenaustausch im Internet zentralen Protokolle – das Internet Protocol (IP),[71] das Border Gateway Protocol (BGP)[72] und das Domain Name System Protocol (DNS Protocol)[73] – zwar für einzigartig effiziente Kommunikation, haben jedoch – jedenfalls in ihrer Ursprungsfassung – kaum Sicherheitsmechanismen etabliert.[74] Eine Erhöhung des Sicherheitsniveaus muss daher auf Änderung dieser Protokolle zielen. Die Protokolle sind in als Request for Comments (RFCs) bezeichneten technischen Normen definiert, die von divers besetzten Fachgruppen der Internet Engineering Task Force (IETF) erarbeitet werden und dann auf Empfehlung der IETF von der Internet Engineering Steering Group (IESG) einem Multistakeholder-basierten Zustimmungsverfahren unterzogen werden.[75] In jüngerer Zeit hat die IETF tatsächlich verschiedene Anpassungen vorgenommen, die die Sicherheitslücken minimieren sollen. Doch sind diese neuen Protokollversionen weder universell implementiert – teilweise würde ihre Implementierung eine tiefgreifende Veränderung der Nutzungsgewohnheiten des Internets voraussetzen – noch sind sie ihrerseits stets fehlerfrei.

Worin die Schwachstellen der Protokolle bzw. ihrer Änderungen liegen, erschließt sich nur aus einer hier nicht leistbaren technischen Analyse. Für die hiesigen Zwecke reicht es aus, an einzelnen Beispielen zu zeigen, welcher

Wollen kleinere AS, etwa vorwiegend im Endkundengeschäft tätige Internet Service Provider, für ihre Kunden auf die Verbindungen dieser Tier-1-Provider zugreifen, um Daten mit deren Kunden oder anderen Internet-Teilnehmern auszutauschen, müssen sie für die Vermittlung grundsätzlich bezahlen. Unter dem Gesichtspunkt der Marktmacht ist diese starke Hierarchisierung des Internets nicht unproblematisch. Unter IT-Sicherheitsgesichtspunkten vereinfacht die Hierarchisierung jedoch die Identifikation von Akteuren, die für die Sicherheitsgewährleistung in Anspruch genommen werden können.

[71] Siehe oben § 6 Fn. 66.

[72] Das BGP wird seit 1994 eingesetzt. In seiner aktuellen Version ist es seit 2006 in RFC 4271 geregelt, zuletzt geändert durch RFC 8654.

[73] Das DNS Protocol setzt sich aus zahlreichen RFC zusammen, vgl. die Übersicht unter https://en.wikipedia.org/wiki/Domain_Name_System#Standards.

[74] Prägnant *Sivakumar*, Generative Security, AJIL Unbound 110 (2017), S. 358 f.: „As with any other technology, the tool embodied a set of politics and values, be it as a tool of communication designed to withstand a Cold War-era nuclear strike or highly recognizable cornerstone consumer product of an advertising-revenue driven Internet company. However, what the tool distinctly lacked were features of security and privacy that were desirable to, and perhaps implicitly assumed, by its users in this incident." Vgl. für das IP: *D. Clark*, The Design Philosophy of the DARPA Internet Protocols, Computer Communication Review 18:4 (1988), S. 106 ff.

[75] Siehe die Übersicht unter http://www.ietf.org/. Vgl. zu den Standards: http://www.rfc-editor.org. Zur Organisation der IETF und zum Verfahren der Standardsetzung näher *Kettemann*, The Normative Order of the Internet, 2020, S. 32, 260.

grundsätzlichen Art die Risiken sind, welche Entitäten potenziell die Verantwortung für eine Verbesserung der Sicherheitslage tragen, aber auch, wie begrenzt die Möglichkeiten zur Verbesserung in der Praxis sind.

(1) Internet Protocol (IP)[76]: Das IP schreibt vor, dass jedes von einem Rechner gesendete IP-Datagramm in seinen Kopfdaten (Header) die IP-Adresse des Absenders enthält; an diese Adresse wird dann die Antwort des Empfängers geleitet. Das IP sieht keine Schutzmaßnahmen vor, die verhindern, dass die Kopfdaten manipuliert und ein anderes IT-System als Absender eingetragen wird. Findet eine solche Manipulation statt, wird die Antwort des Empfängers an dieses Dritt-System weitergleitet, während der Erstsender anonym bleibt. Dieses sogenannte IP-Spoofing kann für verschiedene Zwecke ausgenutzt werden. Es eröffnet insbesondere die Möglichkeit für sog. Denial of Service (DoS)-Attacken: Durch unzählige Anfragen im Namen eines Dritten kann der Angreifer umfangreichen Datenverkehr zu dessen IT-System lenken, dieses zur Überlastung bringen und funktionsunfähig machen. Derartige Attacken haben nach wie vor ein erhebliches Stör- und Schädigungspotenzial. Bereits ab Mitte der 1990er-Jahre hat die IETF eine Reihe neuer Standards erlassen, die darauf zielen, das IP-System sicherer zu machen. Diese unter dem Begriff Internet Protocol Security (IPsec) zusammengefassten Standards sollen eine sog. Ende-zu-Ende-Sicherheit auf der Internetschicht gewährleisten.[77] Sie nutzen zur Authentifizierung zwischen Sender und Empfänger und zum Schutz der Kommunikation kryptographische Methoden. Das System gilt als verhältnismäßig sicher, ist jedoch nicht gänzlich immun gegen Attacken. Das Vertrauen in das als kompliziert zu bedienen geltende System litt auch darunter, dass die U. S. National Security Agency (NSA) der kompromittierenden Einflussnahme auf die dem Protokoll zugrundeliegende Verschlüsselungstechnologie bezichtigt wurde.[78] Heute findet IPSec vor allem im Rahmen virtueller privater Netzwerke (VPN) Einsatz. Im Rahmen der Kommunikation über das öffentliche Internet sind die Probleme des IP-Spoofing jedoch nach wie vor weitgehend ungelöst.

(2) Domain Name System Protocol (DNS): Das DNS Protocol bzw. die darauf basierenden Systeme erfüllen verschiedene Funktionen: Vor allem übersetzt das Protokoll die bekannten und einprägsamen Domainnamen (www.nyu.edu) in jene numerischen IP-Adressen, über die sich die an das Internet angeschlossenen IT-Systeme eindeutig identifizieren lassen, was das IP-basierte Routing der Daten ermöglicht. Hierfür greift das DNS Protocol mit dem Domain Name System auf eine weltweit verteilte Datenbank zu, die auch als Telefonbuch des Internets bezeichnet wird. Seine große praktische Bedeutung bezieht das DNS daraus, dass zahlreiche Internet-Anwendungen davon Gebrauch machen. Zur Umsetzung benötigt das DNS-Protokoll Organisationen, die die Verteilung und Verwaltung des Namensraums und das tägliche Management der Nameserver gewährleisten. Aus rechtlicher Sicht hat das DNS-System bisher vor allem insoweit Aufmerksamkeit auf sich gezogen, als die Zuständigkeit von IANA bzw. der

[76] Ausführlich hierzu *IETF*, Security Assessment of the Internet Protocol Version 4, RfC 6274, July 2011, https://tools.ietf.org/html/rfc6274; *F. Gont*, IPv6 Security for IPv4 Engineers, 2019, https://www.internetsociety.org/wp-content/uploads/2019/03/deploy360-ipv6-security-v1.0.pdf.

[77] Dokumentiert unter https://en.wikipedia.org/wiki/IPsec#IETF_documentation.

[78] Hierzu https://en.wikipedia.org/wiki/IPsec#Alleged_NSA_interference.

Delegatare für die Verteilung der Domain-Namen in Rede steht.[79] Die hierfür etablierten Governance-Strukturen von IANA und ICANN sind zuletzt 2016 im Zuge der Überführung der Kontrolle vom U.S.-Handelsministerium auf die ICANN zugeordnete Multistakeholder Community intensiv diskutiert worden.[80] Aktuell rücken hingegen die Sicherheitsrisiken des DNS in den Vordergrund. Denn in der ursprünglichen Fassung basiert das DNS weitgehend auf Vertrauen. Gelingt es Angreifern, einen DNS-Server zu übernehmen, können sie das DNS-System mit falschen Informationen füttern. Gibt ein Nutzer dann einen Domainnamen ein (etwa de.wikipedia.org) und vertraut darauf, dass das DNS-System diesem Namen die richtige IP-Adresse zuordnet, kann er – für ihn unerkennbar – an eine falsche IP-Adresse geleitet werden, auf der sich womöglich eine gefälschte Seite befindet, der er seine Daten anvertraut oder die so präpariert ist, dass mit dem Aufruf ein Schadprogramm heruntergeladen wird (Drive-by-Infection). Auch insoweit hat sich die IETF um Abhilfe bemüht und eine Reihe zusätzlicher Protokolle vorgelegt, die als Domain Name System Security Extensions (DNSSEC) bekannt sind und die die Integrität und Authentizität (nicht die Verfügbarkeit und Vertraulichkeit) der Antworten auf DNS-Anfragen sichern sollen.[81] Wie im Falle des IPSec erweist sich die Implementierung der Protokollergänzungen jedoch als schwergängig; zudem enthalten die Ergänzungen neue eigene Schwachstellen. Dennoch bzw. deshalb wird hier in jüngster Zeit verstärkt über eine rechtliche Regulierung der DNS-Sicherheit nachgedacht.[82]

(3) Transmission Control Protocol (TCP): Das TCP ist eng mit dem IP verbunden.[83] Primäre Funktion des TCP ist es, einen zuverlässigen Ende-zu Ende-Transport von Daten vom Sender zum Empfänger zu gewährleisten. Stark vereinfacht legt das TCP Regeln dafür fest, wie zwischen Sender und Empfänger sichergestellt werden kann, dass die gesendeten Daten vollständig und nicht korrumpiert sind; hierzu werden Prüfsummen verwendet und Empfangsbestätigungen ausgetauscht. Auch diese Prüfverfahren können jedoch manipuliert werden.[84] Dies kann dafür genutzt werden, um den Server des Empfängers lahmzulegen, die Verbindung zu übernehmen oder um schadhafte Daten beim Empfänger einzuschleusen. Um diese Schwachstellen zu beseitigen, wurde Transport Layer Security (TLS) – auch bekannt unter dem Namen des Vorgängers Secure Sockets Layer (SSL) – entwickelt. Das technisch komplexe TSL unterstützt verschiedene kryptographische Methoden, die die Privatheit und Integrität der Kommunikation zwischen Sender und Empfänger sichern sollen.[85] Gemeinsam mit

[79] Dazu bereits *M. Mueller*, Ruling the Root, 2002, S. 134 ff.

[80] Siehe *ICANN*, Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends, 1.10.2016; *K. Raustiala*, Governing The Internet, AJIL 110 (2017), S. 491 ff.

[81] Dokumentiert unter: https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions#IETF_standards.

[82] Vgl. ErwGr 84, 100, 109 f. NIS 2-RL. Dazu weiter unten § 6 II. 7.

[83] Das TCP Protocol setzt sich aus zahlreichen RFC zusammen, vgl. die Übersicht unter https://en.wikipedia.org/wiki/Transmission_Control_Protocol#RFC.

[84] Ausführlich dazu *Center for the Protection of National Infrastructure*, Security Assessment of the TCP, 2009.

[85] Detailliert *Sohr/Kemmerich*, Technische Grundlagen der Informationssicherheit, in: Kipker (Hrsg.), 2020, Kap. 2 Rn. 84 ff.

dem Protokoll HTTPS[86] wird TLS unter anderem dazu verwendet, sensible Kommunikationen wie Bankgeschäfte über das Internet abzuwickeln. Auch bei diesen, eigentlich zur Verbesserung der Sicherheit eingeführten Protokollen wurden jedoch mehrfach große Sicherheitslücken entdeckt; bekannt geworden ist insbesondere der sog. „Heartbleed"-Programmfehler, der verschlüsselte Kommunikation über Online-Dienste kompromittiert hat.[87]

(4) Border Gateway Protocol (BGP)[88]: Das BGP reagiert auf das Problem, wie Kommunikation, die die Grenzen eines unter einheitlicher Verwaltung stehenden Netzwerks bzw. Autonomen Systems (AS)[89] überschreitet, vom Sender zum Empfänger gelangt. Im Internet existiert keine zentrale Stelle, die die aktuelle Topologie des ganzen Internets kennt und die auf dieser Grundlage darüber entscheiden kann, welchen Weg ein Datenpaket nehmen soll. Stattdessen greift das BGP, das regelt, wie einzelne Router Entscheidungen über die Weiterleitung von Datenpaketen zwischen AS treffen. Grundlage dieser Entscheidungen sind Informationen, die das AS über seine jeweiligen Nachbarn gesammelt hat. Die Kenntnis von der Topologie seiner Netzwerkumgebung wird dem AS nicht (nur) manuell einprogrammiert. Vielmehr automatisiert das BGP den Informationsaustausch zwischen den Routern verschiedener AS: So sendet jedes AS periodisch Informationen über bestimmte ihm bekannte Verbindungsrouten, insbesondere zu den von ihm verwalteten IP-Adressen, an die BGP-Router anderer AS, die diese Informationen wiederum verarbeiten und ihre eigenen Routingtabellen entsprechend ergänzen bzw. anpassen. Das BGP initiiert und institutionalisiert damit gewissermaßen ein permanentes kollaboratives Entdeckungsverfahren. Hat ein AS auf diese Weise mögliche Routen bestimmt, stellt sich das Problem, welche Route gewählt wird. In der Praxis machen Netzbetreiber die Routing-Entscheidung vorwiegend von strategischen und ökonomischen Kriterien abhängig (Policy-basiertes Routing). – Wie das DNS beruht das BGP im Kern auf Vertrauen.[90] Denn es setzt darauf, dass die übermittelten Daten richtig sind, ohne dass dafür im Protokoll selbst Garantien oder Prüfverfahren vorgesehen sind. Wird ein BGP-Router gehackt, nimmt ein Betreiber bewusst Fehleinstellungen vor oder liegt ein unbeabsichtigter Fehler vor (Routing Leak; BGP Highjacking), sendet der Router falsche Informationen. Entsprechende Fehler haben bereits mehrfach zu massiven Ausfällen von Teilen des Internets geführt.[91] Trotz aller dieser mittlerweile weithin bekannten Schwächen von BGP konnte sich auf-

[86] Dokumentiert unter: https://datatracker.ietf.org/doc/html/rfc2818.

[87] *BSI*, Die Lage der IT-Sicherheit in Deutschland 2014, 2014, S. 32 f.

[88] Vgl. oben § 6 Fn. 72.

[89] Zum Begriff siehe oben § 6 Fn. 64. Da der Betreiber eines AS sein ganzes Netzwerk überblicken kann, stellt das (interne) Routing für ihn kein Problem dar. Hingegen fehlt ihm die Kenntnis der Topographie außerhalb seines AS.

[90] Instruktiv hierzu *O. Lystrup*, BGP and the System of Trust that Runs the Internet Pt. 1, 21.9.2021.

[91] Durch entsprechende Anordnungen gegenüber den Betreibern von BGP-Routern können staatliche Stellen landesintern effektiv das Internet „abschalten". Ägypten hat dies 2011 demonstriert. Dazu aus völkerrechtlicher Sicht *M. Kettemann*, Das Internet als internationales Schutzgut, ZaöRV 72 (2012), S. 469 ff. Soweit in Rechtsvorschriften für bestimmte Gefahrenlagen eine Unterbrechung oder Verhinderung der Telekommunikation vorgesehen ist, müsste dies – soweit das Internet davon erfasst sein soll – auf diesem Wege operieren, vgl. etwa § 34d Abs. 1 PAG Thüringen.

grund der komplexen technischen Anforderungen und der großen finanziellen Implikationen bisher keine Initiative zur Reform des Protokolls durchsetzen. Stattdessen hat sich eine private Sicherheitsindustrie entwickelt.

Zusammenfassend lässt sich an dieser Stelle festhalten, dass zahlreiche Internetprotokolle jedenfalls in ihrer ursprünglichen Fassung kaum Sicherheitsaspekte berücksichtigt haben. Mit der Entwicklung des Internets zu einem weltweiten offenen Netz wurde deutlich, dass hier erhebliche Anpassungen erforderlich sind. In diesem Sinne haben die zuständigen Stellen, insbesondere die IETF und die IEGS, Sicherheitsanalysen durchgeführt und die alten Protokolle teilweise aktualisiert und teilweise durch neue Protokolle ersetzt oder ergänzt. Bisher hat jedoch keine dieser Reformen für eine umfassende Verbesserung der Internetsicherheit sorgen können. Problematisch ist zudem, dass für die maßgeblichen Gremien gut dokumentiert ist, welchen Einfluss ökonomische und politische Interessen auf die dortige Standardisierungsarbeit nehmen.[92] Als globale, private Gremien können sich IETF und IEGS bisher den Zumutungen der etwa durch das Grundgesetz aufgegebenen „Normierung der Normung" effektiv entziehen.[93]

c) … von der Aufgabenbeschreibung zur rechtlichen Regulierung

Die analytische Unterscheidung der drei Schichten bzw. Teilaufgaben darf nicht darüber hinwegtäuschen, dass Angreifer regelmäßig Angriffsvektoren verwenden, die Schwachstellen unterschiedlicher Schichten ausnutzen. So wird beispielsweise mittels Social Engineering ein Nutzer veranlasst, eine unauffällige Malware auf dem eigenen IT-System zu installieren, etwa einen Keylogger, der die Tastaturanschläge protokolliert. Alternativ kann dieses Ergebnis auch über eine Drive-by-Infection infolge der Manipulation eines DNS-Servers erzielt werden. Diese Software bzw. die mit ihrer Hilfe gewonnenen Erkenntnisse werden vom Angreifer anschließend genutzt, um sich vollen Zugriff auf das Ziel-IT-System und dessen Netzwerk zu verschaffen; dort werden dann, unter Ausnutzung von Schwächen der Netzwerksicherheit, von Software-Vulnerabilitäten oder von Backdoors zusätzliche Schadprogramme

[92] Vgl. auch allgemein zum Einfluss von Unternehmen auf die Regulierung der Internet-Technologien *Mueller*, Ruling the Root, 2002; *L. DeNardis*, Protocol Politics, 2009; *M. Mueller*, Networks and States, 2010; L. DeNardis (Hrsg.), Opening Standards, 2011; E. Brousseau/M. Marzouki/C. Méadel (Hrsg.), Governance, Regulation and Powers on the Internet, 2012; *I. Brown/C. Marsden*, Regulating Code, 2013; *L. DeNardis*, The Global War for Internet Governance, 2014; *dies.*, The Internet Design Tension between Surveillance and Security, IEEEA 37:2 (2015), S. 72; *Kettemann*, The Normative Order of the Internet, 2020, S. 49 ff. Allerdings setzen technische Funktionalitäten politischen Gestaltbarkeitswünschen oft Grenzen, vgl. *R. Whitt*, A Deference to Protocol, Cardozo Arts & Entertainment Law Journal 31 (2013), S. 689 (695 f.).

[93] Siehe oben § 5 III. 2. b) aa).

nachgeladen. Mit deren Hilfe werden dann Handlungen vorgenommen, die die Verfügbarkeit, Integrität oder Vertraulichkeit der gespeicherten Daten beeinträchtigen, etwa durch eine Kopie der Daten, deren Löschung oder die Übernahme von Steuerungsfunktionen. Dies zieht wiederum sehr unterschiedliche Schadensarten nach sich, von bloß temporären Funktionsbeeinträchtigungen der betroffenen IT-Systeme und Netzwerke über permanente Schäden auf IT-Ebene (etwa durch gelöschte oder gestohlene Daten) bis hin zu mehr oder weniger umfassenden Schädigungen der IT-Systeme selbst oder ihrer Umwelt (Fehlsteuerung von autonomen Fahrzeugen, Ausfall von Krankenhäusern, Energieversorgern oder Nuklearanlagen etc.).

Bereits für solche Standardattacken reichen eindimensionale Sicherungsmechanismen somit nicht aus. Hinzu kommt, dass Angriffe auch die Vernetzung der Systeme untereinander ausnutzen können. Dementsprechend hat die Enquete-Kommission „Internet und digitale Gesellschaft" schon 2013 festgehalten, dass IT-Risiken „systemischer Natur [sind], das heißt isoliert betrachtet stellen sie kein Risiko dar, wohl aber im Zusammenwirken. Hat ein Angreifer es etwa geschafft, die Daten innerhalb eines Systems zu kompromittieren, verliert jeder Authentifizierungsmechanismus seinen Wert. Die bloße Absicherung nur eines Teilbereichs eines IT-Systems ist unzureichend, um den Schutz zu gewährleisten."[94] Aus dem gleichen Grund betreffen Risiken nie nur einzelne Sektoren.[95]

All dies spricht auch aus rechtlicher Sicht für einen umfassenden Regulierungsansatz, wie er im Technikrecht ohnehin empfohlen wird und wie er mit Blick auf die ihrerseits umfassende staatliche Schutzverantwortung auch verfassungsrechtlich geboten erscheint.[96] Dabei muss Regulierung nicht auf eine nie erreichbare vollständige Sicherheit zielen. Anliegen des technischen Sicherheitsrechts ist vielmehr, das Risiko von Rechtsgutsbeeinträchtigungen in akzeptablen Grenzen zu halten.[97] Doch auch hierfür muss das Risiko zunächst einmal in seiner ganzen Breite erfasst und dann auch regulatorisch adressiert werden.

Bei alldem sollte die rechtliche Regulierung keinen Kodifikationsanspruch erheben; ein solcher wäre angesichts der Vielschichtigkeit der Materie zum

---

[94] *Deutscher Bundestag*, Neunter Zwischenbericht der Enquete-Kommission „Internet und digitale Gesellschaft" – Zugang, Struktur und Sicherheit im Netz, 19.3.2013, BT Drs. 17/12541, S. 56. Entsprechend bereits *P. Sommer/I. Brown*, Reducing Systemic Cybersecurity Risk, 14.1.2011.

[95] Dazu weiter unter § 6 II. 5. Eine allein auf den Schutz von als „kritisch" eingestuften IT-Systemen fokussierte Regulierung ist daher insgesamt nicht risikoadäquat.

[96] Siehe oben § 5 II.

[97] *K. Vieweg*, Produkthaftungsrecht in: Schulte/Schröder (Hrsg.), Handbuch des Technikrechts, 2011, S. 337 (361): „Technische Sicherheit erweist sich damit immer als ein wertender Begriff auf einer gleitenden Skala technischer Möglichkeiten."

Scheitern verurteilt.[98] Die Pluralität und die Heterogenität des Informationssicherheitsrechts sind nicht nur Folge eines fehlenden Systemwillens der handelnden Stellen. Sie resultieren vielmehr auch aus der Schwierigkeit, auf eine technisch komplexe, globale und dynamische Problemlage vorhersehbare, lokale und – im Interesse der Rechtssicherheit zumindest zweitweise – statische Antworten in den Formen des Rechts finden zu müssen. Erschwerend kommt hinzu, dass Gefährdungen der Informationssicherheit ganz unterschiedliche Ursachen und Folgen haben. Schließlich sind die einzelnen Akteure im Informationssicherheitsfeld – man denke an einen Verbraucher einerseits und an den Betreiber einer kritischen Infrastruktur andererseits – schon unter Belastungsgesichtspunkten unterschiedlich zu behandeln. Eine wesentliche Vereinheitlichung oder Vereinfachung der Rechtslage ist aus diesen Gründen nicht zu erwarten.

Das geltende Recht enthält dementsprechend an zahlreichen unterschiedlichen Stellen Regelungen, die die verschiedenen Teilaufgaben und Regulierungsschichten teils übergreifend adressieren und die teils punktuell Vorgaben machen.[99] Zuletzt hat das nach einem komplizierten Gesetzgebungsverfahren[100] am 28.5.2021 in Kraft getretene IT-SiG 2.0[101] sich erstmals um eine Zusammenführung verschiedener Regelungsdimension im Sinne eines „Querschnittsgesetzes" für die IT-Sicherheit bemüht. Dennoch bleibt auch das IT-SiG 2.0 im Kern ein nationales und auch sektorales Regulierungsvorhaben zur Reform des nach wie vor auf den Systemschutz fokussierten BSIG. Allein durch einen Blick in das reformierte BSIG erschließen sich die Strukturen des Rechts der Informationssicherheit daher nicht. Gleiches gilt für die NIS-RL

[98] Zu Konzept und fortdauernder Relevanz der Kodifikationsidee mit unterschiedlichen Akzenten *W. Kahl*, Kodifizierung des Verwaltungsverfahrensrechts in Deutschland und in der EU, JuS 2018, S. 1025 ff. *O. Lepsius*, Gesetzesstruktur im Wandel (Teil 1), JuS 2019, S. 14 ff. Zur daran anschließenden Idee der Kodifikation eines Informationsgesetzbuches *M. Kloepfer*, Informationsgesetzbuch – Zukunftsvision?, K&R 1999, S. 241 ff.

[99] Vgl. dazu bereits die Bestandsaufnahme oben unter § 2 I.

[100] Zur Kritik am Verfahren siehe die Stellungnahme des Nationalen Normenkontrollrats, abgedruckt in: *Deutscher Bundestag*, Gesetzesentwurf der Bundesregierung zum IT-SiG 2.0, BT-Drs. 19/26106, S. 100 (Anlage 2). Zur Bewertung der Inhalte des Gesetzes vgl. die fast einhellige Kritik der Sachverständigen im Rahmen der Anhörung des Ausschusses für Inneres und Heimat am 1.3.2021, dokumentiert unter: https://www.bundestag.de/dokumente/textarchiv/2021/kw09-pa-innen-informationstechnik-821484. Siehe den Überblick bei *Hornung*, Das IT-Sicherheitsgesetz 2.0, NJW 2021, S. 1985 f.

[101] Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme v. 18.5.2021, BGBl. I S. 1122. Die Bezeichnung „IT-SiG 2.0", die der Referentenentwurf noch im Titel trug und die sich nach wie vor in der Begründung findet (BT-Drs. 19/26106, 2, 107; BT-Drs. 19/28844), hat sich eingebürgert, vgl. *Hornung*, Das IT-Sicherheitsgesetz 2.0, NJW 2021, S. 1985. Zum Gesetz ausführlich auch *M. Schallbruch*, Das IT-Sicherheitsgesetz 2.0 (Teil I), CR 2021, S. 450 ff.; *ders.*, Das IT-Sicherheitsgesetz 2.0 (Teil II), CR 2021, S. 516 ff.; sowie die Dokumentation und der Kommentar von Ritter (Hrsg.), Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2022.

bzw. die NIS 2-RL. Bemühungen zur Rekonstruktion der prägenden Strukturen des „Regimekomplexes“[102] müssen daher auch zahlreiche weitere einschlägige Rechtsetzungsakte auf verallgemeinerbare Charakteristika hin analysieren. Erste und wichtigste Gemeinsamkeit dieser Regelungen ist ihre Ausrichtung auf die eingangs beschriebenen Schutzziele der Informationssicherheit (vgl. § 2 Abs. 2 S. 4 BSIG bzw. Art. 4 Nr. 2 NIS-Richtlinie).

2. Territorialisierung des Informationssicherheitsproblems

a) Informationssicherheit als globales Problem

Als eine wichtige Ursache für die Schwierigkeit, die Informationssicherheitskrise regulatorisch in den Griff zu bekommen, gilt gemeinhin die territorial begrenzte Gestaltungmacht der Nationalstaaten und supranationalen Organisationen sowie der Ausfall der koordinierenden Instanzen des Völkerrechts.[103] Denn die umfassende Vernetzung informationstechnischer Systeme über das Internet führt dazu, dass sich Informationssicherheitsrisiken durch ein territorial begrenztes Vorgehen nicht umfassend einhegen lassen. Dies legt eine globale Lösung nahe. Insoweit zeigt die jüngste Einigung der Mitgliedstaaten der Vereinten Nationen auf Leitlinien zum Umgang mit dem Cybersicherheitsproblem zwar, dass ein internationaler Konsens nicht gänzlich außer Reichweite ist.[104] Dieser zielt jedoch bisher nur auf den kleinsten gemeinsamen Nenner, lässt also keine umfassende Lösung erwarten. Rechtsordnungen müssen daher nach wie vor unterhalb der Ebene des Völkerrechts nach Wegen suchen, um auf das globale Informationssicherheitsproblem Einfluss zu nehmen.[105]

Entterritorialisierung ist kein Problem, das nur das Informationssicherheitsrecht betrifft. Angesichts zunehmend vernetzter und auf globalen Liefer-

---

[102] Siehe oben § 6 Fn. 12.

[103] Siehe spezifisch *Kettemann*, The Normative Order of the Internet, 2020, S. 64.

[104] Siehe oben § 4 Fn. 139.

[105] Von diesen rechtlichen Strategien zu unterscheiden sind die faktischen Anreize, die Rechtsordnungen auf Akteure in Drittstaaten ausüben. Hierzu und zu dem auf Drittstaaten wirkenden Druck, die eigenen Regulierungsstandards anzupassen, grundlegend *A. Bradford*, The Brussels Effect, Nw. U. L. Rev. 107 (2012), S. 1 ff.; jetzt nochmals monographisch *dies.*, The Brussels Effect, 2020. Skeptisch zur empirischen Basis dieser These *A. Young*, The European Union as a global regulator?, Journal of European Public Policy 22 (2015), S. 1233 ff.; vgl. auch *J. Frankenreiter*, The Missing “California Effect” in Data Privacy Law, 2021. Kritisch zu den mit dem „Brussels effect“ verbundenen normativen Ansprüchen auf eine globale Ausstrahlung des Unionsrechts *R. Vatanparast*, Designed to Serve Mankind?, ZaöRV 80 (2020), S. 819 ff.; *S. Mercer*, The Limitations of European Data Protection as a Model for Global Privacy Regulation, 114 (2020), S. 20 ff. Nuanciert die Darstellung des Einflusses des Unionsrechts im Bereich des Datenschutzes bei *P. Schwartz*, Global Data Privacy Law, N.Y.U. L. Rev. 94 (2018), S. 771 ff. Allgemein bereits *A. Peters*, Wettbewerb von Rechtsordnungen, in: VVDStRL 69 (2010), S. 7 ff.

ketten basierender Techniksysteme ist Entterritorialisierung vielmehr für weite Bereiche des Technikrechts, aber auch für zahlreiche sonstige Rechtsmaterien eine drängende Herausforderung. Während Menschen, Güter und Daten immer mobiler werden, büßt das Territorium, der physische Raum, immer mehr an Bedeutung ein.[106] Das relativiert den Zusammenhang von Herstellung und Durchsetzung letztverbindlicher Entscheidungen, der im territorialen Herrschaftsverband vergleichsweise einfach möglich ist und der allgemein als Bedingung für die Verrechtlichung von Konflikten und damit als Garant für eine der zentralen gesellschaftlichen Leistungen des Rechts gilt.

Die Lockerung dieses Zusammenhangs darf allerdings nicht mit dem Wegfall von Regulierung bzw. einem Ende rechtlicher Regulierbarkeit verwechselt werden. Auch der zeitweise als unregulierbar[107] apostrophierte „Cyber-Raum“[108] basiert, wie schon früh gezeigt wurde, auf technischen Infrastruktu-

[106] Allgemein zur Relevanz des „Raumes“ für politische und rechtliche Gemeinschaften nur *K. Economides/M. Blacksell/C. Watkins*, The Spatial Analysis of Legal Systems, Journal of Law and Society 13 (1986), S. 161 ff.; *G. Winkler*, Raum und Recht, 1999; *N. Blomley/D. Delaney/R. Ford*, The Legal Geographies Reader, 2001; *U. Di Fabio*, Der Verfassungsstaat in der Weltgesellschaft, 2001, S. 52; H. Dreier/H. Forkel/K. Laubenthal (Hrsg.), Raum und Recht, 2002; *B. Kempen*, Staat und Raum, 2014; K. Odendahl/T. Giegerich (Hrsg.), Räume im Völker- und Europarecht, 2014. Noch allgemeiner zum juristischen Raum-Begriff: *S. Müller-Mall*, Legal Spaces, 2013; *A. Siehr*, Das Recht am Öffentlichen Raum, 2017. Aus der ebenfalls kaum mehr überschaubaren Literatur zur Herausforderung des Rechts als Ordnungsfaktor durch die Globalisierung vgl. nur die grundlegenden Beiträge von *M. Ruffert*, Die Globalisierung als Herausforderung an das Öffentliche Recht, 2004; *R. Poscher*, Globalisierung, in: VVDStRL 67 (2008), S. 163 ff.; G. Handl/J. Zekoll/P. Zumbansen (Hrsg.), Beyond Territoriality, 2012; *H. Lindahl*, Fault Lines of Globalization, 2013; *Viellechner*, Transnationalisierung des Rechts, 2013; sowie den hilfreichen Überblick über die internationale Debatte bei *N. Walker*, Intimations of Global Law, 2015. Siehe auch *J. Bast*, Völker- und unionsrechtliche Anstöße zur Entterritorialisierung des Rechts, in: VVDStRL 76 (2017), S. 277 ff.; *K. Schmalenbach*, Völker- und unionsrechtliche Anstöße zur Entterritorialisierung des Rechts, in: VVDStRL 76 (2017), S. 245 ff.; *A. Kahl*, Entterritorialisierung im Wirtschaftsrecht und im Kommunikationsrecht, in: VVDStRL 76 (2017), S. 343 ff.; *M. Cornils*, Entterritorialisierung im Wirtschaftsrecht und im Kommunikationsrecht, in: VVDStRL 76 (2017), S. 390 ff. Die Debatte um das Recht unter den Bedingungen der Globalisierung gewinnt ihre Komplexität auch dadurch, dass sich hier Fragen nach dem Souveränitätsbegriff und den Grundlagen der internationalen Kooperation mit Themen von Zugehörigkeit und Bürgerschaft sowie der Verantwortungsteilung zwischen hoheitlichen Stellen und transnational agierenden privaten Akteuren mischen. Zu letzteren siehe bereits oben § 2 Fn. 73.

[107] Locus classicus: *J. Barlow*, A Declaration of the Independence of Cyberspace, 8.2.1996, gedruckt: *ders.*, A Declaration of the Independence of Cyberspace, in: Ludlow (Hrsg.), Crypto Anarchy, Cyberstates, And Pirate Utopias. Part II, 2001, S. 27 ff.

[108] Vielzitiert hierzu: *L. Lessig*, The Zones of Cyberspace, Stan. L. Rev. 48 (1996), S. 1403 ff. („Cyberspace is a place. People live there.“); entsprechend *ders.*, Code: Version 2.0, 2006, S. 298, 391. Einflussreich weiter: *I. Trotter Hardy*, The Proper Legal Regime for "Cyberspace", U. Pitt. L. Rev. 55 (1994), S. 993 (994 f.); *D. Post*, Governing Cyberspace, Wayne L. Rev. 43 (1996), S. 155 ff.; *D. Johnson/D. Post*, Law and Borders, Stan. L. Rev. 48 (1996), S. 1367 ff.; *F. Mayer*, Recht und Cyberspace, NJW 1996, S. 1782 ff.; *ders.*, Völkerrecht

ren, deren geographische Standorte regelmäßig eindeutig identifiziert werden können.[109] Der Streit um das „Ob" der rechtlichen Regulierbarkeit des Cyber-Raums war daher in der Sache oft eine Auseinandersetzung um die Art und Weise der Regulierung.[110] Die geographische Frage blieb und bleibt dennoch relevant, da sich regulierende Instanzen bei den im Internet typischerweise grenzüberschreitenden Sachverhalten regelmäßig mit den Beschränkungen der eigenen Vollstreckungsmacht, mit konkurrierenden Regelungsansprüchen fremder Hoheitsgebiete und mit den Grenzen der eigenen Jurisdiktionsmacht konfrontiert sehen.[111]

Bleibt dann, wie im Fall der Informationssicherheit, eine kompensatorische Verrechtlichung auf der Ebene des Völkerrechts fast gänzlich aus, stehen allerdings noch andere Strategien zur Verfügung. Drei dieser Strategien sollen hier näher betrachtet und auf ihre Passfähigkeit für das Recht der Informationssicherheit hin untersucht werden. Dabei ist zu berücksichtigen, dass sich nicht alle Schichten des Informationssicherheitsproblems in gleicher Weise für diese

---

und Cyberspace, in: Thiedeke (Hrsg.), Soziologie des Cyberspace, 2004, S. 491 ff. Umfassend *S. Hobe*, Cyberspace, in: Isensee/Kirchhof (Hrsg.), HStR, Bd. XI, 3. Aufl. 2013, § 231; und jetzt *Haake*, Technik – Recht – Raum, 2022.

[109] Frühzeitig *J. Goldsmith*, The Internet and the Abiding Significance of Territorial Sovereignty, Indiana Journal of Global Legal Studies 5 (1998), S. 475 ff.; weiter auch A. Thierer/C. Crews (Hrsg.), Who Rules the Net? Internet Governance and Jurisdiction, 2003; *J. Cohen*, Cyberspace As/And Space, Colum. L. Rev. 107 (2007), S. 210 ff.; *J. Goldsmith/T. Wu*, Who Controls the Internet?, 2008; *R. Ford*, Against Cyberspace, in: Sarat/Douglas/Umphry (Hrsg.), The Place of Law, 2009, S. 147 ff.; *Walter*, Cyber Security als Herausforderung für das Völkerrecht, JZ 70 (2015), S. 685 ff.

Das ursprünglich als Verteidigung gegen die unbedachte Übertragung normativer Ansprüche der alten, territorialen Ordnung auf den neuen Cyber-Raum erdachte Konzept des „Cyberspace" hatte einen unbeabsichtigten Nebeneffekt: So nutzten Vertreter eben dieser alten Ordnung, namentlich die U.S.-Gerichte, die Raum-Metapher, um unter Verweis auf die Dinglichkeit des Internets sachenrechtliche Regelungen auf Internet-Transaktionen anzuwenden. Vgl. *D. Burk*, Legal Consequences of the Cyberspatial Metaphor, in: Consalvo/Baym et al. (Hrsg.), Internet Research Annual, Bd. 1, 2003, S. 17 ff.; *M. Lemley*, Place and Cyberspace, Calif. L. Rev. 91 (2003), S. 521 ff.; *D. Hunter*, Cyberspace as Place, Calif. L. Rev. 91 (2003), S. 439 ff.; kritisch zur Stoßrichtung der Metaphern-Kritik etwa *D. McGowan*, The Trespass Trouble, J. L. Econ. & Pol'y 1 (2005), S. 109 ff.; zur komplexen Thematik weiter nur *V. Boehme-Neßler*, Das Ende des Staates?, ZÖR 64 (2009), S. 145 ff.; *M. Berberich*, Virtuelles Eigentum, 2010, S. 35 ff.

[110] So bereits *L. Lessig*, The Path of Cyberlaw, Yale L. J. 104 (1995), S. 1743 ff.; *T. Wu*, Cyberspace Sovereignty, Harv. J. L. & Tech. 10 (1997), S. 647 ff.; *J. Delacourt*, The International Impact of Internet Regulation, Harv. Int'l L. J. 38 (1997), S. 207 ff.

[111] Aus der uferlosen Literatur vgl. nur schlaglichtartig *M. Fagin*, Regulating Speech Across Borders, Mich. Telecomm. & Tech. L. Rev. 9 (2003), S. 395 ff.; W. Drake/E. Wilson (Hrsg.), Governing Global Electronic Networks, 2008; *B. Maier*, How Has the Law Attempted to Tackle the Borderless Nature of the Internet?, Int'l J. L. & Info. Tech. 18 (2010), S. 142 ff.; *T. Wu*, The Master Switch, 2011; *O. Pollicino/M. Bassini*, The law of the Internet, in: Maduro/Tuori/Sankari (Hrsg.), Transnational Law, 2014, S. 346 ff.; *M. Hathaway*, Connected Choices, American Foreign Policy Interests 36 (2014), S. 300 ff.; *Z. Clopton*, Territoriality, Technology, and National Security, U. Chi L. Rev. 83 (2016), S. 45 ff.

Strategien, die im Kern je auf eine Territorialisierung des Informationssicherheitsproblems hinarbeiten, eignen. Das gilt insbesondere für die internetspezifischen Sicherheitsrisiken, namentlich die Schwächen der grundlegenden Internet-Protokolle. Für eine effektive Regulierung führt hier an einer Befassung der maßgeblichen transnationalen Akteure, insbesondere am IETF, kein Weg vorbei; diese müssen im Wege privater Regelsetzung den Normmangel kompensieren, den Nationalstaaten und internationale Organisation im Feld der (völker-)rechtlichen Regulierung der Internetsicherheit lassen.[112]

b) Expansive Jurisdiktionsregeln

An anderer Stelle kann sich Informationssicherheitsregulierung jedoch durch geschickte Wahl des Anknüpfungsortes Zugriff auf prima facie globale Prozesse und Strukturen verschaffen.[113] Ein für das Informationssicherheitsrecht hochrelevantes Beispiel hierfür ist Art. 3 Abs. 2 DSGVO, der unter bestimmten Bedingungen auch verantwortliche System- und Netzwerkbetreiber, die nicht in der EU niedergelassen sind, dem Regime der DSGVO unterwirft.[114] Dieses sogenannte Marktortprinzip[115] gilt auch für die vom Verarbeiter zu ergreifenden technischen und organisatorischen Maßnahmen zur Datensicherheit gemäß Art. 32 DSGVO. Diese für das Informationssicherheitsrecht zentrale Norm,[116] die vor allem die Schicht der System- und Netzwerksicherheit reguliert, erzeugt somit bereits heute faktisch eine globale Rechtswirkung.

Eine entsprechende allgemeine Regelung findet sich für KRITIS-Betreiber – bzw. in der Terminologie der NIS 2-RL für Anbieter „wesentlicher und wichtiger Dienste" – nicht; soweit sich diese Dienste durch ihre Infrastrukturqualität definieren, sind Jurisdiktionsprobleme in der Praxis hier nicht so drängend wie im Datenschutzrecht, werden die entsprechenden Dienste doch

[112] Dazu oben § 2 Fn. 73; § 6 Fn. 75 und 106.

[113] Dazu aus der öffentlich-rechtlichen Literatur allgemein *K. Vogel*, Der räumliche Anwendungsbereich der Verwaltungsrechtsnorm, 1965; *E. Reimer*, Der Ort des Unterlassens, 2004; *C. Ohler*, Die Kollisionsordnung des Allgemeinen Verwaltungsrechts, 2005, S. 327 ff.; *M. Kment*, Grenzüberschreitendes Verwaltungshandeln, 2010, S. 104 ff.; *J. Menzel*, Internationales Öffentliches Recht, 2011, S. 325 ff.

[114] Zur territorialen Reichweite des EU-Datenschutzrechts siehe nur *C. Kuner*, Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law, International Data Privacy Law 5:4 (2015), S. 235 ff.; *J. Hörnle*, Juggling More Than Three Balls at Once, Int'l J. L. & Info. Tech. 27:2 (2019), S. 142 ff.; *S. Koloßa*, The GDPR's Extra-Territorial Scope, ZaöRV 80 (2020), S. 791 ff. Allgemein zur Nutzung entsprechender Strategien im Unionsrecht *J. Scott*, Extraterritoriality and Territorial Extension in EU Law, Am. J. Comp. L. 62 (2014), S. 87 ff.; sowie die Beiträge in M. Cremona/J. Scott (Hrsg.), EU Law Beyond EU Borders, 2018.

[115] Genau genommen handelt es sich um eine „Mischung aus subjektivem Territorialitäts-, Marktort- und Ausrichtungsprinzip", vgl. *J. Oster*, Internationale Zuständigkeit und anwendbares Recht im Datenschutz, ZEuP 2021, S. 275 (284 f.).

[116] Dazu näher sogleich unter § 6 II. 5.

regelmäßig „vor Ort" angeboten (Energieversorgung, Wasserversorgung etc.). Zusätzlich kann dies durch Registrierungspflichten abgesichert werden.[117] Mit der sachlich sinnvollen Ausweitung des Rechts kritischer Infrastrukturen auf die Aspekte System- und Komponentensicherheit durch die NIS-RL und das NIS-RL-Umsetzungsgesetz[118] von 2017 begann sich dies jedoch zu ändern: Will das BSI zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des IT-Systems eines KRITIS-Betreibers gemäß § 5b Abs. 6 BSIG vom Hersteller des kompromittierten informationstechnischen Systems verlangen, an der Wiederherstellung der Sicherheit oder Funktionsfähigkeit mitzuwirken, stellt sich die Frage, wie diese Anordnung umgesetzt werden soll, wenn dieser Hersteller – wie im Fall von Hard- und Software-Produkten wohl regelmäßig der Fall sein dürfte – nicht in Deutschland ansässig ist.[119] Hier fehlt es bislang an den behördlichen Zugriff erleichternden Vorgaben – und dementsprechend auch an praktischen Beispielen.[120] Die für einzelne sicherheitskritische Komponenten im Telekommunikationssektor vorgesehenen (und in ihrer Effektivität umstrittenen) Regelungen in §§ 2 Abs. 13, 9b BSIG, § 165 Abs. 4 TKG können schon aufgrund ihrer restriktiven Fassung kaum als Vorbild für eine umfassende Regulierung der Hersteller von Software und Hardware dienen.

Weiter sind hingegen bereits die der System- und Netzwerksicherheit bzw. auch der Internetsicherheit zuzurechnenden Regelungen für die erstmals durch die NIS-Richtlinie erfassten Anbieter „digitaler Dienste" (Online-Marktplätze, Online-Suchmaschinen oder Cloud-Computing-Dienste). Sofern diese nicht in der Union niedergelassen sind, aber Dienste innerhalb der Union bereitstellen, müssen sie gemäß Art. 18 Abs. 2 NIS-RL einen in einem Mitgliedstaat der Union niedergelassenen Vertreter benennen (vgl. entsprechend Art. 27 DSGVO). Diesen Weg setzt nun Art. 26 Abs. 3 NIS 2-RL fort und erweitert ihn u. a. auf DNS Service Provider, sog. Top Level Domain (TLD)-Registrare und die Anbieter von DNS-Registrierungsdiensten. Diese im Lichte der komplizierten Jurisdiktionsregelungen des traditionellen IPR und des IZPR durchaus „hemdsärmelig" wirkenden Bestimmungen[121] sind für

[117] Vgl. § 8b Abs. 3 i. V. m. § 14 Abs. 2 Nr. 5 BSIG. Entsprechend für Unternehmen im besonderen öffentlichen Interesse im Sinne des § 2 Abs. 14 S. 1 Nr. 1 und 2 BSIG (nicht: Nr. 3!): § 8f Abs. 5 S. 1 i. V. m. § 14 Abs. 2 Nr. 5 BSIG.

[118] Dazu und zum Folgenden weiter § 6 II. 4. b).

[119] Vgl. *Ritter*, in: ders. (Hrsg.), Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2022, Teil 1 Rn. 67.

[120] *Keppeler*, in: Ritter (Hrsg.), Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2022, § 5b BSIG Rn. 266.

[121] Zu den dogmatischen Schwierigkeiten, die sich aus dem Nebeneinander der territorialen Zuständigkeitsregelungen der DSGVO und weiterer Kollisionsregime ergeben, ausführlich *Oster*, Internationale Zuständigkeit und anwendbares Recht im Datenschutz, ZEuP 2021, S. 275 ff.; *J. Lüttringhaus*, Das internationale Datenprivatrecht, ZVglRWiss 117 (2018), S. 50 ff.; *M. Thon*, Transnationaler Datenschutz: Das Internationale Datenprivatrecht der DS-GVO, RabelsZ 84 (2020), S. 24 ff.

die jüngere Digitalgesetzgebung der Union nicht untypisch.[122] Weder völkernoch unionsrechtlich begegnet die Praxis durchgreifenden Bedenken, solange und soweit die Regulierung der extraterritorialen Handlungen dem Rechtsgüterschutz innerhalb des Territoriums der Union dient.[123] Eben dies ist bei IT-Sicherheitsfragen regelmäßig der Fall. Auch wenn es einen erheblichen regulatorischen Kraftakt bedeuten würde, sollte ein entsprechender Ansatz für den Bereich der Komponentensicherheit in Erwägung gezogen werden.

c) Koordination und Kooperation

Ganz anders setzt die zweite Strategie an. Diese zielt nicht auf eine Ausdehnung der Regelungsmacht über die Grenzen des eigenen Territoriums hinaus. Stattdessen soll das Fehlen übergeordneter Rechtsetzungs- oder Rechtsdurchsetzungsinstanzen auf dem Verwaltungswege durch ein koordiniertes Zusammenwirken lokaler Behörden in regionalen oder globalen Netzwerken kompensiert werden. Innerhalb der Europäischen Union ist ein derartiges Vorgehen bereits in zahlreichen Feldern an der Tagesordnung.[124]

---

[122] Vgl. die Verordnung über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste – DSA), deren Art. 2 Abs. 1 die Vorgaben des DSA für alle Vermittlungsdienste (Intermediäre) für anwendbar erklärt, „die für Nutzer mit Niederlassungsort oder Sitz in der Union angeboten werden, ungeachtet des Niederlassungsorts des Anbieters dieser Vermittlungsdienste". Gemäß Art. 3 lit. d und e DSA kann von einem solchen „Anbieten" ausgegangen werden, wenn der Anbieter eine „wesentliche Verbindung zur Union" hat, was der Fall ist, wenn er seine Niederlassung innerhalb der EU hat oder sofern er eine erhebliche Zahl von Nutzern in einem oder mehreren Mitgliedstaaten im Verhältnis zu dessen bzw. deren Bevölkerung hat oder wenn seine Tätigkeiten auf Nutzer in der EU ausgerichtet sind. Siehe auch allgemein *C. Kuner*, The Internet and the Global Reach of EU Law, in: Cremona/Scott (Hrsg.), EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law, 2018, S. 112 ff.

[123] Hierzu instruktiv *H. Krämer*, Extraterritoriale Wirkungen des Unionsrechts, EuR 2021, S. 137 ff. Zur primärrechtlichen Gestattung (und zu den Limitationen) extraterritorialen Unionsrechts EuGH, C-18/18 v. 3.10.2019, Rn. 48 ff. – Glawischnig-Piesczek (dazu instruktiv *G. Spindler*, Weltweite Löschungspflichten bei Persönlichkeitsrechtsverletzungen im Internet, NJW 2019, S. 3274 [3276 f.]); EuGH, C-507/17 v. 24.9.2019, Rn. 58, 61 – Google LLC. Siehe auch *C. Ryngaert/M. Taylor*, The GDPR as Global Data Protection Regulation?, AJIL Unbound 114 (2020), S. 5 ff. Allgemein zu den völkerrechtlichen Anforderungen siehe *H. Buxbaum*, Territory, Territoriality, and the Resolution of Jurisdictional Conflict, Am. J. Comp. L. 57 (2009), S. 631 ff.; *Walter*, Cyber Security als Herausforderung für das Völkerrecht, JZ 70 (2015), S. 685 (691) m. w. N.; *C. Ryngaert*, Jurisdiction in International Law, 2. Aufl. 2015, S. 189 ff.; *J. Crawford*, Brownlie's Principles of Public International Law, 9. Aufl. 2019, S. 440 ff.

[124] Zum Netzwerk-Konzept im europäischen Verwaltungsrecht aus der unüberschaubaren Literatur siehe nur *U. Mager*, Die europäische Verwaltung zwischen Hierarchie und Netzwerk, in: Trute/Groß et al. (Hrsg.), Allgemeines Verwaltungsrecht, 2008, S. 369 ff.; *W. Kahl*, Europäische Behördenkooperationen, in: Holoubek (Hrsg.), Verfahren der Zusammenarbeit, 2012, S. 15 ff.; *M. Kment*, Der Europäische Verbund für territoriale Zusammenarbeit, DV 45 (2012), S. 155 ff.; *Gärditz*, Der digitalisierte Raum des Netzes als emergente

Auch im Recht der Informationssicherheit finden sich entsprechende Strukturen. Dies gilt in erster Linie für die durch die NIS-RL etablierten europäischen Informationsnetzwerke. So hat die NIS-RL eine „Kooperationsgruppe" aus Vertretern der Mitgliedstaaten, der Kommission und ENISA begründet (Art. 11 NIS-RL) und weitreichende Informations- und Koordinierungspflichten bei grenzüberschreitenden IT-Sicherheitszwischenfällen angeordnet.[125] Durch die NIS 2-RL wird dies Netzwerk weiter ausgebaut (Art. 14 NIS 2-RL) und durch das – seit 2020 bereits auf informeller Basis tätige – Krisenbewältigungsinstrument Cyber Crisis Liaison Organisation Network (EU CyCLONe) ergänzt (Art. 16 NIS 2-RL).[126] Zu erwähnen sind in diesem Zusammenhang auch das durch die Verordnung (EU) 2021/887 etablierte Netzwerk nationaler Koordinierungszentren und das unter der Schirmherrschaft von ENISA stehende Vollzugsnetzwerk aus nationalen CSIRTs und CERT-EU (vgl. Art. 15 NIS 2-RL).[127] Das CSIRT-Netzwerk und die komplexen, das Zertifizierungswesen tragenden Organisationsstrukturen zeigen, dass derartige Netzwerke auch weit in den gesellschaftlichen Bereich hineinragen können. Im Bereich des IT-Strafrechts existiert mit EUROJUST zudem eine für den justiziellen Bereich wichtige Koordinierungsstelle (vgl. Art. 85 AEUV).

Ein hohes Maß an Verbindlichkeit können solche Kooperationen jedoch nur dort erreichen, wo ein entsprechender rechtlicher Integrationsrahmen existiert. Außerhalb des Unionsrechts fehlt ein derartiger Rahmen bislang für die Informationssicherheitsregulierung weitgehend. Die Zusammenarbeit muss sich hier der tradierten Formen der internationalen Rechtshilfe bedienen. Kurzfristige Abhilfe ist angesichts des fehlenden politischen Willens nicht in Sicht. Art. 7 NIS 2-RL hält die Union jetzt allerdings dazu an, im Rahmen des Art. 218 AEUV entsprechende Verträge abzuschließen.[128]

Ordnung, Der Staat 54 (2015), S. 113 (114); *Simantiras*, Netzwerke im Europäischen Verwaltungsverbund, 2016, S. 19 ff.; *E. Westermann*, Legitimation im europäischen Regulierungsverbund, 2017, S. 25 ff.; *M. Schwind*, Netzwerke im Europäischen Verwaltungsrecht, 2017; *C. Kibler*, Datenschutzaufsicht im europäischen Verbund, 2021, S. 287 ff. Speziell zum Sicherheitsrecht *B. Schöndorf-Haubold*, Netzwerke in der deutschen und europäischen Sicherheitsarchitektur, in: Boysen/Bühring et al. (Hrsg.), Netzwerke, 2007, S. 149 ff. Zu internationalen Verwaltungskooperationen siehe C. Möllers/A. Voßkuhle/C. Walter (Hrsg.), Internationales Verwaltungsrecht, 2007; *M. Glaser*, Internationale Verwaltungsbeziehungen, 2010; *Kment*, Grenzüberschreitendes Verwaltungshandeln, 2010, S. 300 ff.; *Knauff*, Der Regelungsverbund, 2010.

[125] Dazu *Wischmeyer*, Informationssicherheitsrecht, DV 50 (2017), S. 155 (173 ff.).

[126] Hierzu und zu weiteren Kooperationsformaten § 6 II. 3. b) und c).

[127] Hierzu § 6 II. 6 b).

[128] Auch ErwGr 54 CSA fordert ENISA zu stärkerem Engagement in diese Richtung auf: „Cyberbedrohungen bestehen weltweit. Um die Cybersicherheitsstandards, einschließlich

d) Lokalisierungspflichten

Die dritte Strategie versucht, globale Probleme, für die eine Lösung auf globaler Ebene nicht in Sicht ist, zu „lokalisieren". Dies ist nicht unter allen Umständen möglich und kann zudem erhebliche Folgekosten nach sich ziehen.[129] Im Bereich des Datenschutzes kann die Schrems II-Entscheidung des EuGH als Schritt in diese Richtung verstanden werden, reagiert sie doch auf den fehlenden internationalen bzw. transatlantischen Konsens über das richtige Maß an Privatheitsschutz mit einer de facto-Datenlokalisierungspflicht.[130]

Diese Judikatur zielt primär auf den Schutz personenbezogener Daten vor unrechtmäßiger Verarbeitung. Sie hat jedoch über den bereits erwähnten Art. 32 DSGVO auch Folgewirkungen für die Durchsetzung der Vorgaben zur Informationssicherheit; indem sie materiell-rechtlich zu einer Verarbeitung der Daten auf dem Territorium der Union zwingt, wird der territoriale Rechtsdurchsetzungszusammenhang auch im Punkt Informationssicherheit geschützt. Die NIS 2-RL enthält nun für den Bereich der Internetsicherheit Ansätze, die ebenfalls in diese Richtung weisen, wenn die lokal ansässigen Anbieter von wichtigen Internet-Infrastrukturdiensten, insbesondere Anbieter von DNS-Dienstleitungen und sog. TLD-Registrare, in das Regulierungsregime einbezogen werden (vgl. Annex I Nr. 8 NIS 2-RL; vgl. bisher Annex II Nr. 7 NIS-RL); flankiert wird dies durch die bereits erwähnte breite Jurisdiktionsregelung des Art. 26 NIS 2-RL. Auf die mit diesem Ansatz verbundenen Risiken wird noch gesondert einzugehen sein.[131]

---

der Notwendigkeit der Festlegung gemeinsamer Verhaltensnormen und der Annahme von Verhaltenskodizes, der Verwendung internationaler Normen und des Informationsaustauschs zu verbessern sowie eine zügigere internationale Zusammenarbeit bei der Abwehr und einen weltweiten gemeinsamen Ansatz für Probleme der Netz- und Informationssicherheit zu fördern, bedarf es einer engeren internationalen Zusammenarbeit. In dieser Hinsicht sollte die ENISA ein stärkeres Engagement der Union und die Zusammenarbeit mit Drittländern und internationalen Organisationen unterstützen, indem sie den einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union gegebenenfalls die erforderlichen Sachkenntnisse und Analysen zur Verfügung stellt."

[129] Eine extreme Maßnahme zur „Lokalisierung" des Informationssicherheitsproblems wäre die Entkopplung der nationalen Autonomen Systeme vom globalen Netz. Dies ist bislang nur für totalitäre Staaten eine Option, vgl. § 6 Fn. 91.

[130] Zu diesem Effekt und den damit verbundenen normativen Kosten *A. Chander*, Is Data Localization a Solution for Schrems II?, Journal of International Economic Law 23:3 (2020), S. 771 ff.; *T. Christakis*, European Digital Sovereignty, 2020, S. 64 ff. Zu den aus unterschiedlichen Motiven verfolgten Bestrebungen, die globale Datenverkehrsfreiheit durch rechtliche oder faktische Datenlokalisierungspflichten abzulösen, um so staatliche bzw. supranationale Zugriffsmöglichkeiten zu stärken, siehe *Kettemann*, The Normative Order of the Internet, 2020, S. 165 f. Aufschlussreich auch *Glen*, Internet Governance: Territorializing Cyberspace?, Politics & Policy 42 (2014), S. 635 ff. Zur Thematik allgemein schließlich noch *J. Daskal*, The Un-Territoriality of Data, Yale L. J. 125 (2015), S. 326 ff.; *C. Kuner*, Data Nationalism and its Discontents, Emory L. J. 64 (2015), S. 2089 ff.

[131] Siehe § 6 II. 7.

e) Zwischenfazit

Von einer Ohnmacht des Staates angesichts der Globalisierung kann nach alldem nicht die Rede sein. Vielmehr existieren verschiedene Praktiken, derer sich Rechtsordnungen bedienen können, um über die eigene territoriale Begrenzung hinaus Einfluss auf die globale Informationssicherheitslage zu nehmen. Diese werden in Teilbereichen des Informationssicherheitsrechts bereits aktiv vom Gesetzgeber genutzt. Entsprechende Strategien haben jedoch Kosten. So erhöht jeder (supra-)nationale Alleingang die Fragmentierung des globalen Technologierahmens.[132]

Dennoch sollten sich in Zukunft staatliche Stellen – jedenfalls in Ländern und Regionen mit hinreichenden politischen und wirtschaftlichen Ressourcen – bewusst machen, dass sie durchaus über eine (begrenzte) globale Regelungsmacht verfügen, die auf allen Schichten des Informationssicherheitsproblems, insbesondere auch im Bereich der Komponenten- und Internetsicherheit eingesetzt werden kann.[133] Allerdings bedarf es, um diese Optionen zu nutzen, hinreichender Expertise. Wie stets gilt, dass die Herausforderung der Globalisierung weniger in der Einschränkung als in der Überforderung der einzelstaatlichen Problemlösungskapazitäten besteht.[134]

3. Aufbau einer regulatorischen Kommunikations- und Wissensinfrastruktur

a) Informationssicherheit als Wissensproblem und als öffentliches Gut

Unabhängig davon, ob Regulierung Impulse für Innovationen setzen oder die Risiken der Informationstechnik einhegen will – entsprechende Maßnahmen verlangen Kenntnis der technischen Details und des sozialen Kontextes der rechtlichen Interventionen. In diesem Sinne stellt Informationssicherheit aus

[132] Zur technischen und rechtlichen Fragmentierung des Internets bzw. der Internetregulierung: *L. DeNardis*, One Internet, 2016; *W. Drake/V. Cerf/W. Kleinwächter*, Internet Fragmentation: An Overview, 2016; (entdramatisierend) *Mueller*, Will the Internet Fragment?, 2017; *Kettemann*, The Normative Order of the Internet, 2020, S. 166 ff. Zur unüberschaubaren und mittlerweile selbst schon historisierten „Fragmentierungsdebatte" im Völkerrecht s. nur diskursprägend *ILC*, Fragmentation of International Law, Report of the Study Group of the International Law Commission, 13.4.2006, A/CN.4/L.682, sowie aus der Literatur: *A. Fischer-Lescano/G. Teubner*, Fragmentierung des Weltrechts, in: Albert/Stichweh (Hrsg.), Weltstaat und Weltstaatlichkeit, 2007, S. 37 ff.; *C. Thiele*, Fragmentierung des Völkerrechts, AVR 46 (2008), S. 1 ff.; *K. Bautze*, Die Fragmentierungsdebatte, AVR 54 (2016), S. 91. Eine Rückschau bei *A. Peters*, The Refinement of International Law, I•CON 15 (2017), S. 671 ff.

[133] Allgemein hierzu *C. Brummer*, Territoriality as a Regulatory Technique, University of Cincinnati L. Rev. 79 (2011), S. 499 ff.

[134] Vgl. ähnlich *R. Mayntz*, Die Handlungsfähigkeit des Nationalstaats in Zeiten der Globalisierung, in: Heidbrink/Hirsch (Hrsg.), Staat ohne Verantwortung?, 2007, S. 267 (274).

regulatorischer Sicht auch und vielleicht sogar in erster Linie ein „Wissensproblem" dar – und ist als solches auch bereits analysiert worden.[135]

Allgemein ist der große Wissensbedarf des Rechts heute ein gut erforschtes Thema.[136] Nicht nur im Fall der Informationssicherheit hat es die Rechtsordnung mit Phänomenen zu tun, die neu und wandelbar sind, deren Verhalten schwer zu prognostizieren ist und deren Beeinträchtigung möglicherweise irreversible Folgen hat oder Kaskadeneffekte auslöst.[137] Das Problem des Regulierungswissens darf dabei nicht auf die Existenz von technischen Standards reduziert werden. Diese sind zwar erforderlich, damit die mit dem Erlass und der Durchsetzung des Rechts befassten staatlichen Stellen prüfen können, ob die regulatorischen Anforderungen beachtet wurden. Auch die Kontrolle, ob vertragliche Abreden eingehalten wurden, setzt entsprechende Standards voraus.[138] Die Ausarbeitung und Anwendung dieser Standards gelingt jedoch nur dort, wo eine Kommunikations- und Wissensinfrastruktur existiert, die die im System Technik organisierten Akteure und die Akteure des Rechtssystems zusammenführt und die langfristig den Aufbau belastbaren Regulierungswissens ermöglicht. Denn rechtliche Regulierung kann nicht nur auf eigenes Fachwissen setzen, sondern muss versuchen, in Austausch mit der gesellschaftlichen

[135] *H. Leisterer*, Internetsicherheit in Europa, 2018, S. 1 und passim; *Egloff/Dunn Cavelty*, Attribution and Knowledge Creation Assemblages in Cybersecurity Politics, Journal of Cybersecurity 7:1 (2021), S. 1 ff.; *Calliess/Baumgarten*, Cybersecurity in the EU, German L. J. 21 (2020), S. 1149 (1157). Siehe auch *S. Gaycken*, Cybersecurity in der Wissensgesellschaft, in: Daase/Engbert/Junk (Hrsg.), Verunsicherte Gesellschaft – Überforderter Staat, 2013, S. 109 ff.

[136] Aus der mittlerweile unüberschaubaren Literatur zum Themenfeld siehe insbes. C. Engel/J. Halfmann/M. Schulte (Hrsg.), Wissen – Nichtwissen – Unsicheres Wissen, 2002; I. Spiecker gen. Döhmann/P. Collin (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, 2008; A. Voßkuhle/G. F. Schuppert (Hrsg.), Governance von und durch Wissen, 2008; H. C. Röhl (Hrsg.), Wissen – Zur kognitiven Dimension des Rechts, 2010; *W. Hoffmann-Riem*, Regulierungswissen in der Regulierung, in: Bora/Henkel/Reinhard (Hrsg.), Wissensregulierung und Regulierungswissen, 2014, S. 135 ff.; Münkler (Hrsg.), Dimensionen des Wissens im Recht, 2019.

[137] Zu den spezifischen Wissensformen, die für den Umgang mit diesen Herausforderungen nötig sind, vgl. neben der soeben zitierten Literatur bereits ausführlich *K.-H. Ladeur*, Umweltrecht und technologische Innovation, UTR (1988), S. 305 (308 ff.); *R. Wolf*, „Herrschaft kraft Wissen" in der Risikogesellschaft, Soziale Welt 39 (1988), S. 164 (180 ff.); *Ladeur*, Das Umweltrecht der Wissensgesellschaft, 1995, S. 120 ff. Insbesondere das Technikrecht, das sich seit jeher intensiv um die Verkoppelung von rechtlichem und technischem Wissen bemüht hat, stellt hierzu einen Kanon etablierter Instrumente bereit, vgl. *M. Schulte*, Wissensgenerierung im Technikrecht, in: Spiecker gen. Döhmann/Collin (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, 2008, S. 259 ff.; *Schulze-Fielitz*, Technik und Umweltrecht, in: Schulte/Schröder (Hrsg.), Handbuch des Technikrechts, 2011, S. 455 (460 f.) m. w. N.

[138] Zur Bestimmbarkeit des Haftungsmaßstabs als Kernproblem der haftungsrechtlichen Betrachtungsweise aus Sicht des Informationssicherheitsrechts *M. Rafsendjanim/D. Bomhard*, IT-Sicherheit im Zivilrecht und in der Vertragsgestaltung, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 9 Rn. 30 f. Dazu gleich weiter in § 6 Fn. 143.

und technischen Wissensordnung zu gelangen.[139] Der Versuch einer regulatorischen Einhegung neuer und komplexer Risiken ist daher stets durch Maßnahmen zur Wissensgenerierung und -distribution zu flankieren.[140] Auf Seite der Privaten gilt es insoweit, Mechanismen zu etablieren, die sich der Problematik annehmen und dazu beitragen, entsprechendes Wissen zu erzeugen und technische Lösungen zu implementieren; dies kann in Gestalt von Forschungsförderung oder auch in der Setzung von Anreizen zur Etablierung privater Standardisierungsaktivitäten bestehen. Entsprechende private Aktivitäten sind dann mit der Verwaltung zu koppeln; dort bedarf es eigenständiger spezialisierter Organisationseinheiten sowie hinreichend leistungsfähiger administrativer Netzwerke, die das ihnen präsentierte Wissen weiterverarbeiten können.

Nationaler und europäischer Gesetzgeber haben diesen Themen in jüngerer Zeit einen großen Stellenwert eingeräumt. Auch wenn sich nach wie vor Lücken und Inkonsistenzen der Kommunikations- und Wissensinfrastruktur im Bereich Informationssicherheit identifizieren lassen, sind mittlerweile wesentliche wissensregulatorische Bausteine am Platz, die gleich im Detail betrachtet werden sollen.[141]

Dass der Staat überhaupt intervenierend tätig werden muss und den Aufbau einer solchen Wissensinfrastruktur nicht allein dem Markt überlassen kann, erklärt sich auch daraus, dass IT-Sicherheit aus ökonomischer Sicht Eigenschaften eines „öffentlichen Guts" aufweist.[142] So sind Marktteilnehmer von sich aus meist nicht in der Lage, die Qualität von Software zu überprüfen. Ohne zentrale Standards und Zertifizierungen lassen sich ferner keine hinreichend konkreten vertraglichen Abreden zur IT-Sicherheit treffen.[143] Dement-

[139] Dazu allgemein *A. Voßkuhle*, Rationaler Staat, in: ders./Schuppert (Hrsg.), Governance von und durch Wissen, 2008, S. 13 (18 f.), mit Verweis auf *A. Landwehr*, Diskurs – Macht – Wissen, Archiv für Kulturgeschichte 87 (2003), S. 71 ff.

[140] Vgl. aus der umfangreichen Literatur nur *Wollenschläger*, Wissensgenerierung im Verfahren, 2009, S. 29 ff.; *Augsberg*, Informationsverwaltungsrecht, 2014, S. 41 ff.; *M. Seckelmann*, Evaluation und Recht, 2018, S. 23 ff.

[141] Umfassend zum Folgenden auch *Leisterer*, Internetsicherheit in Europa, 2018.

[142] Zur ökonomischen Dimension siehe *R. Anderson*, Why Information Security is Hard, 2001; *L. Gordon/M. Loeb*, The Economics of Information Security Investment, ACM Transactions on Information and System Security 5 (2002), S. 438 ff.; M. Grady/F. Parisi (Hrsg.), The Law and Economics of Cybersecurity, 2005; *M. Gallaher/A. Link/B. Rowe*, Cyber Security, 2008; P. Shane/J. Hunker (Hrsg.), Cybersecurity, 2013; *S. Beissel*, Cybersecurity Investments, 2016. Siehe auch *N. Sales*, Regulating Cyber-Security, Nw. U. L. Rev. 107 (2013), S. 1503 (1527 f.) m. w. N.

[143] Aus der aktuellen Literatur zur Rolle des Vertragsrechts und dem Befund, dass nach wie vor in Verträgen über IT-Leistungen kaum je konkrete Abreden zur IT-Sicherheit getroffen werden, *G. Spindler*, IT-Sicherheitsgesetz und zivilrechtliche Haftung, CR 2016, S. 297 ff.; *K. Mehrbrey/M. Schreibauer*, Haftungsverhältnisse bei Cyber-Angriffen, MMR 2016, S. 75 ff.; *M. Gehrmann/P. Voigt*, IT-Sicherheit, CR 2017, S. 93 ff.; *Rafsendjanim/Bomhard*, IT-Sicherheit im Zivilrecht und in der Vertragsgestaltung, in: Hornung/Schallbruch

sprechend fehlt es oft an der Bereitschaft, entsprechende Aufschläge für sichere Software zu bezahlen. Ohne Meldepflichten für Zwischenfälle, die – wie gleich zu zeigen sein wird – ein wesentliches Element der Wissensinfrastruktur sind, besteht zudem kaum hinreichende Markttransparenz, die für jede realistische Risikokalkulation, auch auf Versicherungsseite, essenziell ist.[144] Staatliche Intervention ist daher notwendig, um den Prozess der privaten Wissensgenerierung zu effektuieren.

b) Forschungs- und Innovationsförderung zwischen Staat und Markt

Schon aus den grundrechtlichen Gewährleistungspflichten lässt sich die Forderung ableiten, dass der Staat zum Schutz der Informationssicherheit Maßnahmen der Forschungs- und Innovationsförderung ergreifen muss.[145] Dem trägt die Politik bereits umfassend Rechnung.[146]

Bemerkenswert ist insbesondere der Versuch, der fehlenden Vernetzung zwischen Staat, Wirtschaft und Forschung, aber auch dem konkreten Mangel an Wagniskapitalfinanzierung durch den Aufbau neuer spezialisierter Forschungsförderungsorganisationen beizukommen. So sind auf der Grundlage von Beschlüssen der Bundesregierung 2019 und 2020 die Agentur für Sprunginnovation (SPRIND) und die Agentur für Innovation in der Cybersicherheit (Cyberagentur) je in der Rechtsform einer GmbH eingerichtet worden.[147] Erstere arbeitet im Auftrag des BMBF und des BMWK und widmet sich der Forschungsförderung im Bereich „disruptiver" Technologien, darunter insbesondere auch der Cybersicherheit, aus ziviler Perspektive. Zweitere soll unter Anbindung an das BMI und das BMVg Projekte der IT-Sicherheit anstoßen,

(Hrsg.), IT-Sicherheitsrecht, 2021, § 9 Rn. 75 ff. Anders für Verträge speziell über IT-Sicherheitsleistungen und für Outsourcing-Verträge, *Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022, Rn. 96 ff., 544 ff. (mit dem Hinweis, a. a. O., Rn. 104, dass „größere Unternehmen bei der Inanspruchnahme externer IT-Leistungen den Anbietern regelmäßig bei Vertragsschluss umfassende Regelwerke zur Umsetzung rechtlicher IT-Sicherheitspflichten" vorlegen); knapp auch *Conrad*, Compliance, IT-Sicherheit, Ordnungsmäßigkeit der Datenverarbeitung, in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht 3. Aufl. 2019, § 33 Rn. 315 ff. Keine klaren Aussagen hierzu trifft *N. Wiegand*, IT-Vertragsrecht, in: Kipker (Hrsg.), 2020, Kap. 7.

[144] Zum Problem von Cyberversicherungen siehe bereits § 4 Fn. 148.

[145] Siehe oben § 5 II. 1. Zur Einwirkung des Rechts auf Innovationsprozesse durch die Förderung von Forschung und Entwicklung siehe die Diskussion und die Nachweise bei § 3 Fn. 67.

[146] Siehe den Überblick über die umfangreichen Aktivitäten des Bundes in diesem Bereich bei *BMBF*, Digital. Sicher. Souverän. Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit 2021–2026, Juni 2021.

[147] Hierzu *Herpig/Rupp*, Deutschlands staatliche Cybersicherheitsarchitektur, 8. Aufl. 2022, S. 112 f. m. w. N. Für entsprechende Initiativen auf EU-Ebene siehe *A. Bendiek/E. Pander Maat*, The EU's Regulatory Approach to Cybersecurity, SWP Working Paper, 2019, S. 14, 23.

die für Sicherheitsbehörden und Militär relevant sind. Die Einrichtung der Agenturen zeigt, dass der Staat den Handlungsbedarf erkannt hat. Der Gründungsprozess erwies sich jedoch als schleppend; verschiedene Anzeichen deuten zudem darauf hin, dass die Institutionen die ihnen zugedachte Funktion nicht hinreichend erfüllen können. Die Gründe hierfür sind teils (dienst-, haushalts- und vergabe-)rechtlicher, vor allem aber verwaltungspraktischer Natur.[148]

Einen vergleichbaren, allerdings stärker forschungszentrierten Zweck verfolgt das bereits erwähnte Europäische Kompetenzzentrum für Cybersicherheit und das daran angeschlossene Netz nationaler Koordinierungszentren, die gemeinsam zur Stärkung von Forschung und Entwicklung im Bereich der zivilen Informationssicherheit beitragen sollen.[149] Auch hier lassen sich bei näherer Betrachtung erhebliche, die Funktionsfähigkeit des Zentrums gefährdende Konstruktionsmängel identifizieren.[150]

c) Aufbau spezialisierter Organisationseinheiten und administrativer Netzwerke zur Verarbeitung gesellschaftlich generierten Wissens

Für ein derart bedeutendes und technisch geprägtes Problemfeld wie die Informationssicherheit führt auf staatlicher Seite an der Einrichtung spezialisierter Organisationseinheiten und Informationsnetzwerke, in denen „organisationales Wissen" kultiviert werden kann, kein Weg vorbei.[151] Eine zentrale Stelle mit breiten Zuständigkeiten muss innerhalb der Verwaltung und in die Gesellschaft hinein als Ansprechpartner und Koordinierungsstelle für das Thema Informationssicherheit wirken. Die Konkretisierung der differenzierten Pflichtenprogramme setzt zudem feste Expertise bei den Behörden voraus, denen die Effektuierung und Kontrolle konkret übertragen ist. Eine Institutionalisierung ist schließlich Vorbedingung für eine nicht nur lernwillige, sondern auch lernfähige Verwaltung, die ihre Perspektive über die Erledigung des konkreten Vorgangs hinaus weiten kann.[152] Organisationsfragen berühren nicht

---

[148] Vgl. das aus verwaltungswissenschaftlicher Sicht bemerkenswerte Interview mit dem Gründungsdirektor der Agentur für Sprunginnovation, Rafael Laguna de la Vera, bei *P. Bernau*, „Deutschland scheitert in kleinen Schritten", F.A.Z., 30.5.2021. Aktuell ist ein „SprinD-Freiheitsgesetz" in Planung.

[149] Siehe oben § 5 Fn. 238.

[150] Vgl. *Gräfin von Wintzingerode/Müllmann/Spiecker gen. Döhmann*, Ein Netzwerk für Europas Cybersicherheit, NVwZ 2021, S. 690 (694 f.).

[151] Zum Wandel der „Kultur des Wissenstauschs", die von „primär personalem auf stärker organisationales Wissen" umstellt, allgemein *Augsberg*, Informationsverwaltungsrecht, 2014, S. 106; vgl. auch *Hoffmann-Riem*, Einleitende Problemskizze, in: ders./Schmidt-Aßmann (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, 2000, S. 9 (33 f.).

[152] Zur Verwaltung als lernendem System grundlegend *A. Benz*, Kooperative Verwaltung, 1994, S. 130 f., 137, 145; *M. Eifert*, Regulierte Selbstregulierung und die lernende Verwaltung, DV Beiheft 4 (2001), S. 137 ff.; *C. Sabel/W. Simon*, Minimalism and Experimenta-

nur die administrative Wissensorganisation. Sie sind vielmehr auch – aus verfassungsrechtlicher Sicht wohl sogar in erster Linie – Legitimations-, Gewaltenteilungs- und Rechtsstaatsfragen. Als solche sind sie hier bereits gewürdigt worden.[153] Die folgenden Ausführungen konzentrieren sich daher darauf, die Organisation der Informationssicherheitsverwaltung als Mittel zum Aufbau einer regulatorischen Wissensinfrastruktur zu analysieren.

Beim Aufbau entsprechender Fachverwaltungen haben Union und Mitgliedstaaten im vergangenen Jahrzehnt erhebliche Fortschritte erzielt. In Deutschland kommt dem BSI spätestens seit 2015 die Funktion der zentralen nationalen Regulierungsbehörde in Sachen Informationssicherheit zu.[154] Mit jeder neuen Gesetzesänderung wachsen Aufgabenportfolio und Budget des BSI weiter an. Eine ähnliche Aufwertung erlebt in Europa ENISA, die seit 2019 als European Union Agency for Cybersecurity firmiert.[155]

Im Falle des BSI spiegelt sich dies im neugefassten § 1 BSIG 2021, der das BSI in S. 2 als die „zentrale Stelle für Informationssicherheit auf nationaler Ebene" positioniert, die „auf Grundlage wissenschaftlich-technischer Erkenntnisse" tätig wird (S. 3),[156] vor allem in der immer umfassenderen Aufgabenbeschreibung des § 3 BSIG 2021.[157] Diese wurde durch das IT-SiG 2.0 nicht nur um die Tätigkeit des BSI als nationale Behörde für die Cybersicherheitszertifizierung (§ 3 Abs. 1 S. 2 Nr. 5a BSIG 2021), sondern auch um neue Zuständigkeiten für die Beratung, Information und Warnung von staatlichen und privaten Stellen, insbesondere der Verbraucher erweitert (§ 3 Abs. 1 S. 2 Nr. 12a, 14, 14a, 17 BSIG 2021). Ebenso wurde dem Amt eine noch aktivere Rolle bei der Entwicklung und Empfehlung von informationssicherheitsbezogenen Standards (§ 3 Abs. 1 S. 2 Nr. 19, 20 BSIG 2021), bei der Untersuchung von IT-Systemen und Produkten (§§ 7a, 7b BSIG 2021) und erstmals auch bei der operativen Gefahrenabwehr (§§ 7c, 7d BSIG 2021) zuerkannt. Das BSI ist zudem nun die zentrale deutsche Meldestelle für Informationssicherheit und hat weitreichende Befugnisse zur Verarbeitung der auf diese Weise erlangten Informationen erhalten (§§ 4b, 5c BSIG 2021). Haushaltstechnisch wird dieser

lism in the Administrative State, Georgetown L. J. 100 (2011), S. 53 ff.; *de Búrca/Keohane/Sabel*, Global Experimentalist Governance, British Journal of Political Science 44 (2014), S. 477 ff.; *Seckelmann*, Evaluation und Recht, 2018, S. 190 ff.

[153] Siehe oben § 5 III. 2.

[154] Vor einer Überforderung der Behörde warnend *M. Schallbruch*, IT-Sicherheitsrecht (Folge 3), CR 2018, S. 215 (223).

[155] Zu den Aufgaben und Befugnisse dieser Behörden im Einzelnen vgl. die nachstehenden Ausführungen unter § 6 II. 4 bis 8.

[156] Zu den mit dieser Änderung verbundenen Zielen näher *Keppeler/Schulte*, in: Ritter (Hrsg.), Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2022, § 1 BSIG Rn. 104.

[157] Zur Erleichterung des Zugriffs werden in diesem Abschnitt die durch das IT-SiG 2.0 im BSIG vorgenommenen Änderungen und Ergänzungen als „BSIG 2021" zitiert.

Aufgabenzuwachs durch einen erheblichen Personalaufwuchs der Behörde um mehrere hundert zusätzliche Stellen unterfüttert.[158]

Angesichts der differenzierten Problemstellungen, die die Aufgabe Informationssicherheit schon aus technischer Sicht bereitet, kann es mit dem Aufbau einer einzelnen Fachbehörde jedoch nicht sein Bewenden haben. Bei für die Verwaltung ganz neuen Materien bietet die Konzentration einer Aufgabe bei einer Behörde zwar kurzfristig Vorteile, da sich behördenintern rasch und gezielt Wissen aufbauen lässt. Die Integration operativer Funktionen erhöht das Wissensniveau nochmals und ermöglicht vergleichsweise schnelle Reaktionen bei akuten Zwischenfällen.[159] Eine Aufspaltung der Zuständigkeiten und Fähigkeiten innerhalb der Verwaltung kann demgegenüber kontraproduktiv wirken, da Wissen und Fähigkeiten innerhalb der Verwaltung weder gleichmäßig verteilt sind noch verlustfrei distribuiert werden können. Mittelfristig wird bei Querschnittsmaterien wie der Informationssicherheit die Zuweisung der Aufgabe an eine einzelne „Superbehörde" – unabhängig von den kompetenzrechtlichen Problemen eines solchen Projekts – den sektoralen Besonderheiten jedoch nicht gerecht werden. In solchen Fällen bietet es sich an, übergeordnete regulatorische und operative Tätigkeiten bei der Fachbehörde zu konzentrieren und Routinetätigkeiten sowie spezielle Aufgabenbereiche an andere Stellen in der Verwaltung zu delegieren. Schon jetzt sind sowohl auf nationaler als auch auf Unionsebene neben der Zentralstelle zahlreiche weitere Wissensakteure mit Aspekten der Regulierung von Informationssicherheit betraut, so etwa die BNetzA mit der Erstellung der IT-Sicherheitskataloge für die KRITIS-Betreiber im Sektor Energie und die Datenschutzbehörden dort, wo personenbezogene Daten betroffen sind.[160]

Ergänzt werden müssen diese Organisationsstrukturen durch vertikale und horizontale Informationsmechanismen (vgl. hierzu Art. 10 NIS-RL/Art. 13 NIS 2-RL). Diese müssen die wechselseitigen Kooperationsbedarfe einer ebenenübergreifenden und auch sonst dezentralisierten und dekonzentrierten Informationssicherheitsverwaltung bewältigen.[161] Das geltende Recht sieht zu diesem Zweck verschiedene Koordinationspflichten des BSI mit weiteren Fachbehörden vor bzw. räumt letzteren Beteiligungsrechte an Entscheidungs-

---

[158] Siehe dazu im Detail die Gesetzesbegründung *Deutscher Bundestag*, Gesetzesentwurf der Bundesregierung zum IT-SiG 2.0, BT-Drs. 19/26106, S. 36 f.

[159] Zu den operativen Funktionen des BSI als nationales CERT/CSIRT siehe § 6 II. 8. b).

[160] Zum Panorama der auf nationaler und Unionsseite involvierten Stellen siehe oben § 5 III. 1. b). Zum Begriff des „Wissensakteurs" im vorliegenden Kontext *Leisterer*, Internetsicherheit in Europa, 2018, S. 42 ff.

[161] Zum Begriff der „Kooperation" als kommunikatives Zusammenwirken unterschiedlicher, sich im jeweiligen Interaktionsprozess wechselseitig als gleichberechtigt anerkennender Organisationseinheiten zur Realisierung gemeinsamer Ziele siehe *Benz*, Kooperative Verwaltung, 1994, S. 38 f. m. w. N.

verfahren des BSI ein.[162] Die Balance dieser Verbundstruktur ist delikat, gilt es doch einerseits zu verhindern, dass allzu weitreichende Koordinationspflichten zur Lähmung der Verwaltung führen, andererseits aber sicherzustellen, dass die Fachbehörden hinreichend gehört werden, um den Entscheidungen des BSI auch in der Ebene praktische Durchschlagskraft zu verleihen.[163] Vor analogen Herausforderungen steht ENISA bei der Organisation der Kooperationsbeziehungen im europäischen Rahmen.

d) Aufbau kooperativer Plattformen zum Informationsaustausch zwischen Staat und Gesellschaft

Wissenstransfer und -distribution müssen auch im Verhältnis von Staat und Gesellschaft gestärkt werden. In Sachen Informationssicherheit existieren hierfür sehr unterschiedlich ausgestaltete Kommunikationsplattformen. Die Organisation des diesbezüglichen Informationsaustauschs hat sich kontinuierlich formalisiert.

Ursprünglich beschränkte sich die Rolle des BSI im Umgang mit dem privaten Sektor ganz auf informelle Formen der Information und Kooperation.[164] Hiervon zeugen insbesondere die 2005 und 2007 verabschiedeten IT-Sicherheitsstrategien des BMI.[165] Entsprechende Formen einer indirekten Steuerung durch Behördenhandeln, die vor allem auf Sensibilisierung der Öffentlichkeit

[162] Hierzu weiter § 6 II. 5. b).

[163] Parallelstrukturen bestehen insbes. im Verhältnis zum Datenschutzrecht. So obliegt die Durchsetzung der datenschutzrechtlichen IT-Sicherheitsvorgaben den Datenschutzbehörden. Dies gilt auch für die technischen und organisatorischen Sicherheitsvorgaben des Telemediendatenschutzes (bisher § 13 Abs. 7 TMG und jetzt – weitgehend unverändert – § 19 Abs. 4 TTDSG). Die Rolle des BSI beschränkt sich insoweit auf die Konkretisierung des vom Datenschutzrecht verlangten Stands der Technik; Kontrolle und Durchsetzung nehmen die Datenschutz- bzw. sonstigen Aufsichtsbehörden vor.

Eine bessere Nutzung der Fachkompetenz des BSI sieht demgegenüber das IT-SiG im Verhältnis zur Bundesnetzagentur im Telekommunikationssektor vor. Danach konkretisieren BSI und BNetzA die IT-Sicherheitskataloge im wechselseitigen Einvernehmen (§ 167 Abs. 1 TKG). Für die Definition der Sicherheitskataloge nach § 11 Abs. 1a und Abs. 1b EnWG ist es demgegenüber bei der vorrangigen Zuständigkeit der Regulierungsbehörde geblieben, die sich hierzu mit dem BSI nach wie vor nur ins Benehmen setzen muss, vgl. *BNetzA*, IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz, August 2015; *dies.*, IT-Sicherheitskatalog für Betreiber von Energieanlagen, Dezember 2018. Auch die Kontroll- und Durchsetzungsbefugnisse verbleiben dort bei der Regulierungsbehörde.

[164] Zur Frühphase vgl. *Wiater*, Sicherheitspolitik zwischen Staat und Markt, 2013, S. 96 ff. Siehe auch *H. Hill*, Verwaltungskultur und Kompetenzen, in: ders. (Hrsg.), Transparenz, Partizipation, Kollaboration, 2014, S. 125 ff.

[165] *BMI*, Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI), 2005; *BMI*, Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen, 2007. Bei UP KRITIS beteiligten sich etwa 30 große KRITIS-Betreiber und Interessenverbände sowie verschiedene Stellen des Bundes an der kooperativen Ausarbeitung von IT-Sicherheitsstandards.

und „moral persuasion" zielen, sind aus anderen Bereichen der Wirtschaftsregulierung bekannt.[166] In Europa entfaltete das Modell einer beratenden Stelle, die zugleich Koordinierungsaufgaben für private und öffentliche Aktivitäten übernahm, Vorbildwirkung. So konzentrierte sich die 2005 geschaffene ENISA zunächst ebenfalls weitgehend auf den informellen Informationsaustausch.

Auch heute noch pflegen die zuständigen Behörden einen umfassenden informellen Informationsaustausch mit dem Privatsektor. Im Falle des BSI erfolgt dieser vor allem über die vom BSI und dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom) initiierte „Allianz für Cyber-Sicherheit". Der Allianz, die zwar ihre Geschäftsstelle beim BSI hat, jedoch keinerlei hoheitliche Funktionen wahrnimmt, gehören derzeit über 5000 Behörden, Unternehmen und Forschungseinrichtungen an; ihr Zweck ist der Austausch zu allen die Cybersicherheit betreffenden Fragestellungen.[167] Ein ähnliches Austauschformat stellt die öffentlich-private Partnerschaft zum Schutz Kritischer Infrastrukturen (UP KRITIS) dar.[168] Auch der Nationale Cyber-Sicherheitsrat, in dem Vertreter von Bund und Ländern gemeinsam mit der Wirtschaft Ziele der Informationssicherheitspolitik besprechen, arbeitet weitgehend informell.[169] Die entsprechenden Aktivitäten des BSI wurden durch das IT-SiG 2.0 nochmals explizit als Behördenaufgabe festgeschrieben unter besonderer Betonung des Verbraucherschutzes, § 3 Abs. 1 S. 2 Nr. 14 und 14a BSIG.[170]

Einen Schritt hin zur Verrechtlichung stellte dann das IT-SiG von 2015 dar, das die hoheitlichen Befugnisse des BSI erheblich stärkte – auch die informelle Kommunikation erfolgt heute im Schatten der Hierarchie – sowie neue, stärker formalisierte Kommunikationsforen einführte. So wird seither bei der Ausbildung von Sicherheitsstandards vermehrt auf hoheitlich regulierte Selbstregulierung gesetzt.[171] Entsprechend hat die NIS-Richtlinie das zuvor lose Netzwerk aus unionalen und mitgliedstaatlichen Stellen einerseits und Privaten andererseits stark aufgewertet und ENISA mit Koordinationsaufgaben betraut.[172] Der CSA hat dann 2019 das Zusammenwirken von privaten Zertifi-

---

[166] Grundlegend *W. Brohm*, Strukturen der Wirtschaftsverwaltung, 1969, S. 234 ff. Zur Bedeutung indirekter Steuerung im Informationssicherheitsdiskurs *Wiater*, Sicherheitspolitik zwischen Staat und Markt, 2013, S. 82 ff., 162 ff.

[167] Zur Selbstdarstellung: https://www.allianz-fuer-cybersicherheit.de.

[168] Näher dazu https://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/UPK/upk_node.html.

[169] Näher dazu https://www.bmvg.de/de/themen/cybersicherheit/partnerschaften-zur-cybersicherheit/cyber-sicherheitsrat.

[170] Zu den hohen Erwartungen des Gesetzgebers gerade in Sachen Verbraucherinformation siehe BT-Drs. 19/26106, S. 59 f.

[171] Siehe § 6 II. 5. b).

[172] *Wischmeyer*, Informationssicherheitsrecht, DV 50 (2017), S. 155 (174 f.).

zierungsinstitutionen und Aufsichtsbehörden in den Blick genommen. Details hierzu werden noch berichtet.[173] An dieser Stelle genügt der Hinweis, dass durch die Bündelung der entsprechenden Kommunikation beim BSI, das als nationale Zertifizierungsstelle für IT-Sicherheit fungiert (§ 9 Abs. 1 BSIG), und bei ENISA, das unionsweit eine Koordinations- und Steuerungsfunktion für den neu geschaffenen Behördenverbund – die „European Cybersecurity Certification Group" – übernimmt (Art. 8 Abs. 1 lit. e i. V. m. Art. 62 Abs. 5 CSA), die Einbeziehung in die Organisation des Zertifizierungsprozesses zugleich zur Stärkung der Fachkompetenz der Behörden beitragen dürfte.

Hingewiesen sei abschließend noch auf den Austausch in operativen Belangen, auf den sich der 2002 vom CERT-Bund (BSI) und weiteren Akteuren gegründete Deutsche CERT-Verbund konzentriert, dem heute neben weiteren privaten Akteuren auch die IT-Notfalls-Teams zahlreicher Länder, Universitäten und Unternehmen angehören.[174] Das unionale Äquivalent hierzu ist das durch die NIS-Richtlinie eingesetzte CSIRTs Netzwerk (Art. 12 NIS-RL), das durch die jüngste Reform nochmals erheblich in seiner Bedeutung aufgewertet wird (vgl. Art. 15 NIS 2-RL).[175]

e) Transparenzförderung durch Melde- und Informationspflichten

Nicht immer teilen private Akteure ihre Informationen freiwillig mit staatlichen Stellen. Insbesondere bei IT-Zwischenfällen ist der Anreiz zur Geheimhaltung groß. Dadurch fehlt es an Markttransparenz, die Grundlage angemessener Risikokalkulationen ist.[176] Zudem wird staatlichen Stellen so die Möglichkeit genommen, Sanktionen zu verhängen und die unmittelbar vom Angriff Betroffenen sowie Dritte, die dasselbe verwundbare System einsetzen, zu warnen.

Aus diesen Gründen spielen Meldepflichten für IT-Sicherheitszwischenfälle eine zentrale Rolle in der Wissensinfrastruktur des Informationssicherheitsrechts.[177] Ähnlich wie in anderen Gebieten des Verwaltungsrechts[178] verpflichten diverse Normen hier die Betreiber kritischer Infrastrukturen sowie weiterer Dienste durch Eigenkontrollsysteme oder sonst entdeckte „erhebliche" potenzielle oder aktuelle Störungen unverzüglich an das BSI bzw. die zu-

[173] Siehe § 6 II. 6.

[174] Näher dazu https://www.cert-verbund.de. Dazu weiter § 6 II. 8. b).

[175] Näher dazu https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network.

[176] Siehe § 6 Fn. 143.

[177] Die Rechtslage vor dem IT-SiG 2.0 wird monographisch aufgearbeitet bei *F. Schneider*, Meldepflichten im IT-Sicherheitsrecht, 2017.

[178] Dazu im Überblick *Wischmeyer*, Informationsbeziehungen in der Verwaltung, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 3. Aufl. 2022, § 24 Rn. 83. Vgl. dazu aus dem Sicherheitsrecht auch *N. Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, 2014, S. 286 ff., 493 ff.

ständige Behörde zu melden.[179] Bei einem Verstoß drohen Sanktionen.[180] Sind personenbezogene Daten betroffen, greift die DSGVO; danach muss die verantwortliche Stelle bei Sicherheitszwischenfällen unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden gemäß Art. 33 Abs. 1 und 2 DSGVO Meldung an die Datenschutzaufsichtsbehörden erstatten und gegebenenfalls gemäß Art. 34 DSGVO die Betroffenen informieren.[181] Was Letztere betrifft, spielen Meldepflichten für die Effektuierung des Haftungsrechts eine wichtige Rolle.[182]

Mit Blick auf die Wissensakkumulation und -distribution ist die Ausgestaltung der Meldeketten von hoher Relevanz. Im Sinne der Koordinierungsfunktion des BSI erscheint es gegenwärtig sinnvoll, dass die Behörde unmittelbar von allen erheblichen IT-Zwischenfällen benachrichtigt wird. Hierfür hat der Gesetzgeber durch die Zentralisierung der Meldewege für KRITIS-Betreiber gesorgt. Darüber hinaus erscheint es nachvollziehbar, wenn der Gesetzgeber als Adressat der Meldepflichten die je zuständige Aufsichtsbehörde benennt, die zusätzlich mit der Entgegennahme von Meldungen zur Informationssicherheit beauftragt wird.[183] Dies kann zur Entlastung des BSI beitragen und ist im Interesse der Betroffenen, einen einheitlichen Ansprechpartner für administrative Belange zu erhalten. Allerdings darf dies nicht zulasten der Koordinierungsfunktion des BSI gehen. Es ist daher jedenfalls für eine rechtzeitige Weiterleitung der Informationen von der Fachbehörde an das BSI zu

[179] Zu den unionsrechtlichen Vorgaben vgl. Art. 14 Abs. 3 und Art. 16 Abs. 3 NIS-RL bzw. jetzt Art. 23 NIS 2-RL. Umgesetzt wurden die Vorgaben der NIS-RL insbes. durch §§ 8b Abs. 4 S. 1; 8c Abs. 3 S. 1; 8f Abs. 7 S. 1 und Abs. 8 BSIG; § 44b AtG; § 11 Abs. 1c EnWG; § 168 TKG. Zu Umfang und Inhalt der gesetzlichen Meldepflichten vgl. die Hinweise in *Deutscher Bundestag*, Gesetzesentwurf der Bundesregierung zum IT-SiG 2.0, BT-Drs. 19/26106, S. 82; *N. Winter*, Meldepflichten bei Cyberangriffen, CR 2020, S. 576 ff.; *Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022, Rn. 221 ff. (nach DSGVO), 277 ff., 315 ff., 334 ff. (nach BSIG), 413 ff. (nach TKG), 438 ff. (nach EnWG), 447 (nach AtG), 465 (nach SGB V). Das BSI stellt für Meldungen unter https://mip.bsi.bund.de ein Meldeportal bereit. Siehe auch die FAQ der Behörde zur Meldepflicht, abrufbar unter https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/KRITIS-FAQ/FAQ-zur-Meldepflicht/faq-zur-meldepflicht_node.html.

[180] Verstöße gegen Meldepflichten können als Ordnungswidrigkeiten geahndet werden, vgl. § 14 Abs. 2 Nr. 7 BSIG; § 95 Abs. 1 Nr. 2b EnWG. Siehe jetzt die unionsrechtliche Verpflichtung zur Einführung von Ordnungswidrigkeitstatbeständen in Art. 34 Abs. 4 und 5 NIS 2-RL.

[181] Dazu näher *D. Müllmann/M. Volkamer*, Meldepflicht von Mitarbeitenden bei IT-Sicherheits- und Datenschutzvorfällen, ZD 2021, S. 8 ff. Aus der aufsichtsbehördlichen Praxis siehe *EDPB*, Guidelines 01/2021 on Examples regarding Personal Data Breach Notification, Version 2.0, 14.12.2021.

[182] Dazu weiter § 6 II. 8. c).

[183] So ist etwa gemäß § 54 Zahlungsdiensteaufsichtsgesetz (ZAG) zunächst die BaFin direkter Adressat einer Meldung und nur bei Finanzinstitutionen, die auch als KRITIS klassifiziert sind, zusätzlich das BSI.

sorgen.[184] Die gesetzgeberische Praxis bewegt sich in diese Richtung. Abgesehen vom Datenschutzrecht, das insoweit durch die unionsrechtliche Vorprägung eine Meldung an die Datenschutzaufsichtsbehörden verlangt, ist durch die jüngsten Reformen eine Konsolidierung und Standardisierung der Meldewege unter Berücksichtigung der zentralen Stellung des BSI erfolgt.[185] Je weiter der Anwendungsbereich der Meldepflichten gezogen wird, desto mehr und desto mehr „triviale" Fälle werden allerdings gemeldet werden. Um die Fachbehörden nicht zu überfordern, sieht Art. 23 NIS 2-RL hier eine sinnvolle Akzentverlagerung vor; so sind nunmehr standardmäßig nicht die nationalen Fachbehörden, sondern die stärker technisch-operativ ausgerichteten CERTs/CSIRTs (vgl. Art. 10 und 11 NIS 2-RL) als Adressaten der Meldungen vorgesehen. Da das Unionsrecht eine enge Zusammenarbeit zwischen Fachbehörde und CERT/CSIRT verlangt (vgl. Art. 12 und 13 NIS 2-RL) – die Funktion der Fachbehörde und des CERT/CSIRT kann auch gemeinsam einer Stelle übertragen werden – bleibt die Informationshoheit ersterer gewahrt.

Neben diesen Fragen der administrativen Zweckmäßigkeit wird die Verfassungsmäßigkeit der Meldepflichten viel diskutiert. Im Fall der Informationssicherheit bestehen jedoch angesichts der großen Bedeutung funktionierender IT-Systeme sowie der zurückhaltenden Ausgestaltung der aktuell angeordneten Pflichten keine ernsthaften Zweifel an deren Geeignetheit, Erforderlichkeit und Angemessenheit.[186]

Zusätzlich abgesichert wird der Informationsfluss zwischen Betreibern und Behörden durch teils umfangreiche Nachweispflichten. So müssen gemäß § 8a Abs. 3 BSIG bzw. Art. 15 NIS-RL/Art. 32 NIS 2-RL die KRITIS-Betreiber dem BSI alle zwei Jahre die Erfüllung der Sicherheitsstandards in Form von Sicherheitsaudits, Prüfungen oder Zertifizierungen nachweisen.[187] Das BSIG

[184] Zur mittelfristigen Perspektive, die eine Verlängerung der Meldewege bis auf die unionale Ebene vorsehen muss, siehe § 6 II. 3. g).

[185] Vgl. beispielsweise noch § 109a Abs. 1 TKG i. d. F. des Gesetzes zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6.7.2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union vom 23.6.2017 (BGBl. I S. 1885). Siehe dagegen jetzt die gestärkte Stellung des BSI in § 168 TKG n. F.

[186] Zur Vereinbarkeit mit den unternehmerischen Freiheiten siehe oben § 5 I. 1. Siehe auch *Schneider*, Meldepflichten im IT-Sicherheitsrecht, 2017, S. 576. Meldepflichten stellen im Übrigen keinen Verstoß gegen das grundrechtliche Verbot der Selbstbezichtigung dar; jedoch können einer straf- und ordnungswidrigkeitsrechtlichen Sanktionierung des gemeldeten Verhaltens im Einzelfall Grenzen gezogen sein. Dementsprechend ordnet § 43 Abs. 4 BDSG an, dass eine Meldung in einem Bußgeldverfahren gegen den Meldepflichtigen bzw. Benachrichtigenden nur mit dessen Zustimmung verwendet werden darf. Art. 23 Abs. 1 UAbs. 1 S. 4 NIS 2-RL sieht nun vor: „The mere act of notification shall not subject the notifying entity to increased liability."

[187] Erneut folgen aus der DSGVO noch weitergehende Pflichten. Siehe auch § 109 Abs. 4 TKG.

enthält zudem klassisch ordnungsrechtliche Befugnisse. So räumen §§ 8a Abs. 4; 8c Abs. 4 BSIG dem BSI ein umfassendes Überprüfungsrecht ein und verpflichten die Betreiber zur Auskunftserteilung.[188]

Dort, wo keine Melde- oder sonstige Informationspflichten bestehen und wo daher auch nicht auf die damit verbundenen Meldewege zurückgegriffen werden kann, stellt sich die Frage, in welcher Form eine Veröffentlichung von Schwachstellen erfolgen kann. Diese Frage ist nicht trivial, da das entsprechende Wissen nicht in die falschen Hände gelangen sollte. Auch benötigt es üblicherweise Zeit, bis die für die Komponenten-, System- oder Netzwerksicherheit verantwortlichen Hersteller, Betreiber und sonstigen Akteure durch entsprechende Patches reagieren können. Schließlich kann eine sofortige Veröffentlichung Ermittlungen gegen die Angreifer gefährden.

Für den Umgang mit Informationen über solche Schwachstellen haben sich international Leitlinien für „responsible disclosure" (auch: „coordinated disclosure") etabliert.[189] In Deutschland ist dieser Prozess bisher kaum formalisiert.[190] § 4b Abs. 3 BSIG sieht hier nur ein recht schwergängiges Verfahren vor.[191] Die hieraus resultierenden Rechtsunsicherheiten gerade für IT-Sicherheitsforscher verlangen dringend nach einer gesetzlichen Regelung.[192] Art. 7 Abs. 2 NIS 2-RL fordern dies nun auch unionsrechtlich.[193] Danach muss jeder Mitgliedstaat ein CSIRT als Koordinator für die koordinierte Offenlegung von Sicherheitslücken benennen; dieses CSIRT fungiert dann als Vertrauensmittler, der erforderlichenfalls zwischen meldender Stelle, dem Hersteller oder Anbieter des kompromittierten IT-Produkts oder -Dienstes vermittelt. Betrifft die gemeldete Schwachstelle mehrere Hersteller oder Anbieter in der Union, so vermittelt das benannte CSIRT die Informationen im CSIRT-Netz weiter. Darüber hinaus beauftragt Art. 12 Abs. 2 NIS 2-RL ENISA mit der Entwicklung und Pflege eines zentralen Schwachstellenregisters. Der Erfolg dieses Ansatzes dürfte allerdings davon abhängen, dass es gelingt, ihn mit den gleich zu berichtenden Informationspflichten, wie sie vor allem durch die DSGVO begründet werden, zu synchronisieren; die Ausnahmeklauseln in Art. 34 Abs. 3 DSGVO bzw. in § 29 S. 3 BDSG, die eine Informationspflicht entfallen lassen, sind insoweit bislang unspezifisch formuliert.[194]

---

[188] Weiter dazu § 6 II. 8. a).

[189] Vgl. den Überblick bei *CEPS*, Software Vulnerability Disclosure in Europe, Juni 2018.

[190] Vgl. dazu *BSI*, Handhabung von Schwachstellen. Empfehlungen für Hersteller, BSI-CS 019, Version 2.0, 11.7.2018.

[191] Zu den Problemen siehe *Keppeler*, in: Ritter (Hrsg.), Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2022, § 4b BSIG Rn. 210 ff.

[192] Hierzu näher *S. Golla*, IT-Sicherheit und Strafrecht, JZ 76 (2021), S. 985 ff. Dazu weiter unter § 6 II. 8. d).

[193] Zu einer Bewertung dieser Norm siehe *S. Schmitz/S. Schiffner*, Responsible Vulnerability Disclosure under the NIS 2.0 Proposal, JIPITEC 12 (2021), S. 447 ff.

[194] Vgl. auch *Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022, Rn. 228.

f) Formen und Verfahren der Wissensdistribution

Bei der Distribution des auf staatlicher Seite generierten Wissens lassen sich zwei Konstellationen unterscheiden. Innerhalb der staatlichen Strukturen selbst müssen, wie erwähnt, Prozesse des inneradministrativen Informationsaustauschs etabliert werden. Dies gilt sowohl im nationalen wie im Unionskontext.[195] In diesem Sinne ordnet Art. 14 Abs. 5, 6 NIS-RL an, dass die zuständige mitgliedstaatliche Behörde bei „erheblichen" Zwischenfällen auch weitere potenziell betroffene Mitgliedstaaten informieren muss (leicht modifiziert durch Art. 23 Abs. 6 NIS 2-RL); sie ist dabei gehalten, die Sicherheit des Anbieters, dessen kommerzielle Interessen und die Vertraulichkeit der Informationen in der Meldung zu gewährleisten sowie Informationen zum effektiven Umgang mit dem Vorfall weiterzugeben.[196] Innerstaatlich sieht § 8b Abs. 2 Nr. 2 BSIG vor, dass das BSI „potentielle Auswirkungen auf die Verfügbarkeit der Kritischen Infrastrukturen in Zusammenarbeit mit den zuständigen Aufsichtsbehörden und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)" analysiert und gemäß § 8b Abs. 2 Nr. 4 BSIG weitere Behörden in Bund und Ländern informiert. Der interne Informationsaustausch zwischen BSI, KRITIS-Betreibern und sonstigen Behörden und Unternehmen garantiert einen gewissen Schutz der Vertraulichkeit etwa von Geschäftsgeheimnissen, was einen weiteren Anreiz zur Offenbarung der Informationen geben kann.[197] Darüber hinaus sind in Zukunft verstärkt Vorgaben zum Austausch relevanter Informationen zwischen Fachbehörden und dem BSI sowohl über konkrete Sicherheitszwischenfälle als auch allgemein in Sachen Informationssicherheit zu implementieren.

Gleichzeitig ist ein gegenüber der allgemeinen Öffentlichkeit geschlossenes Informationssystem nur begrenzt effektiv. Aus diesem Grund sieht § 7 Abs. 1 S. 1 BSIG vor, dass das BSI die Öffentlichkeit oder betroffene Kreise warnen oder auch den Einsatz bestimmter Sicherheitsprodukte empfehlen darf (vgl.

---

[195] Hierzu allgemein *Wischmeyer*, Informationsbeziehungen in der Verwaltung, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 3. Aufl. 2022, § 24; *A. von Bogdandy/L. Hering*, Die Informationsbeziehungen im europäischen Verwaltungsverbund, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 3. Aufl. 2022, § 25. Siehe zum Folgenden bereits *Wischmeyer/Mohnert*, Recht der Informationssicherheit, in: Frenz (Hrsg.), Handbuch Industrie 4.0, 2019, S. 215 (226 ff.).

[196] Wann ein erheblicher und damit meldepflichtiger Sicherheitsvorfall gemäß Art. 14 Abs. 4 NIS-RL vorliegt, wird in der Durchführungsverordnung (EU) 2018/151 der Kommission geregelt. Allgemein dazu auch *Leisterer*, Internetsicherheit in Europa, 2018, S. 201 ff.

[197] Allgemein zu den Grenzen des inneradministrativen Informationsaustauschs *Wischmeyer*, Informationsbeziehungen in der Verwaltung, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 3. Aufl. 2022, § 24 Rn. 32 ff. Speziell für die Informationssicherheit: *Leisterer*, Internetsicherheit in Europa, 2018, S. 142 ff.

auch die differenzierten Vorgaben in Art. 23 Abs. 6 und 7 NIS 2-RL).[198] Konkrete Auskunft über die aufgrund der Meldepflicht nach § 8b BSIG vom BSI erlangten Erkenntnisse erhält die Öffentlichkeit hingegen nach § 8e BSIG nur auf Antrag und nur dann, wenn dem weder schutzwürdige Interessen des betroffenen Betreibers noch sonstige wesentliche Sicherheitsinteressen entgegenstehen. Dies ist deutlich defensiver als die datenschutzrechtliche Regelung in Art. 34 DSGVO, wonach die Verantwortlichen die Betroffenen unverzüglich über relevante Zwischenfälle bzw. Störungen, die von Datenverarbeitungssystemen ausgehen, benachrichtigen und über etwaige technische Abhilfemöglichkeiten informieren müssen.[199]

Die Vorzüge eines solchen proaktiven Informationsmanagementsystems liegen jedenfalls aus Sicht der Betroffenen auf der Hand. Gleichzeitig gilt jedoch, dass es – wie soeben dargestellt – der „verantwortliche" Umfang mit Schwachstellen gebieten kann, Information über deren Existenz oder jedenfalls über deren Ausmaß und Natur zunächst zurückzuhalten. Diese sowohl aus rechtspolitischer als auch aus (unions-)verfassungsrechtlicher Sicht einfache Kollisionslage – das verfassungsrechtliche Interesse der Betroffenen an einer unverzüglichen Information kann und sollte temporär zurückgestellt werden, wenn dafür sinnvolle Gründe des Allgemeinwohls sprechen – ist auf der Ebene des einfachen Rechts, das im Falle der DSGVO das individuelle Informationsinteresse strikt priorisiert, derzeit unzureichend geregelt und bedarf der Anpassung. Verfassungsrechtlich deutlich komplexer wird die Situation, wenn staatliche Stellen sich nicht auf Vermittlungstätigkeiten beim Informationsaustausch zwischen Privaten über Schwachstellen beschränken, sondern die dadurch erlangten Kenntnisse für eigene Zwecke ausnutzen wollen. Auf diese Konstellation ist hier im folgenden Kapitel separat einzugehen.[200]

g) Zwischenfazit

Das Recht der Informationssicherheit nutzt den Kanon etablierter Instrumente zur Wissensgenerierung und -distribution bereits intensiv. Die hohe Informationsdichte muss jedoch auch bewältigt werden. Hierzu müssen die zahlreichen Informationskanäle gebündelt werden, und auf Seiten der Verwal-

[198] Dazu näher gleich für die Komponentensicherheit unter § 6 II. 6. d).

[199] Hervorzuheben ist in diesem Zusammenhang auch die Verpflichtung der Anbieter von Telekommunikationsdienste nach § 168 Abs. 6 TKG, ihre Nutzer darüber in Kenntnis zu setzen, dass deren Systeme kompromittiert sind, und mögliche Schutz- oder Abhilfemaßnahmen zu kommunizieren; vgl. auch die durch das NIS-RL-UmG geschaffene Möglichkeit, den Nutzer hierzu etwa auf eine andere Website umzuleiten (zu § 109a Abs. 4 S. 3 TKG a. F. näher *Ritter*, in: ders. [Hrsg.], Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2022, Teil 1 Rn. 97). Den Hinweis auf IT-Sicherheitsprobleme erhalten die Anbieter über das sog. Providerinformationssystem des BSI, vgl. näher *Ritter*, in: a. a. O., Teil 1 Rn. 49.

[200] Hierzu unter § 7 II.

tung sind ausreichende Kapazitäten zur Strukturierung und Verarbeitung zu implementieren. Andernfalls droht eine Informationsüberflutung. Schlüsselmoment ist ferner eine hinreichende Datenqualität.[201]

Besondere Herausforderungen wirft die Koordination der Wissensbestände zwischen nationaler und unionaler Ebene auf. Hier gilt es, nach dem Vorbild anderer Rechtsbereiche, die nationalen Informationskanäle in ein europäisch geführtes und nach einheitlichen Kriterien administriertes Informationssystem zu überführen.[202] Hier macht die NIS 2-Richtlinie Fortschritte, wenn in Art. 23 NIS 2-RL nationaler und europäischer Meldeweg eng miteinander verwoben werden.

4. Ausgestaltung der Verantwortungsarchitektur

a) Akteure der Informationssicherheit

Effektive rechtliche Regulierung muss jene Stellen identifizieren, die in ihrem jeweiligen Handlungsfeld einen Unterschied machen können. Die Aufschlüsselung der Aufgabe Informationssicherheit und die Unterscheidung verschiedener Regulierungs-„Schichten" hat bereits gezeigt, welche Typen von Ansprechpartnern für die Informationssicherheitsregulierung potenziell in Betracht kommen. Dies sei hier in aller Kürze rekapituliert.[203] So sind natürliche Ansprechpartner, um die Sicherheit von IT-Komponenten (Hardware und Software) zu erhöhen, deren Hersteller. Im Bereich der System- und Netzwerksicherheit lassen sich die jeweiligen Betreiber für die Informationssicherheit in Verantwortung nehmen. In beiden Konstellationen ist ferner das Ökosystem von Drittanbietern zu berücksichtigen, das sich um die Produktion der Komponenten ebenso wie um den Betrieb vernetzter IT-Systeme lagert. Schwie-

[201] Vgl. zur Bedeutung der Datenqualität für die (digitale) Verwaltung ausführlich *K. Heußner*, Informationssysteme im europäischen Verwaltungsverbund, 2007, S. 170 ff.; *L.-S. Deißler*, Gewährleistung von Informationsqualität in europäischen Informationssystemen, 2018.

[202] Zu den unterschiedlichen Verständnissen, die mit dem Begriff des Informationssystems verbunden werden, sowie zu möglichen Vorbildern siehe im Überblick *Wischmeyer*, Informationsbeziehungen in der Verwaltung, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 3. Aufl. 2022, § 24 Rn. 85; vertiefend zu den damit verbundenen Herausforderungen *J.-P. Schneider*, Informationssysteme als Bausteine des Europäischen Verwaltungsverbunds, NVwZ 2012, S. 65 ff.; *Kahl*, Europäische Behördenkooperationen, in: Holoubek (Hrsg.), Verfahren der Zusammenarbeit, 2012, S. 15 ff.; *J.-P. Schneider*, Amtshilfe und Informationsmanagement, in: Schneider/Rennert/Marsch (Hrsg.), ReNEUAL Tagungsband, 2016, S. 197 ff.; *M. Eifert*, Behördliches Informationsmanagement, in: a. a. O., S. 214 ff.; *J.-P. Schneider*, Information exchange, in: Harlow/Leino/della Cananea (Hrsg.), Research Handbook on EU Administrative Law, 2017, S. 81 ff.

[203] Vgl. zu diesen potenziellen „Verteidigern" der Informationssicherheit § 6 II. 1. b). Zur „Gegenseite", den Angreifern, siehe bereits oben § 4 II. 2. a).

riger stellt sich die Situation im Fall der Internetsicherheit dar. Hier ist eine sehr heterogene Gruppe tätig, die neben Anbietern von Infrastruktur- und sonstigen Diensten insbesondere auch die für die technischen Normen zuständigen Fachgremien umfasst.

Es darf nicht übersehen werden, dass die Inpflichtnahme aller gerade genannten Akteure aus verantwortungstheoretischer Sicht nur die zweitbeste Lösung ist. Zumindest auf den ersten Blick läge es näher, jene Akteure in die Pflicht zu nehmen, die die IT-bezogenen Schwachstellen ausnutzen, die also als „Störer" im Rechtssinne operieren. Wie sich die Rechtsordnung an diesem Punkt entwickelt hat und wie sie sich heute positioniert, soll im Folgenden analysiert werden. Dabei ist insbesondere auch auf Lücken in der Verantwortungsarchitektur hinzuweisen, die im Sinne einer effektiven Durchsetzung von Informationssicherheitsinteressen möglichst bald geschlossen werden sollten.

b) Wandel der Verantwortlichkeitsstruktur: Von der Störerhaftung zur Inpflichtnahme privater Dritter für die Risiken der Informationstechnik

Neue Technologien entstehen nie in einem rechtlichen Vakuum. Die Rechtsordnung enthält vielmehr immer schon Normen, die auf die Risiken der neuen Technologien Anwendung finden – und seien es nur die Normen des allgemeinen Haftungsrechts. Das zivilrechtliche Verantwortungsregime garantiert zumindest in der Theorie, dass beim Eintritt von Schäden ein Ansprechpartner zur Verfügung steht. Für Unternehmen wird dies durch Sorgfaltspflichten, die ihren Ursprung im Handels- und Gesellschaftsrecht haben, ergänzt. Die eigentliche regulatorische Frage ist daher stets, ob die tradierten Strukturen ausreichen oder ob zur effektiven Einhegung der neuen Risiken neue Verantwortliche und gegebenenfalls auch neue Pflichtenprogramme bestimmt werden müssen. Mit Blick auf das bewährte, im Grundsatz überaus leistungsfähige Haftungsrecht kann und darf der Gesetzgeber oft abwarten, ob sich mit dessen Hilfe – vermittelt über das Steuerungsmedium des Marktes – tragfähige Lösungen etablieren. Erst wenn das nicht der Fall ist und wenn auch die zur Fortentwicklung des Rechts befugten Instanzen des Rechtsstaats, namentlich die Gerichte, mit den ihnen zur Verfügung stehenden Instrumenten der Auslegung und Rechtsfortbildung der Problematik nicht Herr werden, ist genuiner Handlungsbedarf gegeben.

Dass der Gesetzgeber lange Zeit darauf verzichtet hat, Betreibern von IT-Systemen oder sonst im Ökosystem der IT-Sicherheit relevanten Akteure spezifische Vorgaben zur IT-Sicherheit zu machen, war daher nicht notwendig ein Zeichen von Ignoranz. Es kann auch so verstanden werden, dass der Gesetzgeber zunächst abwarten wollte, ob sich das Informationssicherheitsproblem mit den Mitteln des Haftungsrechts in den Griff bekommen ließ. Aller-

dings wurde schon ab den 1990er-Jahren klar, dass das Haftungsrechts allein[204] mit der Handhabung von Informationssicherheitsrisiken überfordert war.[205] Hierfür war in erster Linie das bereits ausführlich beschriebene Attributionsproblem verantwortlich.[206] Wenn regelmäßig nicht eindeutig bestimmt werden kann, wer einen Schaden, der auf der Ausnutzung von IT-Schwachstellen beruht, herbeigeführt hat, kann das Deliktsrecht seine Restitutions- und Abschreckungsfunktion nicht entfalten. Eben hieran scheiterte auch die analog strukturierte strafrechtliche Verantwortlichkeit.[207] Da IT-Sicherheit zudem, wie ebenfalls bereits berichtet, aus ökonomischer Sicht Eigenschaften eines „öffentlichen Guts" aufweist, ist ferner das Vertragsrecht in seiner Wirkungsweise erheblich eingeschränkt.[208]

Wenn sich der Störer somit in vielen Fällen seiner Verantwortung effektiv entziehen kann, liegt es nahe, stattdessen den Nichtstörer für die Risikoabwehr in die Pflicht zu nehmen.[209] Ein Vorbild hierfür fand sich bereits seit geraumer Zeit im Datenschutzrecht, konkret im Gebot der „Datensicherheit" des § 9 BDSG a. F.[210] Die Vorschrift erklärte alle öffentlichen und nicht-öffentlichen Stellen, die personenbezogene Daten verarbeiteten, zu für die Informationssicherheit verantwortlichen Stellen und ordnete an, dass die Systembetreiber durch technische und organisatorische Maßnahmen sicherzustellen hatten, dass rechtmäßig erhobene Daten insbesondere gegen den unbefugten Zugriff durch Dritte geschützt waren. Trotz der Querschnittsnatur des Datenschutzrechts und der hohen faktischen Bedeutung der Datensicherheit für den Datenschutz liefen diese Bestimmungen jedoch aus ver-

[204] Zur bedeutenden Rolle, die das Haftungsrecht hingegen immer als ein zentrales *Element* im Zusammenwirken mit anderen Regulierungsinstrumenten spielen wird, siehe § 6 II. 8. c).

[205] Grundlegend aus zivilrechtlicher Sicht *J. Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, 1995. Siehe weiter insbes. *G. Spindler*, IT-Sicherheit und Produkthaftung, NJW 2004, S. 3145 ff.; *ders.*, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, 2007; *ders.*, IT-Sicherheit, MMR 2008, S. 7 ff. – je auch mit Nachweisen zum älteren zivilrechtlichen Schrifttum. In der Politik aufgenommen wurden die Erkenntnisse erstmals systematisch durch die Enquete-Kommission „Internet und Gesellschaft", vgl. *Deutscher Bundestag*, Neunter Zwischenbericht der Enquete-Kommission „Internet und digitale Gesellschaft" – Zugang, Struktur und Sicherheit im Netz, 19.3.2013, BT-Drs. 17/12541, S. 65 ff.

[206] Siehe oben § 4 II. 2. b).

[207] Weiter dazu unter § 6 II. 8. d).

[208] Siehe § 6 II. 3. a).

[209] Zu diesem Perspektivwechsel bereits *N. Sales*, Regulating Cyber-Security, Nw. U. L. Rev. 107 (2013), S. 1503 (1544 ff.).

[210] Zu § 9 BDSG a. F., der durch die Anlage (zu § 9 Satz 1) BDSG a. F. weiter konkretisiert wurde, sowie zu landes- und spezialgesetzlichen Parallelnormen seinerzeit ausführlich *W. Ernestus*, in: Simitis (Hrsg.), BDSG, 2014, § 9; *J. Schultze-Melling*, in: Taeger/Gabel (Hrsg.), BDSG, 2. Aufl. 2013, § 9; *D. Heckmann*, Datenschutz, in: ders. (Hrsg.), jurisPK-Internetrecht, 4. Aufl. 2014, Kap. 9 Rn. 245 ff. Vgl. im Übrigen bereits oben § 2 I. 2 und § 3 III.

schiedenen Gründen über lange Zeit leer. Insbesondere gelang es trotz verschiedener Ansätze zur Konkretisierung der technischen Standards nicht, subsumtionsfähige technische Maßstäbe zu entwickeln. Die in der Anlage zu § 9 S. 1 BDSG a. F. benannten Sicherungsmaßnahmen waren zudem bald überholt; der Gesetzgeber konnte oder wollte mit der Dynamik der technischen Entwicklung nicht Schritt halten. Hinzu kamen rechtsgebietsspezifische Probleme: So litten die Klauseln zur Datensicherheit unter den für das Datenschutzrecht seinerzeit allgemein charakteristischen Vollzugsdefiziten.[211] Dass die Sicherungspflichten nach § 9 S. 1 BDSG a. F. in Satz 2 der Norm unter einen allgemeinen Erforderlichkeitsvorbehalt gestellt wurden, relativierte den Befolgungsdruck gleichfalls erheblich.[212] Auch theoretisch-konzeptionell wurde zunächst wenig Aufwand betrieben, um den „objektiven" Aspekt der Datensicherheit in das Schema des im Ausgangspunkt subjektiv-abwehrrechtlich geprägten Datenschutzrechts zu integrieren. Selbst jene Rekonstruktionen des Datenschutzrechts, die den „Systemdatenschutz" in den Mittelpunkt stellten, zogen daraus keine größeren Konsequenzen für die Ausgestaltung der Datensicherheitsklauseln.[213]

Erstmals effektuiert wurde die Inpflichtnahme der „Nichtstörer" für die Risiken der Informationstechnik daher an anderer Stelle, nämlich im Recht der kritischen Infrastrukturen.[214] Als erster Schritt hin zu einer engmaschigeren Regulierung kann der „Umsetzungsplan KRITIS" des BSI von 2007 gelten, der herausarbeitete, in welchem Maße Energiewirtschaft, Gesundheitswesen, Finanz-, Geld- und Versicherungswirtschaft sowie weitere für das Funktionieren der Gesellschaft zentrale Instanzen auf sichere IT-Systeme angewiesen waren. Diese Punkte wurden bald von der Literatur aufgegriffen, die herausarbeitete, dass durch Angriffe auf die IT-Systeme von KRITIS-Betreibern Grundrechte gefährdet werden, deren Genuss vom Funktionieren des digitalen Raums

---

[211] Hierzu näher *Ernestus*, in: Simitis (Hrsg.), BDSG, 2014, § 9 Rn. 63 ff. Aus der allgemeinen Literatur zum Vollzugsdefizit im Datenschutzrecht siehe nur *T. Kingreen/J. Kühling*, Der überspannte Parlamentsvorbehalt im Datenschutzrecht, JZ 70 (2015), S. 213 (215).

[212] Dazu *W. Ernestus*, Bedarf die Anlage zu § 9 BDSG einer Modernisierung?, RDV 2000, S. 146 ff.

[213] Vgl. seinerzeit insbes. *Albers*, Umgang mit personenbezogenen Informationen und Daten, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 2. Aufl. 2012, § 22 Rn. 102 ff.

[214] Dass der KRITIS-Diskurs gerade in seiner Anfangszeit stark durch den Aspekt der Informationssicherheit geprägt war, wurde bereits dargestellt, siehe oben § 4. I. 2. d). Zur Verbindung der Diskurse näher *Sonntag*, IT-Sicherheit kritischer Infrastrukturen, 2005; *G. Spindler*, IT-Sicherheit und kritische Infrastrukturen, in: Kloepfer (Hrsg.), Schutz kritischer Infrastrukturen, 2010, S. 85 ff.; *M. Schmidt-Preuß*, Europäische und internationale Ansätze, in: a. a. O., S. 67 ff.; *S. Schulz*, „Datenautobahn" als Infrastruktur, in: Hill/Schliesky (Hrsg.), Die Vermessung des virtuellen Raums, 2012, S. 265 ff.; *Schulz/Tischer*, Internet als kritische Infrastruktur, ZG 2013, S. 339 ff.

abhängt, was staatliche Regulierungspflichten auslöst.[215] Ein Einschreiten lag daher unter dem Gesichtspunkt der staatlichen Gewährleistungsverantwortung nahe. Bis sich dies in einem umfassenden Regulierungsprogramm niederschlug, dauerte es jedoch. Die Novelle des BSIG von 2009 konzentrierte sich zunächst weitgehend darauf, das BSI als maßgeblichen IT-Sicherheitsdienstleister für die Bundesverwaltung zu positionieren (§§ 4, 5 BSIG).

Den eigentlichen Durchbruch für die Inpflichtnahme des privaten Sektors – erneut vorrangig in Gestalt der KRITIS-Betreiber – stellten das 2015 verabschiedete IT-Sicherheitsgesetz (IT-SiG)[216] und die 2016 verabschiedete Network and Information Security Directive (NIS-Richtlinie)[217] dar.[218] Die Rechtsakte überführten verschiedene aus dem allgemeinen Technikrecht bekannte Instrumente ins Recht der Informationssicherheit und stärkten die Kontrollbefugnisse des BSI gegenüber Privaten. Dabei gaben sie den vormaligen koo-

[215] Dazu bereits ausführlich oben unter § 5 II. Frühzeitig insbesondere *Heckmann*, Staatliche Schutz- und Förderpflichten zur Gewährleistung von IT-Sicherheit, in: Rüßmann (Hrsg.), FS Käfer, 2009, S. 129 ff.; *Möllers/Pflug*, Verfassungsrechtliche Rahmenbedingungen des Schutzes kritischer IT-Infrastrukturen, in: Kloepfer (Hrsg.), Schutz kritischer Infrastrukturen, 2010, S. 47 ff.; *Deutscher Bundestag*, Neunter Zwischenbericht der Enquete-Kommission „Internet und digitale Gesellschaft" – Zugang, Struktur und Sicherheit im Netz, 19.3.2013, BT-Drs. 17/12541, S. 32.

[216] Die folgenden Passagen orientieren sich teilweise an *Wischmeyer*, Informationssicherheitsrecht, DV 50 (2017), S. 155 (161 ff.). Zum IT-SiG – einem Artikelgesetz, das insbes. im BSIG, EnWG, TKG, AtG und TMG Änderungen vornahm – siehe im Detail *C. de Wyl/M. Weise/A. Bartsch*, Neue Sicherheitsanforderungen, N&R 2015, S. 23 ff.; *G. Hornung*, Neue Pflichten für Betreiber kritischer Infrastrukturen, NJW 2015, S. 3334 ff.; *Roßnagel*, Das IT-Sicherheitsgesetz, DVBl. 2015, S. 1206 ff. Ebd. auch zu sektorspezifischen Vorläuferregeln wie der punktuellen Verfügbarkeitsgarantie nach § 5 PTSG. Zum Rechtsstand vor Erlass des IT-SiG 2.0 siehe auch im Überblick *M. Fischer*, IT-Sicherheitsanforderungen an Kritische Infrastrukturen und digitale Dienste, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 13.

[217] Dazu insbes. *M. Gercke*, Der Entwurf für eine EU-Richtlinie über Netz- und Informationssicherheit (NIS), CR 2016, S. 28 ff.

[218] Mit dem IT-SiG kam der deutsche Gesetzgeber dem Unionsgesetzgeber zuvor. Die Ziele und Instrumente der Rechtsakte unterschieden sich nicht wesentlich. Die NIS-Richtlinie erfasst allerdings nicht nur die den KRITIS-Betreibern entsprechenden Anbieter „wesentlicher Dienste" (Art. 14 NIS-RL; dazu gleich § 6 Fn. 219), sondern auch die Betreiber „digitaler Dienste" (Art. 16 NIS-RL), d. h. Online-Marktplätze, Suchmaschinen und Cloud-Computing-Dienste. Über das (dem IT-SiG strukturell vergleichbare) Pflichtenprogramm für die beiden Arten von Anbietern hinaus enthält die Richtlinie zudem einige direkt an die Mitgliedstaaten gerichtete Verpflichtungen, insbesondere zur Ausarbeitung einer nationalen IT-Sicherheits-Strategie, zur Einrichtung eines nationalen CSIRT und zur Benennung verantwortlicher Behörden. Eingeführt wurde zudem ein Mechanismus zur Koordination der nationalen Cybersicherheitsbehörden. Insofern bestand im deutschen Recht nur geringer Anpassungsbedarf, dem der deutsche Gesetzgeber durch das NIS-RL-Umsetzungsgesetz von 2017 (BGBl. 2017 I S. 1885) Rechnung trug. Siehe dazu näher *Schallbruch*, IT-Sicherheitsrecht (Teil 1), CR 2017, S. 648 (649). Das NIS-RL-UmG baute zudem die Rolle des BSI weiter aus, vgl. Art. 4 des NIS-RL-UmG bzw. §§ 291b, 307 SGB V. Vgl. auch *Gehrmann/Voigt*, IT-Sicherheit, CR 2017, S. 93 (96 f.).

perativen Ansatz nicht gänzlich auf, entwickelten diesen jedoch zu einer Form hoheitlich regulierter Selbstregulierung fort, wobei vor allem den Betreibern kritischer Infrastrukturen Sicherungspflichten für ihre IT-Systeme in Gestalt sektorspezifischer Mindestanforderungen aufgegeben wurden. Wichtiger noch als dieser Wandel des Regulierungsmodells war der damit einhergehende Perspektivwechsel: Nunmehr galt das rechtliche Interesse nicht mehr vorrangig den Angreifern, sondern den Betreibern der IT-Systeme, denen abverlangt wurde, eine effektive Verteidigung zu organisieren. Das Gesetz selbst gab Sektoren und grobe Kriterien vor, die dann im Verordnungswege konkretisiert wurden; dabei wurde der Adressatenkreis der Regulierung im Verhältnis zu früheren Ansätzen erheblich erweitert.[219] Auf diese Weise konnte der Gesetzgeber das Attributionsproblem umgehen, waren die Betreiber von Infrastrukturen doch in aller Regel gut greifbar. Erleichtert wurde das regulatorische Vorgehen auch dadurch, dass die KRITIS-Sektoren üblicherweise bereits engmaschig reguliert wurden, sodass (zusätzliche) Vorgaben zur Informationssicherheit nicht auf prinzipiellen Widerstand stießen; letztlich wurde dem oft ohnehin schon engen Regulierungskorsett nur eine weitere Komponente hinzugefügt. Schließlich ermöglichte die Konzentration auf die als KRITIS eingestuften Sektoren die Ausarbeitung recht spezifischer Standards, was die Durchsetzung beförderte.

c) Adressaten des Informationssicherheitsrechts

Seit 2015 hat sich die Verantwortungsarchitektur des Informationssicherheitsrechts weiter ausdifferenziert und über den Kreis der Betreiber kritischer Infrastrukturen hinaus erweitert. Insbesondere in der jüngsten Zeit nimmt der Gesetzgeber zunehmend auch solche Akteure in den Blick, die zur Gewährleistung der Komponenten- und der Internetsicherheit beitragen können.

aa) System- und Netzwerksicherheit

Eine erhebliche faktische Erweiterung seines personellen Anwendungsbereichs erfuhr das Recht der Informationssicherheit durch die Reformen des Datenschutzrechts, namentlich den Erlass der DSGVO.[220] Zwar war, wie be-

[219] Die konkrete Einstufung als Betreiber einer kritischen Infrastruktur richtet sich seither nach § 2 Abs. 10 BSIG bzw. nach den Schwellenwerten der auf § 10 Abs. 1 BSIG gestützten BSI-KritisV v. 22.4.2016 (zu dieser bereits oben § 4 Fn. 56). BSIG und BSI-KritisV ziehen den Begriff der kritischen Infrastrukturen punktuell weiter als die NIS-RL, die von „wesentlichen Diensten" spricht, vgl. Art. 4 Nr. 4 und 5 Abs. 2 i. V. m. Anhang II der RL. Zu den Differenzen im Detail *Schallbruch*, IT-Sicherheitsrecht (Teil 1), CR 2017, S. 648 (650 f.).

[220] Eine Übersicht über den gegenwärtigen Stand der datenschutzrechtlichen Regelungen zur Informationssicherheit bietet *Jandt*, IT-Sicherheit als Mittel und als Bedrohung des Datenschutzes, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 17.

richtet, Datensicherheit seit jeher Teil des Datenschutzrechts. Über die allgemeine Wirksamkeitssteigerung hinaus, die der Datenschutz durch die Reformen erfahren hat, ist jedoch auch speziell der Aspekt der Informationssicherheit aufgewertet worden. So zählt nach Art. 5 Abs. 1 lit. f DSGVO der „Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung" personenbezogener Daten nun zu den allgemeinen Grundsätzen der Datenverarbeitung. Informationssicherheit muss infolge dieser Hochzonung in allen Phasen der Datenverarbeitung Berücksichtigung finden. Alle datenschutzrechtlich Verantwortlichen (Art. 24 DSGVO) und Auftragsverarbeiter (Art. 28 DSGVO) sind hiernach zu entsprechenden Risikoabschätzungen gezwungen, die auch dokumentiert werden müssen (Art. 5 Abs. 2 DSGVO).[221] Die Prüfung von Informationssicherheitsaspekten wird damit zur Routinemaßnahme. Art. 32 DSGVO als Nachfolgeregelung zu § 9 BDSG a. F. kann somit auf eine ganz andere Weise vom breiten Anwendungsbereich des Datenschutzrechts profitieren.[222] Sie knüpft zudem an die etablierte und ausdifferenzierte Dogmatik zur datenschutzrechtlichen Verantwortlichkeit an. Die hier erfassten Akteure sehen sich also auch von dieser Warte aus regulatorischem Druck ausgesetzt.

Ähnlich in die Breite drängen jetzt das BSIG bzw. die weiteren durch das IT-SiG und das IT-SiG 2.0 reformierten Rechtsakte, darunter beispielsweise

[221] Zur Relevanz von Art. 28 Abs. 3 UAbs. 1 lit. c DSGVO, der den Auftragsverarbeiter nochmals explizit auf Art. 32 DSGVO verpflichtet, siehe *Martini*, in: Paal/Pauly (Hrsg.), DS-GVO, 3. Aufl. 2021 Art. 32 Rn. 10.

[222] Zum weiten Begriff des personenbezogenen Datums, der für die Eröffnung des Anwendungsbereichs der DSGVO maßgeblich ist, siehe § 5 Fn. 109. Hinzu kommt, dass Aspekte der Informationssicherheit auch in bereichsspezifischen Regelungen zum Datenschutz eine Rolle spielen und dort entweder die Vorgaben der DSGVO konkretisieren oder für bestimmte vom Anwendungsbereich der DSGVO ausgeklammerte Sachbereiche ähnliche Vorgaben zur Informationssicherheit einführen. Vgl. dazu für den staatlichen Bereich beispielhaft Art. 37, 44 VO (EG) Nr. 810/2009 (Visakodex); Art. 15, 16 VO (EG) 1987/2006 (SIS II); Art. 4 Abs. 1, 34 VO (EU) Nr. 603/2013 (Eurodac); Art. 40 EKEK. Speziell für mitgliedstaatliche Stellen im Bereich der Strafverfolgung und Gefahrenabwehr greifen die Art. 29–31 der JI-Richtlinie 2016/680, die Art. 32 DSGVO stark angenähert sind, aber keine konkreten Regelbeispiele nennen und die Anforderungen an die Verantwortlichen leicht absenken; umgesetzt werden diese Vorgaben in § 64 BDSG. Siehe auch Art. VI-29 ReNEUAL-Musterentwurf für ein Europäisches Verwaltungsverfahrensrecht. Der durch das IT-SiG eingeführte und als großer Wurf geplante § 13 Abs. 7 TMG, der als Teil des Telemedien-Datenschutzes Informationssicherheitspflichten für kommerzielle Telemedienanbieter (Websites, Webserver etc.) vorsah (dazu *C. Djeffal*, Neue Sicherungspflicht, MMR 2015, S. 716 ff.), hat hingegen kaum Wirkungen gezeitigt; zu möglichen Gründen *Gehrmann/Voigt*, IT-Sicherheit, CR 2017, S. 93 (94); *M. Schallbruch*, IT-Sicherheitsrecht (Folge 2), CR 2017, S. 798 f.; *Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022, Rn. 171. Inwieweit § 19 Abs. 4 TTDSG als Nachfolgevorschrift bzw. langfristig die E-Privacy-Verordnung neben dem BSIG und der DSGVO eigenständige Impulse werden setzen können, bleibt abzuwarten, vgl. *Martini*, in: Paal/Pauly (Hrsg.), DS-GVO, 3. Aufl. 2021 Art. 32 Rn. 17g.

die Regelungen zur IT-Sicherheit der „Smart Meter“,[223] im Versicherungs- und Bankenrecht[224], im Gesundheitsrecht[225] sowie im Telekommunikations-[226] und im Energiewirtschaftsrecht[227]. Insbesondere das IT-SiG 2.0 hat das BSIG in Richtung einer horizontalen Regulierung für „große“ Unternehmen fortentwickelt. Nicht nur wird mit der Siedlungsabfallentsorgung ein weiterer Sektor als kritische Infrastruktur im Sinne des § 2 Abs. 10 S. 1 Nr. 1 BSIG 2021[228] ausgewiesen. Vor allem wird mit den „Unternehmen im besonderen öffentlichen Interesse“ (auch: „KRITIS light“) eine weitere Kategorie von Unternehmen einer (partiellen) Regulierung nach dem BSIG unterworfen. Dies sind Hersteller i. S. v. § 60 AWV (Rüstungshersteller), Unternehmen von erheblicher volkswirtschaftlicher Bedeutung[229] und deren wesentliche Zulieferer sowie bestimmte Betreiber im Gefahrstoffbereich (§ 2 Abs. 14 BSIG 2021). Zusammen mit den seit dem NIS-RL-Umsetzungsgesetz von 2017[230] ebenfalls in das BSIG eingezogenen Anbietern „digitaler Dienste“ (§ 2 Abs. 11 BSIG)[231] reguliert das BSI jetzt zahlreiche Wirtschaftssektoren und hat sich damit weit vom ursprünglichen KRITIS-Konzept entfernt, das stark auf die Sicherung

[223] §§ 19 ff. Messstellenbetriebsgesetz (MsbG). Eine wie in § 19 MsbG produktbezogene Verpflichtung zum Einbau von Sicherheitsvorkehrungen enthält etwa auch § 4 Abs. 3 Nr. 5 Funkanlagengesetz.

[224] Relevante Normen sind etwa §§ 27, 53, 54 ZAG, § 25a Abs. 1 S. 3 Nr. 5 KWG, § 80 WpHG, § 13 PrüfBV. Dazu näher *Gehrmann/Voigt*, IT-Sicherheit, CR 2017, S. 93 (98 f.); *Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022, Rn. 485 ff. Zur europäischen und internationalen Dimension ausführlich *Calliess/Baumgarten*, Cybersecurity in the EU, German L. J. 21 (2020), S. 1149 (1162 f., 1165 ff.) m. w. N.

[225] Relevante Normen sind etwa §§ 75b; 75c; 139e Abs. 2 und 10; 311 Abs. 1 Nr. 4; 325; 329 SGB V. Dazu näher *Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022, Rn. 450 ff.

[226] Vgl. §§ 165 ff. TKG. Dazu gleich näher unter § 6 II. 5. c).

[227] Vgl. etwa §§ 21c Abs. 5 S. 2, 21e Abs. 1 und 3, 21f Abs. 1, 21i Abs. 1 EnWG. Siehe auch den Überblick bei *A. von Bremen*, IT-Sicherheitsrecht in der Energiewirtschaft, EWeRK 2020, S. 29 ff.

[228] Zur Erleichterung der Lektüre werden in diesem Abschnitt die durch das IT-SiG 2.0 im BSIG vorgenommenen Änderungen und Ergänzungen erneut als „BSIG 2021“ zitiert.

[229] Zur Erstreckung des BSIG auf „große“ Unternehmen siehe § 2 Abs. 14 S. 1 Nr. 2 BSIG; welche Unternehmen „von erheblicher wirtschaftlicher Bedeutung“ sind, soll in Anlehnung an die Methoden der Monopolkommission zur Bestimmung der größten inländischen Unternehmen durch Rechtsverordnung geregelt werden. Unternehmen im besonderen öffentlichen Interesse unterliegen einem im Vergleich mit KRITIS-Betreibern deutlich abgespeckten Pflichtenprogramm, vgl. § 8f BSIG 2021 und weiter unter § 6 II. 5.

[230] Siehe oben § 6 Fn. 218.

[231] Insoweit wirkt die NIS-RL nach herrschender Auffassung vollharmonisierend; dies führt dazu, dass § 8c BSIG insoweit § 19 TTDSG vorgeht, vgl. dazu gleich § 6 Fn. 240. Soweit Unternehmen nach § 8c BSIG zugleich KRITIS-Unternehmen sind, geht dies allerdings wiederum vor, vgl. *S. Ritter/L. Schulte*, Rechtliche Anforderungen an Anbieter digitaler Dienste, die zugleich kritische Infrastrukturen sind, CR 2019, S. 617 ff.; *Ritter*, in: ders. (Hrsg.), Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2022, Teil 1 Rn. 86 m. w. N.

der physischen Resilienz des deutschen Staates ausgerichtet war.[232] Umso wichtiger werden vor diesem Hintergrund die Schwellenwerte, die im Einzelfall über die Einbeziehung eines Anbieters in die Regulierung entscheiden.[233] Diese werden, soweit sie nicht durch andere Rechtsakte definiert sind, weiterhin durch Rechtsverordnung bestimmt.[234] Hier hat die parallel zum IT-SIG 2.0 vorangetriebene Überarbeitung der maßgeblichen KRITIS-Verordnung, deren jüngste Änderungen zum 1.1.2022 in Kraft getreten sind, gleichfalls zu einer Ausweitung des Anwendungsbereichs durch Absenkung der Schwellenwerte und Einbeziehung neuer Anlagentypen geführt.[235]

In die gleiche Richtung wie das IT-SiG 2.0 wurde auch die NIS 2-RL fortentwickelt. Zwar bleiben die Betreiber „wesentlicher Einrichtungen", die den KRITIS-Betreibern des deutschen Rechts entsprechen, die Hauptansprechpartner auch des europäischen Gesetzgebers.[236] Die NIS 2-RL erweitert den Kreis der einbezogenen Unternehmen jedoch um die Betreiber „wichtiger Einrichtungen" (*important entities*), eine Kategorie, die im Unionsrecht, vor allem in der RCE-RL[237], bisher keine Entsprechung hat und die im deutschen Recht teilweise (aber nicht vollständig) durch die Kategorien der digitalen

[232] Siehe oben § 4 I. 2. d).

[233] Zur Kritik an einem rein quantitativen Schwellenwertbegriff siehe *Ritter*, in: ders. (Hrsg.), Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2022, Teil 1 Rn. 9 m. w. N.

[234] Vgl. § 2 Abs. 10 S. 2 i. V. m. § 10 Abs. 1 BSIG für KRITIS-Betreiber und § 2 Abs. 14 S. 2 i. V. m. § 10 Abs. 5 BSIG 2021 für Unternehmen von erheblicher volkswirtschaftlicher Bedeutung. Wer „digitaler Dienst" ist, bestimmt sich nach Anhang III zur NIS-RL i. V. m. Art. 4 Nr. 17 bis 19 NIS-RL, vgl. auch § 2 Abs. 11 BSIG.

[235] Die Zahl der einbezogenen Unternehmen hat sich allein dadurch um etwa ein Fünftel auf etwa 1900 erhöht, vgl. *BMI*, Referentenentwurf. Zweite Verordnung zur Änderung der BSI-Kritisverordnung, 22.4.2021, S. 2. Die genaue Bestimmung von Unternehmen von „erheblicher volkswirtschaftlicher Bedeutung" soll 2022 durch eine gesonderte Verordnung (vgl. § 10 Abs. 5 BSIG) erfolgen. Siehe auch die transparente Aufbereitung unter https://www.openkritis.de/IT-sicherheitsgesetz/kritis-anlagen_kritisv_itsig20.html. Vgl. zur Systematik der KritisV auch *Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022, Rn. 257 ff.

[236] Die im Sinne der RCE-Richtlinie als „kritische Einrichtungen" (critical entities) firmierenden Sektoren (vgl. Art. 2 Nr. 1 RCE-RL i. V. m. Anhang) entsprechen weitgehend den „wesentlichen Einrichtungen" (essential services), die in Anhang I zur NIS 2-RL definiert sind; diese sind wiederum mit den durch das IT-SiG 2.0 modifizierten Sektoren identisch, schließen allerdings – anders als das BSIG – nun auch die öffentliche Verwaltung ein.

[237] In diesem Zusammenhang ist erneut darauf hinzuweisen, dass parallel zum Entwurf der NIS 2-RL auch die Ersetzung der Richtlinie 2008/116/EC durch eine neue „Richtlinie über die Resilienz kritischer Einrichtungen" (RCE-Richtlinie) betrieben wurde (vgl. oben § 1 Fn. 30 und soeben § 6 Fn. 236). Beide Richtlinien zielen, gewissermaßen komplementär, darauf, das Schutzniveau kritischer Infrastrukturen deutlich zu erhöhen, haben also einen weitgehend identischen Anwendungsbereich. In der RCE-Richtlinie steht allerdings die Resilienz- und Vorsorgeplanung im Mittelpunkt, mithin Gesichtspunkte, die dem klassischen Katastrophenschutz zuzuordnen sind, während sich die NIS 2-RL speziell der IT-Sicherheit widmet.

Dienste (§ 2 Abs. 11 BSIG) und durch die „Unternehmen im besonderen öffentlichen Interesse" (§ 2 Abs. 14 BSIG 2021) abgedeckt wird.[238]

Trotz dieser Tendenz zur Horizontalisierung der Materie entfalten die zahlreichen sektorspezifischen Rechtsakte zur Informationssicherheit nach wie vor ihre Kraft.[239] Soweit sich deren Anwendungsbereich teilweise mit der KRITIS-Regulierung überlappt, gehen sie als speziellere Regelungen nach allgemeinen Regeln grundsätzlich vor (vgl. § 8d Abs. 2 und 3 BSIG). Nicht in allen Fällen ist jedoch eine Abgrenzung im Einzelfall problemlos möglich.[240] Hier ist der Gesetzgeber aufgerufen, entweder den Normbestand weiter zu arrondieren oder für eindeutige Kollisionsregeln zu sorgen.

bb) Komponenten- und Internetsicherheit

Traditionell hat das Datenschutzrecht nur die für die Datenverarbeitung verantwortlichen Stellen für die Informationssicherheitsgewährleistung in die Pflicht genommen. Auch die von Art. 32 Abs. 1 DSGVO geforderten technischen und organisatorischen Maßnahmen stellen noch den System- und Netzwerkschutz in den Vordergrund. Allerdings sind, wie erwähnt, die Netzwerk- und Systembetreiber zur Erfüllung ihrer Pflichten auf hinreichend sichere Hardware- und Software-Produkte angewiesen. Jedenfalls mittelbar übt das Datenschutzrecht somit auch auf die Komponentenhersteller Druck aus. In diesem Sinne „ermutigt" ErwGr 78 S. 4 DSGVO die Hersteller der Produkte, Dienste und Anwendungen, „das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen." Einen direkten Zugriff auf den Hersteller sieht die DSGVO jedoch nicht vor; der in Art. 25 Abs. 1 DSGVO fortwirkende Grundsatz des Art. 5 Abs. 1 lit. f DSGVO (Security by Design) kann daher nur indirekt, nämlich durch entsprechende Beschaffungsentscheidungen des Verantwortlichen, auf der Ebene der Komponentensicherheit zur Geltung gebracht werden.[241] Auch die Internetsicherheit kann durch das unionale

[238] Vgl. die hilfreiche Gegenüberstellung bei https://www.openkritis.de/IT-sicherheitsgesetz/eu-rce-direktive-kritis.html. Zu den Erweiterungen des Anwendungsbereichs im Detail *D.-K. Kipker/P. Birreck/M. Niewöhner/T. Schnorr*, NIS-Richtlinie und der Entwurf der NIS-2-Richtlinie, MMR 2021, S. 214 f.

[239] Siehe hierzu die Hinweise oben in § 6 Fn. 223 bis 227. Vertiefend auch *Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022, Rn. 361 ff.

[240] Vgl. *A. von dem Bussche/T. Schelinski*, Rechtsgrundlagen und Haftungsfolgen in der IT-Sicherheit, in: Leupold/Wiebe/Glossner (Hrsg.), IT-Recht, 4. Aufl. 2021, Teil 7.1, Rn. 51 ff. Zur Abgrenzung von § 19 TTDSG und § 8c BSIG siehe *Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022, Rn. 337 ff.

[241] Designvorgaben, wie sie Art. 25 DSGVO enthält, finden sich verschiedentlich im Umwelt- und Technikrecht sowie in jüngerer Zeit auch im Urheberrecht, vgl. *Specht*, Diktat

Datenschutzrecht allenfalls mittelbar beeinflusst werden, etwa indem die Nutzung bestimmter Verschlüsselungsprotokolle (etwa IPSec oder TLS) verpflichtend und so durch die datenschutzrechtlich Verantwortlichen über den Markt Nachfragedruck erzeugt wird.[242]

Ähnlich stellte sich die Problematik bislang auch im Recht der kritischen Infrastrukturen dar. Die von der Regulierung erfassten Betreiber waren zur Umsetzung der Sicherheitsanforderungen auf die Bereitstellung von sicherer Hardware und Software durch ihre Zulieferer angewiesen, die ihrerseits nicht Adressaten spezifischer regulatorischer Vorgaben waren. Zwar setzte das im IT-SiG 2015 angelegte Zertifizierungsregime gewisse Anreize für die Entwicklung sicherer Komponenten. Dennoch war das Reformgesetz insgesamt der berechtigten Kritik ausgesetzt, dass ein effektiver Schutz der besonders gefährdeten kritischen Infrastrukturen durch die isolierte Inpflichtnahme nur der KRITIS-Betreiber in Anbetracht der umfassenden technischen Vernetzung kaum gewährleistet werden konnte. Hier hat das IT-SiG 2.0 zu einem Perspektivwechsel geführt, indem es sich deutlich stärker den Aspekt der Komponentensicherheit und somit eine ganzheitliche Bestimmung der Aufgabe Informationssicherheit zu eigen gemacht hat. Diese Neuausrichtung kommt bereits in der reformulierten Aufgabenbestimmung des § 2 Abs. 2 BSIG 2021 zum Ausdruck. Diese verwies zuvor nur abstrakt auf die Schutzziele der Informationssicherheit. In der durch das IT-SiG 2.0 geänderten Fassung findet sich hier nun eine fast schon umfassende Beschreibung der Aufgabe Informationssicherheit, die auch die Komponenten- und Prozesssicherheit erwähnt und zudem ein deutlich konkreteres Handlungsprogramm als die Vorgängerfassung entwirft.[243] Inhaltlich wird die Komponentensicher-

---

der Technik, 2019, S. 175 ff. Regulierungstechnisch handelt es sich bei derartigen Vorgaben um eine Form des private enforcement. Dazu allgemein *Appel*, Das Verwaltungsrecht zwischen klassischem dogmatischen Verständnis und steuerungswissenschaftlichem Anspruch, in: VVDStRL 67 (2008), S. 226 (249); *K.-D. Drüen*, Indienstnahme Privater, 2012; *D. Poelzig*, Normdurchsetzung durch Privatrecht, 2012. Im Technologie-Kontext haben die damit verbundenen Fragestellungen v. a. durch den Aufstieg „smarter" Technologien, die in wesentlich größerem Umfang als früher zur Durchsetzung rechtlicher Pflichten genutzt werden können, Aufmerksamkeit auf sich gezogen, vgl. *T. Rademacher*, Wenn neue Technologien altes Recht durchsetzen, JZ 74 (2019), S. 702 ff.

[242] *J. Müller*, in: Koreng/Lachenmann (Hrsg.), Formularhandbuch Datenschutzrecht, 3. Aufl. 2021, E.II.2 Rn. 34, 38.

[243] Die jetzt in § 2 Abs. 2 S. 1 bis 3 BSIG 2021 ergänzte Passage lautet im Volltext: „Informationen sowie informationsverarbeitende Systeme, Komponenten und Prozesse sind besonders schützenswert. Der Zugriff auf diese darf ausschließlich durch autorisierte Personen oder Programme erfolgen. Die Sicherheit in der Informationstechnik und der damit verbundene Schutz von Informationen und informationsverarbeitenden Systemen vor Angriffen und unautorisierten Zugriffen im Sinne dieses Gesetzes erfordert die Einhaltung bestimmter Sicherheitsstandards zur Gewährleistung der informationstechnischen Grundwerte und Schutzziele."

heit[244] dann vor allem über den schon im ersten IT-SiG enthaltenen, nun aber erweiterten § 8b Abs. 6 BSIG konkretisiert, wonach das BSI die Hersteller betroffener Produkte und Systeme zur Mitwirkung an der Beseitigung oder Vermeidung einer Störung verpflichten kann, wobei sich hier in der Praxis komplexe Jurisdiktionsprobleme stellen dürften.[245] Griffiger ist die Regelung für Hersteller sogenannter „kritischer Komponenten" (§ 2 Abs. 13 BSIG 2021), für die dem BSI erweiterte Kontrollrechte eingeräumt werden (§§ 4a Abs. 1–3; 5a S. 1; 7a; 8f Abs. 1 Nr. 3 BSIG 2021); zu beachten ist insoweit auch der im Gesetzgebungsverfahren stark umstrittene § 9b BSIG 2021 („lex Huawei").[246] Letzterer verpflichtet KRITIS-Betreiber zur Anzeige des Einbaus kritischer Komponenten und gestattet dem BMI unter bestimmten Bedingungen, diesen zu untersagen. Die Breitenwirkung der Neuregelung wird allerdings durch das Erfordernis des § 2 Abs. 13 S. 1 Nr. 3 BSIG 2021, wonach die kritischen Komponenten je sektorspezifisch durch Gesetz oder auf Grund eines Gesetzes bestimmt werden, erheblich relativiert. So existiert eine entsprechende gesetzliche Regelung bisher auch nur im Telekommunikationssektor, §§ 165 Abs. 4; 167 Abs. 1 Nr. 2 TKG.[247]

Auch insoweit bewegt sich die NIS 2-RL auf den vom IT-SiG 2.0 eingeschlagenen Pfad. Im Unterschied zur Ursprungsfassung wird nun betont, dass über die Netzwerk- und Systemsicherheit hinaus auch Fragen der Komponentensicherheit zu berücksichtigen sind, wobei ein besonderer Fokus auf der „Sicherheit der Lieferkette" liegt (Art. 21 Abs. 2 lit. d und Abs. 3 NIS 2-RL). Dieser Aspekt ist nach Art. 7 Abs. 2 lit. a NIS 2-RL in den nationalen Cybersicherheitsstrategien verpflichtend zu verankern und ist von der „Kooperationsgruppe" durch Risikobewertungen zu unterstützen (Art. 22 NIS 2-RL).

Während auf diese Weise direkt und – vor allem – indirekt der Druck auf die für die Komponentensicherheit verantwortlichen Akteure erhöht wird, fällt es dem Gesetzgeber nach wie vor deutlich schwerer, Ansprechpartner für Fragen der Internetsicherheit zu identifizieren. Wie erwähnt entziehen sich zentrale Akteure wie die IETF bisher zumindest aus europäischer Sicht einem regula-

---

[244] Siehe hierzu auch die Legaldefinition in § 2 Abs. 9a BSIG 2021: „IT-Produkte im Sinne dieses Gesetzes sind Software, Hardware sowie alle einzelnen oder miteinander verbundenen Komponenten, die Informationen informationstechnisch verarbeiten".

[245] Entsprechend bereits für den insoweit ebenfalls einschlägigen § 5b Abs. 6 BSIG oben bei § 6 Fn. 119.

[246] Dazu im Überblick *Hornung*, Das IT-Sicherheitsgesetz 2.0, NJW 2021, S. 1985 (1987 f.). Kritisch zur Verfassungsmäßigkeit *K. F. Gärditz*, Stellungnahme zum Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme, 28.2.2021, A-Drs. 19 (4)741 E. Vertiefend *Schallbruch*, Das IT-Sicherheitsgesetz 2.0 (Teil I), CR 2021, S. 450 ff.; *Keppeler*, in: Ritter (Hrsg.), Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2022, § 9b BSIG Rn. 621 ff. Zur rechtspolitischen Debatte siehe die Nachweise oben § 1 Fn. 46.

[247] Siehe dazu unten § 6 Fn. 294.

torischen Zugriff. Stattdessen kann jedoch versucht werden, Einfluss auf jene Akteure zu nehmen, die die unter Sicherheitsgesichtspunkten relevanten Protokolle lokal implementieren, also insbesondere die Anbieter von Internet-Infrastrukturdiensten, etwa Netzbetreiber, Betreiber von BGP- und DNS-Servern, Zertifikatstellen, Betreiber von Internetknotenpunkten (etwa DE-CIX in Frankfurt am Main), Internet Service Provider etc., um auf diese Weise auf eine Erhöhung des Niveaus der Internetsicherheit hinzuwirken.[248] Auf die Maßnahmen, die in diese Richtung gehen, ist gleich noch gesondert einzugehen.[249]

d) Zwischenfazit

Im letzten Jahrzehnt hat der Gesetzgeber auf nationaler und auf Unionsebene die Verantwortungsarchitektur des Informationssicherheitsrechts stark ausdifferenziert und wesentlich über den ursprünglichen Kreis der Betreiber „physischer" kritischer Infrastrukturen ausgeweitet. Insbesondere in jüngster Zeit nimmt der Gesetzgeber zunehmend auch solche Akteure in den Blick, die zur Gewährleistung der Komponenten- und, eingeschränkt, der Internetsicherheit beitragen können. Die entsprechenden Ansätze sind noch zaghaft und nicht immer ideal implementiert. Doch auch wenn aktuell Maßnahmen wie § 9b BSIG zurecht der Kritik ausgesetzt sind, kommt die Informationssicherheitsregulierung auf Dauer an einer Verstärkung des Regulierungsdrucks in diesen Bereichen nicht vorbei.

5. Konkretisierung des Pflichtenprogramms für die Netzwerk- und Systemsicherheit

a) Verpflichtung zu technischen und organisatorischen Maßnahmen

Die Identifikation maßgeblicher Akteure und die Zuschreibung von Verantwortlichkeiten führt nur dann zur tatsächlichen Erhöhung des Informationssicherheitsniveaus, wenn dies mit einem konkreten Pflichtenprogramm hinterlegt wird. In der Tradition des Technikrechts enthält sich das Recht der Informationssicherheit insoweit weitgehend einer direkten Steuerung der technischen Sicherungsmaßnahmen und beschränkt sich auf abgestufte Investitions- und Organisationspflichten für die in Pflicht genommenen Hersteller und Betreiber. Investitionspflichten verlangen von den Verantwortlichen typischerweise, für die von ihnen angebotenen Dienste, Systeme, Netzwerke etc. Schutzvorkehrungen zu implementieren, die dem „Stand der Technik" entsprechen bzw.

[248] Zu diesen Akteuren siehe § 6 II. 1. b) cc).
[249] Siehe § 6 II. 7.

bestimmte Zertifizierungen aufweisen.[250] Gefordert ist insoweit, vereinfacht der Einsatz „branchenüblicher ‚Spitzenprodukte'".[251] Organisationspflichten umfassen beispielsweise die Ernennung interner Sicherheitsbeauftragten oder die Einführung eines Risikomanagementsystems.[252]

Erneut erweist sich das Recht der kritischen Infrastrukturen als Vorreiter für solche Regelungen. Bemerkenswert ist dabei das differenzierte Vorgehen des deutschen Gesetzgebers, was die Intensität der Verpflichtung betrifft. So verlangt Art. 14 Abs. 1 NIS-RL ganz allgemein, dass die Mitgliedstaaten von den Betreibern technische und organisatorische Maßnahmen verlangen, die „unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist". Umgesetzt wird dies durch § 8a Abs. 1 S. 1 BSIG, der verlangt, dass die Betreiber Kritischer Infrastrukturen, „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse […] treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind." Über die NIS-Richtlinie hinaus geht dann die in § 8a Abs. 1 Satz 2 BSIG enthaltene und an die KRITIS-Betreiber gerichtete Forderung, den Stand der Technik „einzuhalten".[253] Leicht abgeschwächt ist demgegenüber wiederum die Verpflichtung für Anbieter „digitaler Dienste" (Art. 14 ff. NIS-RL, § 2 Abs. 11 BSIG), die nach § 8c Abs. 2 BSIG den Stand der Technik

[250] Zur Figur des „Stands der Technik" siehe allgemein die Literatur bei § 5 III. 2. b) aa). Zur Unterscheidung zwischen den „anerkannten Regeln der Technik" und dem „Stand der Technik" bzw. dem nochmals anspruchsvolleren „Stand von Wissenschaft und Technik" grundlegend BVerfGE 49, 89 (136). Speziell zu dieser Rechtsfigur im Recht der Informationssicherheit siehe *P. Michaelis*, Cybersecurity: Technische Voraussetzungen der „Maßnahme" nach § 13 Abs. 7 TMG, ITRB 2016, S. 118 ff.; *ders.*, Der „Stand der Technik" im Kontext regulatorischer Anforderungen, DuD 2016, S. 458 ff.; *M. Knopp*, Stand der Technik, DuD 2017, S. 663 ff.; *D. Weidenhammer/R. Gundlach*, Wer kennt den „Stand der Technik"?, DuD 2018, S. 106 ff.

[251] So die griffige Formulierung bei *Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022, Rn. 269.

[252] Ein explizites Erfordernis zur Benennung eines Sicherheitsbeauftragten findet sich im Gesetz nur in § 166 Abs. 1 Nr. 1 TKG. Für „kritische" Energieunternehmen findet sich ein entsprechendes Erfordernis in *BNetzA*, IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz, August 2015. Laut *Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022, Rn. 623, gehört die Benennung eines entsprechenden Beauftragten jedoch zu den allgemeinen Compliance-Pflichten. Eine Pflicht zur Einführung eines IT-Risikomanagementsystems findet sich etwa in § 26 VAG. Zum Datenschutzrecht siehe gleich § 6 Fn. 257.

[253] Zur Begrifflichkeit *Roßnagel*, Das IT-Sicherheitsgesetz, DVBl. 2015, S. 1206 (1208). Laut Art. 14 Abs. 1, 2 NIS-RL sind hingegen die Betreiber „wesentlicher Dienste" unionsrechtlich nur verpflichtet, angemessene technische und organisatorische Maßnahmen zum Schutz der Sicherheit von Netzen und Informationssystemen *unter Berücksichtigung* des Stands der Technik zu schaffen. Die Anbieter „digitaler Dienste" (Art. 14 ff. NIS-RL; § 2 Abs. 11 BSIG) trifft wiederum sowohl nach Art. 16 Abs. 1 S. 2 NIS-RL wie nach § 8c Abs. 2 BSIG „nur" eine Berücksichtigungspflicht.

nur „berücksichtigen“ müssen.[254] Diese Umsetzung ist mit Art. 21 Abs. 1 NIS 2-RL nicht inkompatibel; insgesamt betont das Unionsrecht jetzt jedoch deutlich stärker, dass sich die Sicherheit der von der NIS-Regulierung erfassten Stellen je am konkreten Risiko orientieren muss, das nicht nur mit Blick auf die Auswirkungen für die betroffene Stelle selbst, sondern auch in seiner gesellschaftlichen Dimension zu bestimmen ist.[255] Dies hat sein Vorbild im Datenschutzrecht, das die für die Verarbeitung personenbezogener Daten verantwortlichen Stellen ebenfalls verpflichtet, „geeignete technische und organisatorische Maßnahmen“ zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 32 Abs. 1 DSGVO). Zur Konkretisierung wird dann nicht, wie noch bei § 9 S. 1 BDSG a. F., auf einen starren Maßnahmenkatalog verwiesen. Vielmehr ordnet Art. 32 Abs. 1 DSGVO nun an, dass der jeweilige „Stand der Technik“ zu „berücksichtigen“ ist; dies verlangt eine Einzelfallprüfung.[256] Zugleich führt die Norm verschiedene Regelbeispiele auf, die Leitlinien für die Formulierung des Stands der Technik darstellen.[257]

Analoge Vorgaben finden sich in weiteren sektorspezifischen Normen, etwa im TKG, das von den im Sektor Telekommunikation tätigen Unternehmen verlangt, im Einzelnen differenzierte Schutzvorkehrungen zu implementieren,[258] wobei der Stand der Technik wiederum zu „berücksichtigen“ ist (§ 165 Abs. 1 S. 2 TKG). Bestimmte Telekommunikationsnetzbetreiber dürfen zudem die schon erwähnten „kritischen Komponenten“ (§ 2 Abs. 13 BISG) nur nach vorheriger Zertifizierung einsetzen (§ 165 Abs. 4 TKG). In organisatorischer Hinsicht schreibt das TKG zudem explizit vor, dass Netzbetreiber oder Diensteanbieter Sicherheitsbeauftragte bestimmen und der BNetzA turnusmäßig ein Sicherheitskonzept vorlegen müssen (§ 166 TKG).[259] Auch aus allgemeinen Compliance-Vorgaben, wie sie für das Kapitalgesellschaftsrecht prägend sind (vgl. §§ 91 Abs. 2, 93 AktG, § 43 Abs. 2 GmbHG) lassen sich – zu-

[254] Dazu näher *Roßnagel*, IT-Sicherheitsgesetz, DVBl. 2015, S. 1206 (1208).

[255] Dazu gleich näher unter § 6 II. 5. c).

[256] Den Bedürfnissen der Praxis dürften allerdings die standardisierten Checklisten der Aufsichtsbehörden eher entgegenkommen, vgl. nur *Bayerisches Landesamt für Datenschutzaufsicht*, Good Practice bei technischen und organisatorischen Maßnahmen. Generischer Ansatz nach Art. 32 DS-GVO zur Sicherheit, 13.10.2020. Vgl. auch die Handreichung des Bundesverbands IT-Sicherheit e. V. (TeleTrusT), abrufbar unter https://www.teletrust.de/publikationen/broschueren/stand-der-technik/.

[257] Als organisatorische Maßnahme verlangt das Datenschutzrecht insbesondere die Benennung eines Datenschutzbeauftragten (Art. 37 ff. DSGVO, § 38 BDSG), der bzw. dem auch die Beratung und Überwachung des eigenen Unternehmens in Sachen IT-Sicherheit obliegt.

[258] Dazu gleich näher unter § 6 II. 5. c).

[259] Siehe auch §§ 6 Abs. 2 Nr. 2; 7 Abs. 2 Nr. 3; 9 Abs. 2 Nr. 3 AtG i. V. m der Bekanntmachung „Sicherheitsanforderungen an Kernkraftwerke“, sowie *Gehrmann/Voigt*, IT-Sicherheit, CR 2017, S. 93 (95 f.).

mindest in der Theorie – IT-sicherheitsbezogene Risikofrüherkennungs- und -verhinderungspflichten ableiten.[260]

b) Formen der Konkretisierung des Pflichtenprogramms („Stand der Technik")

Damit dieses Pflichtenprogramm durchgesetzt werden kann – sei es im Wege der behördlichen Überwachung und Kontrolle oder über das Haftungsrecht[261] –, müssen die unbestimmten Rechtsbegriffe konkretisiert werden. Dies geschieht in erster Linie durch technische Normungsinstanzen, deren Maßgaben aus verfassungsrechtlicher Sicht – wie gesehen – nicht unreflektiert in rechtliche Wertungen einfließen dürfen.[262]

Die diversen Akteure im Feld der Informationssicherheit können sich an einer (über-)großen Zahl technischer Normen orientieren.[263] Neben den nationalen Normungsgremien, dem Europäischen Komitee für Normung (CEN) und der Internationalen Organisation für Normung (ISO) sind insbesondere auch das Institute of Electrical and Electronics Engineers (IEEE) sowie, soweit Aspekte der Telekommunikationstechnik betroffen sind, der Telecommunication Standardization Sector innerhalb der Internationalen Fernmeldeunion (ITU-T) aktiv. In Sachen Internetsicherheit gelten zudem die bereits dargestellten RFC des IETF. Die Aktivitäten der vor allem im Feld der Komponenten- und Systemsicherheit tätigen nationalen und internationalen sektorübergreifenden Normungsinstitutionen – vor allem CEN, ISO und IEEE – begegnen jedenfalls dann keinen grundsätzlichen Bedenken, soweit sie sich innerhalb der durch das sog. New Legislative Framework definierten Rahmenbedingungen bewegen.[264] Die Aktivitäten des IETF können hingegen nach hiesigem Verständnis nicht für sich in Anspruch nehmen, demokratisch-rechtsstaatlichen Mindeststandards zu genügen.[265]

---

[260] Dazu *I. Conrad/S. Streitz*, Compliance, IT-Sicherheit, Ordnungsmäßigkeit der Datenverarbeitung, in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht 3. Aufl. 2019, § 33 Rn. 29 ff.; *von dem Bussche/Schelinski*, Rechtsgrundlagen und Haftungsfolgen in der IT-Sicherheit, in: Leupold/Wiebe/Glossner (Hrsg.), IT-Recht, 4. Aufl. 2021, Teil 7.1 Rn. 85 ff.; *Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022, Rn. 32 ff., 511 ff. Siehe *von dem Bussche/Schelinski*, a. a. O., Rn. 104 ff. und *Voigt*, a. a. O., Rn. 66 ff. auch zu den IT-sicherheitsrechtlichen Implikationen, die sich aus §§ 238 ff. HGB für die elektronische Buchführung ergeben.

[261] Zur Angewiesenheit des Haftungsrechts auf hinreichend bestimmte technische Standards siehe oben § 5 Fn. 138, 142.

[262] Siehe oben § 5 III. 2. b).

[263] Überblicksartig *Sohr/Kemmerich*, Technische Grundlagen der Informationssicherheit, in: Kipker (Hrsg.), 2020, Kap. 2 Rn. 203 ff.

[264] Dazu näher unter § 6 II. 6.

[265] Siehe oben § 5 Fn. 285.

Die Normungsgremien adressieren in ihren Normenreihen jeweils verschiedene Aspekte der Komponenten-, Netzwerk- und Systemsicherheit. Eine strikte Trennung nach den einzelnen Schichten ist nicht möglich, allerdings weisen die Normungsreihen Schwerpunkte auf. Übergeordnete Bedeutung für die Materie haben aus deutscher und europäischer Sicht insbesondere folgende Standards: Für die Sicherheit von (Software-)Komponenten ist die allgemeine Normenreihe ISO/IEC 25000 „Software engineering – Software product Quality Requirements and Evaluation (SQuaRE)" mit ihren Vorgaben zur Software-Qualität und Software-Entwicklung zentral.[266] Aus der ISO/IEC 27000-Reihe enthält ISO/IEC27001:2022 im Annex A allgemeine Vorgaben zur IT-Sicherheit in Entwicklungsprozessen.[267] Daneben existieren zahlreiche sektorspezifische Standards.[268] Für die System- und Netzwerksicherheit besonders relevant ist die ISO/IEC 27000-Reihe „Information Security Management Systems", die mehr als 20 Standards zum Management von Informationssicherheitsrisiken umfasst. Für Deutschland sind diese Standards vom BSI in Gestalt des IT-Grundschutzes umgesetzt.[269] Dessen Baustein „NET: Netze und Kommunikation" enthält etwa Vorgaben zur Konfiguration der Netzwerkkomponenten, zu infrastrukturbezogenen Aspekten (etwa zur Sicherheit von Routern oder Kabeln) sowie zum Netz- und Systemmanagement.[270]

Angesichts der verfassungsrechtlichen Sensibilität der Materie ist es zu begrüßen, dass der Gesetzgeber zunehmend detailliertere Vorgaben für die Re-

[266] Verantwortlich dafür ist das Normungsgremium ISO/IEC JTC 1/SC 07 (Software and systems engineering). Die deutsche Version „DIN ISO/IEC 25000 Software-Engineering – Qualitätskriterien und Bewertung von Softwareprodukten (SQuaRE)" wird betreut vom NA 043 Normenausschuss Informationstechnik und Anwendungen (NIA) des Deutschen Instituts für Normung (DIN). Zu den entsprechenden Aktivitäten des National Institute of Standards and Technology siehe SP 800–160 (https://csrc.nist.gov/publications/detail/sp/800–160/vol-1/final).

[267] Inhaltlich spiegelt sich dies im BSI-Grundschutz in Baustein CON.8: Software-Entwicklung, Februar 2021.

[268] Vgl. etwa für den Automobilsektor ISO 26262:2018 „Road vehicles – Functional safety".

[269] Zu den einschlägigen BSI-Standards (200–1: Managementsysteme für Informationssicherheit; 200–2: IT-Grundschutz-Methodik; 200–3: Risikomanagement; 100–4: Notfallmanagement) siehe die Dokumentation unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html.

[270] Als Beispiel für Standardmaßnahmen nennt *Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022, Rn. 268 in Anlehnung an die oben in § 6 Fn. 256 genannte Branchenempfehlung: Nutzung von Multi-Faktor-Authentifizierung; Verschlüsselung von Daten während des Transports und „at rest"; Einsatz sicherer Boot-Prozesse; sichere Software-Administration einschließlich Patch-Management; sichere Benutzer-Administration mit aktiver Sperrmöglichkeit durch den Administrator; Umsetzung von Logging-, Monitoring-, Reporting- und Response-Management-Systemen; Nutzung von Viren- und Malwareschutz; Nutzung von Back-up-Systemen.

zeption dieser und sonstiger Standards macht bzw. eine deutlich aktivere Rolle für staatliche Stellen bei der Konkretisierung der Pflichtenprogramme vorsieht.[271] Hinzu kommen die erwähnten praktischen Gründe, die gegen eine allzu offensive Verlagerung der Verantwortung für die Normsetzung auf technische Expertengremien sprechen. Denn private Standards sind keineswegs ein „Allheilmittel", sondern oft unspezifisch, inkohärent oder auch veraltet. So weisen die Adressaten eines Standards regelmäßig unterschiedliche Fähigkeiten und Risikoprofile auf: Ein globaler Standard kann daher für einzelne Betroffene eine unangemessene Belastung darstellen. So ist die Implementation von Standards teils aufwendig und eher von großen Unternehmen als von Start-ups oder KMUs zu leisten. Standardsetzung beeinflusst damit immer auch die Chancen am Markt. Schließlich ist die Trägheit des technischen Normungswesens zu bedenken. So hat sich dieses insgesamt erst spät der Informationssicherheit angenommen; gerade im Fall der Internetsicherheit wurde zudem übermäßig lange an alten und längst als unsicher erkannten Standards festgehalten.[272] Mehr noch als in anderen Bereichen der Technik stellt sich daher die Frage, inwieweit die traditionellen Normungsinstitutionen den Gesetzgeber bei der Regulierung von Informationssicherheit überhaupt effektiv unterstützen können.

Selbst wenn man dies bejaht, müssen die Nebenfolgen technischer Normen bei der „steuernden Rezeption" privaten Sachverstands durch das Recht berücksichtigt werden. Insoweit lassen sich im Recht der Informationssicherheit verschiedene Stufen der Einwirkung des Rechts auf den Normungsprozess unterscheiden.

Teils erfolgt eine grobe Vorsteuerung der notwendigen technischen und organisatorischen Maßnahmen bereits im Gesetz selbst. So führt der Regelbeispielkatalog des Art. 32 Abs. 1 DSGVO neben allgemeinen „Fähigkeiten", die IT-Systeme aufweisen sollen (lit. b und lit. c), mit der Pseudonymisierung und Verschlüsselung (lit. a) sowie dem turnusmäßigen Überprüfungsverfahren (lit. d) spezifische prozedurale und organisatorische Maßnahmen an, die aus Sicht des Gesetzgebers eine hinreichende Sicherheit von IT-Systemen garantieren können.[273] Die Beispiele sind technologieoffen formuliert, bedürfen also

---

[271] *Schallbruch*, IT-Sicherheitsrecht (Teil 1), CR 2017, S. 648 (649).

[272] Vgl. dazu *Brown/Marsden*, Regulating Code, 2013; *R. Ellis*, Regulating Cybersecurity, IEEE Security & Privacy 12:6 (2014), S. 48 ff. Zur Trägheit des im IETF organisierten technischen Sachverstands siehe § 6 II. 1. b) cc).

[273] So können fortwährend gewartete Backup-Systeme, Pseudonymisierungs- oder Verschlüsselungsmaßnahmen erforderlich sein. Diese Vorgaben werden in der Rechtsprechung zunehmend ernst genommen, vgl. etwa LG Würzburg, B. v. 13.9.2018, 11 O 1741/18 UWG, das aus Art. 32 Abs. 1 lit. a DSGVO folgert, ein Website-Betreiber müsse die mit Hilfe eines Kontaktformulars an ihn übermittelten Daten unter bestimmten Umständen durch SSL- oder TLS-Protokolle sichern. Dazu näher *R. Petrlic*, HTTPS im Lichte der DSGVO, DuD 2018, S. 691 ff. Siehe auch allgemein zu den Mindestschutzanforderungen nach Art. 32 DS-

noch der weiteren Konkretisierung, geben der technischen Normung jedoch zumindest eine Richtung vor. Entsprechende Vorgaben finden sich in § 64 Abs. 2 BDSG und § 8c Abs. 2 S. 2 BSIG.

Angesichts der sonst abweichenden Praxis ist die durch das IT-SiG 2.0 eingeführte Regelung des § 8a Abs. 1a BSIG 2021 in diesem Kontext bemerkenswert. Die Norm verpflichtet KRITIS-Betreiber, ab dem Jahr 2023 „Systeme zur Angriffserkennung" zu nutzen.[274] Diese Systeme werden dann in § 2 Abs. 9b S. 2 BSIG nicht technikneutral, sondern konkret über ihre Methode (Nutzung von Verfahren der Mustererkennung) charakterisiert.[275] Abweichend von den sonstigen Gepflogenheiten wird hier eine technische Detailregelung auf Gesetzesebene getroffen. Auch im Lichte der schlechten Erfahrungen mit § 9 BDSG a. F. erscheint dies als eine sehr spezifische, mit Blick auf künftige Entwicklungen der Sicherheitstechnik möglicherweise sogar hinderliche Festschreibung des gegenwärtigen technischen Entwicklungsstands.[276]

Ein anderer Weg besteht darin, die Konkretisierung des Stands der Technik ganz den Behörden zu übertragen. So weist etwa der durch das IT-SiG 2.0 eingefügte § 3 Abs. 1 S. 2 Nr. 20 BSIG dem BSI die Aufgabe zu, den Stand der Technik „bei sicherheitstechnischen Anforderungen an IT-Produkte unter Berücksichtigung bestehender Normen und Standards sowie Einbeziehung der betroffenen Wirtschaftsverbände" zu *beschreiben* und *veröffentlichen*.[277]

GVO *Müller*, in: Koreng/Lachenmann (Hrsg.), Formularhandbuch Datenschutzrecht, 3. Aufl. 2021, E.II., insbes. zu den Dimensionen Zugangs-, Zutritts-, Zugriffs-, Trennungs-, Weitergabe-, Eingabe-, Verfügbarkeitskontrolle sowie Belastbarkeit und Überprüfungsverfahren.

[274] Entsprechend für KRITIS-Betreiber aus dem Sektor Energie: § 11 Abs. 1d EnWG.

[275] Der Betrieb der Systeme wird auf Seiten des BSI durch die das Informationssystem Malware Information Sharing Platform (MISP) unterstützt, vgl. *Deutscher Bundestag*, Gesetzesentwurf der Bundesregierung zum IT-SiG 2.0, BT-Drs. 19/26106, S. 79.

[276] Abgewogen *Hornung*, Das IT-Sicherheitsgesetz 2.0, NJW 2021, S. 1985 (1987). Siehe auch *Keppeler/Schulte*, in: Ritter (Hrsg.), Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2022, § 2 BSIG Rn. 116, sowie *Schulte*, in: a. a. O., § 8a BSIG Rn. 467 ff., zu weiterhin bestehenden technischen Spielräumen.

[277] Bei der Auslegung des § 3 Abs. 1 Nr. 20 BSIG ist zu berücksichtigen, dass die Norm mit dem Begriff „Stand der Technik" auf einen eindeutig und anspruchsvoll definierten Rechtsbegriff Bezug nimmt, der als „der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen, der nach herrschender Auffassung führender Fachleute das Erreichen des gesetzlich vorgegebenen Zieles gesichert erscheinen lässt", beschrieben wird (vgl. *Bundesministerium der Justiz*, Handbuch der Rechtsförmlichkeit, 3. Aufl. 2008, B.4.5, Rn. 252 ff.; entsprechend bereits BVerfGE 49, 89 [135]). Wenn daher § 3 Abs. 1 Nr. 20 BSIG bei der Ermittlung des Stands der Sicherheitstechnik auch die „Berücksichtigung bestehender Normen und Standards sowie Einbeziehung der betroffenen Wirtschaftsverbände" verlangt, formuliert dies nur zusätzliche Anforderungen, entbindet Behörden und Gerichte jedoch nicht davon, in die „Meinungsstreitigkeiten der Techniker ein[zu]treten, um zu ermitteln, was technisch notwendig, geeignet, angemessen und vermeidbar ist" (vgl. BVerfGE 49, 89 [136]). § 3 Abs. 1 Nr. 20 BSIG senkt daher die Anforderungen an den Stand der Technik nicht auf den Standard ab, den betroffene Wirtschaftsverbände für vertretbar halten, sondern verlangt über die Auseinandersetzung mit der Fachliteratur hinaus zusätzliche Ermittlungsschritte.

Die Behörde definiert also nicht selbständig den Stand der Technik, sondern konsolidiert und publiziert diesen, was angesichts der zersplitterten Normungslandschaft für die Rechtsunterworfenen eine erhebliche Erleichterung darstellen kann. Ähnlich enthält auch der auf Art. 16 Abs. 8 NIS-RL gestützte Durchführungsrechtsakt der Kommission (vgl. § 8c Abs. 2 S. 3 BSIG) technische und organisatorische Vorgaben, die sich als Destillat der einschlägigen technischen Normen darstellen sollen (vgl. jetzt Art. 21 Abs. 5 NIS 2-RL).[278] Der Regierungsentwurf zu § 3 Abs. 1 S. 2 Nr. 20 BSIG hatte noch weitergehend vorgesehen, dass das BSI den Stand der Technik selbständig *entwickeln* sollte, was bedeutet hätte, dass das Amt auch über den Stand der sachverständigen Diskussion hätte hinausgehen können.[279] Schon die Konsolidierung des Stands der Technik erscheint jedoch angesichts der Breite der für IT-Produkte einschlägigen Normungslandschaft als eine durchaus komplexe Aufgabe. Die jetzt gewählte Fassung ist daher unter funktionalen Gesichtspunkten deutlich vorzugswürdig.[280]

Für einzelne Themenfelder wird den Fachbehörden teils jedoch durchaus die eigenständige Entwicklung von Standards für technische und organisatorische Maßnahmen oder zumindest die Mitarbeit an entsprechenden Vorhaben zugemutet. So ist dem BSI ganz allgemein die „Entwicklung von Kriterien, Verfahren und Werkzeugen für die Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen oder Komponenten und für die Prüfung und Bewertung der Konformität im Bereich der IT-Sicherheit" (§ 3 Abs. 1 S. 2 Nr. 4 BSIG) sowie die Ausarbeitung technischer Richtlinien (§ 3 Abs. 1 S. 2 Nr. 6; § 9c Abs. 3 BSIG) aufgegeben; zahlreiche Fachgesetze etwa aus dem Migrations- und Gesundheitsrecht konkretisieren diesen Auftrag dann vor allem für die bislang noch nicht vom NIS-Regime bzw. den §§ 8a ff. BSIG erfasste öffentliche Verwaltung.[281] Das BSI selbst pflegt derzeit mehr als 50 solcher

[278] Vgl. Durchführungsverordnung (EU) 2018/151 der Kommission vom 30.1.2018, ABl. L 26/48. Art. 2 Abs. 5 der Durchführungsverordnung konkretisiert den in Art. 16 Abs. 1 lit. e NIS-RL enthaltenen Hinweis auf die „internationalen Normen" durch den Verweis auf Art. 2 Abs. 1 lit. a der für die Architektur des „new legislative framework" zentralen VO (EU) 1025/2012. Solche Durchführungsrechtsakte existieren auch für einzelne Sektoren, vgl. etwa zum Stand der Technik von Sicherungsanforderungen bei Vertrauensdiensten im Sinne der eIDAS-Verordnung die Durchführungsverordnung (EU) 2015/1502 vom 8.9.2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Art. 8 Abs. 3 eIDAS-Verordnung, ABl. L 235/7.

[279] *Bundesregierung*, (Zweiter) Referentenentwurf zum IT-SiG 2.0, 11.12.2020, S. 7. Vgl. zur in den Anhörungen geäußerten Kritik *Schulte*, in: Ritter (Hrsg.), Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2022, § 3 BSIG Rn. 169 m. w. N.

[280] *Schallbruch*, IT-Sicherheitsrecht (Teil 1), CR 2017, S. 648 (649).

[281] Hier sind nun durch die Einbeziehung der öffentlichen Verwaltung in die NIS 2-RL Änderungen zu erwarten.

Richtlinien,[282] deren Berücksichtigung teilweise durch Gesetz angeordnet wird (vgl. beispielsweise § 64 Abs. 1 S. 2 BDSG). Vielfach werden Fachbehörden bei der Erstellung von Richtlinien zur IT-Sicherheit zur Zusammenarbeit mit dem BSI verpflichtet (vgl. beispielsweise §§ 75b; 75c; 139 Abs. 10 und 11; 303c; 311 Abs. 2 und 6 SGB V). Besondere Bedeutung für das Recht der kritischen Infrastrukturen hat etwa auch der nach §§ 11 Abs. 1a und 1b EnWG durch die BNetzA im Benehmen mit dem BSI zu erstellende Katalog von Sicherheitsanforderungen für „kritische" Energieunternehmen.[283] Für die Kreditwirtschaft haben die Rundschreiben der BaFin eine entsprechende Funktion.[284] Große Breitenwirkung haben schließlich das von den Datenschutzaufsichtsbehörden von Bund und Ländern entworfene Standard-Datenschutzmodell (SDM), das in enger Anlehnung an den vom BSI gepflegten IT-Grundschutz auch Vorgaben zur Konkretisierung der geeigneten technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO macht.[285] Ein eigenständiges Tätigwerden der Fachbehörden dürfte allerdings insbesondere dort sinnvoll und geboten sein, wo Materien für die allgemeinen technischen Normungsorganisationen zu speziell sind. Dies betrifft in erster Linie solche Fragen, die sich aus den spezifischen Sicherheitsbedarfen staatlicher Stellen selbst ergeben und die daher in allgemeinen technischen Normen nur selten thematisiert werden. Gegenüber solchen speziell auf die (national-)staatlichen Bedürfnisse ausgerichteten Kriterienkatalogen tragen auch die Einwände, die sonst aus Sicht der Waren- und Dienstleistungsfreiheit gegen derart partikulare Standards auf der Hand liegen, nicht.

Einen produktiven Mittelweg zwischen der staatlichen Festsetzung und der privat-kollaborativen Findung technischer Standards weist schließlich das in § 8a Abs. 2 BSIG für die KRITIS-Sektoren vorgeschriebene Verfahren vor, wonach die Betreiber Kritischer Infrastrukturen und ihre Branchenverbände branchenspezifische Sicherheitsstandards (B3S) vorschlagen können, deren Tauglichkeit das BSI auf Antrag prüft und gegebenenfalls unter Beteiligung

[282] Vgl. die Darstellung der einschlägigen Richtlinien unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr-nach-thema-sortiert_node.html. Hierzu zählen bspw. die Technischen Richtlinien zu kryptographischen Verfahren (BSI TR-02102) oder die Technische Richtlinie zu „Secure Broadband Router" (BSI TR-03148).

[283] Dazu *Gehrmann/Voigt*, IT-Sicherheit, CR 2017, S. 93 (96).

[284] *BaFin*, Mindestanforderungen an das Risikomanagement (MaRisk), Rundschreiben 10/2021 in der Fassung vom 16.8.2021; *dies.*, Bankaufsichtliche Anforderungen an die IT (BAIT), Rundschreiben 10/2017 in der Fassung vom 16.8.2021; *dies.*, Zahlungsdiensteaufsichtliche Anforderungen an die IT von Zahlungs- und E-Geld-Instituten (ZAIT), Rundschreiben 11/2021 in der Fassung vom 16.8.2021.

[285] *Datenschutzkonferenz*, Das Standard-Datenschutzmodell (Version 2.0b), 17.4.2020, S. 59 f. Der BSI Standard 200–2 verweist im Übrigen seinerseits zurück auf das SDM.

weiterer Behörden durch Verwaltungsakt feststellt.[286] Dieses Verfahren, das Ähnlichkeiten mit Art. 40, 41 DSGVO aufweist, trägt der kooperativen Tradition des Rechtsgebiets Rechnung: Die unterschiedlichen Perspektiven und Funktionalitäten von Unternehmen und Behörden werden auf diese Weise produktiv miteinander gekoppelt.[287]

Abschließend ist in diesem Zusammenhang Art. 19 NIS-RL (jetzt: Art. 25 NIS 2-RL) zu nennen, der die Mitgliedstaaten der Union ganz allgemein auffordert, die Aktivitäten der europäischen und internationalen Normungsorganisationen im Feld der IT-Sicherheit zu fördern und ENISA die Aufgabe überträgt, insoweit koordinierend tätig zu werden. Konkreteres ergibt sich hieraus jedoch nicht.

c) Risikobasierter Ansatz

Als Erscheinungsform sowohl des Technik- wie des „neuen" Sicherheitsrechts ist das Recht der Informationssicherheit im Kern Risikorecht.[288] Auch die grundrechtliche Verortung der Materie in der staatlichen Gewährleistungsverantwortung für die Risiken der Technik legt ein risikobasiertes Vorgehen nahe.[289] Dementsprechend knüpfen die Vorgaben der NIS-RL und des BSIG explizit an die Kritikalität der Infrastrukturbetreiber, mithin an das von ihnen ausgehende Risiko für Staat und Gesellschaft an (vgl. Art. 14 Abs. 1 NIS-RL; Art. 21 Abs. 1 NIS 2-RL; §§ 2 Abs. 10 S. 1 Nr. 2; 10 Abs. 1 BSIG; BSI-KritisV). Das abgeschwächte Pflichtenprogramm, das für die Regulierung der Unternehmen im besonderen öffentlichen Interesse (§§ 8f; 2 Abs. 14 BSIG) greift, trägt deren typischerweise geringerer, aber immer noch substanzieller Risikostruktur Rechnung. Für die sehr breite Gruppe der Anbieter digitaler Dienste i. S. d. § 2 Abs. 11, 12 BSIG, deren IT-Systemen kein abstrakt erhöhtes Risiko zugeschrieben werden kann, schreibt § 8c Abs. 2 S. 1 BSIG konsequenterweise vor, dass notwendige „Maßnahmen zur Bewältigung von Risiken für die Sicherheit der Netz- und Informationssysteme […] unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten [müssen], das dem bestehenden Risiko angemessen ist." Hier muss also eine Risikobeurteilung im Einzelfall vorge-

[286] Vgl. die Übersicht über die Branchenstandards unter https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Stand-der-Technik-umsetzen/Uebersicht-der-B3S/uebersicht-der-b3s_node.html.

[287] Hierzu aus U.S.-Sicht instruktiv *D. Thaw*, The Efficacy of Cybersecurity Regulation, Georgia State U. L. Rev. 30 (2014), S. 287 ff. Zur Rolle privater Standards für die Cybersicherheit des Finanzsektors siehe *Calliess/Baumgarten*, Cybersecurity in the EU, German L. J. 21 (2020), S. 1149 (1159 ff.).

[288] Zum rechtlichen Risikobegriff ausführlich oben § 3 II. 2. und § 4 I. 2. b).

[289] Siehe oben § 5 II. 2.

nommen werden. Dies folgt auch aus der in allen genannten Vorschriften enthaltenen Maßgabe, (nur) „angemessene" Maßnahmen zu implementieren, wobei diese Klausel im konkreten Fall nicht als Schutz der Unternehmen vor einer übermäßigen, vor allem finanziellen, Belastung verstanden werden darf – diesen Zweck erfüllen im BSIG die Schwellenwerte –, sondern sicherstellen soll, dass unter dem Gesichtspunkt der Versorgungssicherheit Aufwand und Ertrag einer Umsetzungsmaßnahme nicht außer Verhältnis stehen (vgl. Art. 21 Abs. 1 S. 3 NIS 2-RL).[290]

Auch das europäisierte Datenschutzrecht folgt dort, wo es um Belange der Informationssicherheit geht, klar dem risikobasierten Ansatz.[291] So macht die DSGVO die Auswahl der aus Sicherheitsgründen geforderten technischen und organisatorischen Maßnahmen nicht nur vom „Stand der Technik", sondern explizit auch von der „Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen" abhängig (Art. 32 Abs. 1 DSGVO), was Spielräume bei der Umsetzung im Einzelfall eröffnet, zugleich aber auch aus Sicht der Regulierungsadressaten die Vorhersehbarkeit des Regulierungsprogramms erschwert.[292]

Wenn der Gesetzgeber auf diese Weise das Pflichtenprogramm risikoorientiert und kontextspezifisch ausgestaltet, ist das im Lichte sowohl der auf Unternehmensseite betroffenen Grundrechte als auch der divergierenden technischen Gefährdungssituationen zwingend. Damit wird zugleich der Vorstellung eine Absage erteilt, das materielle Informationssicherheitsrecht ließe sich als Kanon von allgemeingültigen Pflichten darstellen.[293] Folge dessen ist aller-

[290] Weniger eindeutig formuliert dies § 8a Abs. 1 S. 3 BSIG, der allerdings richtigerweise aus Sicht der Betreiber restriktiv zu interpretieren ist, vgl. *Schulte*, in: Ritter (Hrsg.), Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2022, § 8a BSIG Rn. 464 f. Zum großzügigeren Maßstab des Datenschutzrechts, der eine Berücksichtigung der Implementationskosten gestattet, siehe *Martini*, in: Paal/Pauly (Hrsg.), DS-GVO, 3. Aufl. 2021 Art. 32 Rn. 60 f.; a. A. allerdings *Hansen*, in: S. Simitis/G. Hornung/I. Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 32 DSGVO Rn. 21.

[291] *Petri*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 24 DSGVO Rn. 11 ff. Zur Diskussion, ob die DSGVO auch allgemein einem „rights-based" oder einem „risk-based approach" folgt, vgl. die Nachweise oben in § 5 Fn. 202.

[292] Vgl. *Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022, Rn. 193, 199. Zu der von der oben erwähnten Thematik zu unterscheidenden Diskussion, ob die von Art. 32 DSGVO verlangten Standards durch Vereinbarung zwischen der betroffenen Person und dem Verantwortlichen unterschritten werden können, die in dieser Schärfe nur in dem zwischen subjektiver und objektiver („Systemdatenschutz") Fundierung changierenden Datenschutzrecht stellt, näher *Martini*, in: Paal/Pauly (Hrsg.), DS-GVO, 3. Aufl. 2021 Art. 32 Rn. 4a ff.; sowie restriktiv *S. Jandt*, in: Kühling/Buchner (Hrsg.), DS-GVO, 3. Aufl. 2020, Art. 32 Rn. 40. Aus der aufsichtsbehördlichen Praxis vgl. die rechtlich überzeugenden Stellungnahmen von *DSK*, Beschluss vom 24. November 2021, Ziff. 1; *Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit*, Vermerk: Abdingbarkeit von TOMs (Art. 32 DSGVO), 24.11.2021.

[293] *Freimuth*, Gewährleistung der IT-Sicherheit Kritischer Infrastrukturen, 2018, S. 373 f.

dings, dass sich der Gesetzgeber zumindest grob mit den jeweiligen Risikostrukturen vertraut macht. Als Beispiel hierfür kann das Telekommunikationsrecht dienen, das ein nach unterschiedlichen Risikoprofilen abgestuftes Pflichtenprogramm entwickelt. So verpflichtet das Telekommunikationsrecht zunächst *alle* Erbringer von Telekommunikationsdiensten zur Implementierung von „angemessenen" Schutzvorkehrungen, wobei der Stand der Technik „zu berücksichtigen" ist (§ 165 Abs. 1 S. 2 TKG). Für die unter IT-Sicherheitsgesichtspunkten deutlich sensiblere Untergruppe der Betreiber öffentlicher Telekommunikationsnetze oder öffentlich zugänglicher Telekommunikationsdienste werden dann weiterreichende risikominimierende Vorgaben zum Schutz gegen alle Arten von Störungen, die zu erheblichen Beeinträchtigungen führen können, verlangt, wobei als Regelbeispiel Verschlüsselungspflichten angeführt werden (§ 165 Abs. 2 TKG); auch die Verfügbarkeit der Netze muss gewährleistet sein (§ 165 Abs. 5 TKG). Jener Teil der in § 164 Abs. 2 TKG genannten Unternehmen, die ein erhöhtes Gefährdungspotential aufweisen, wird schließlich zum Einsatz von Systemen zur Angriffserkennung verpflichtet (§ 165 Abs. 3 TKG); welche Unternehmen erfasst sind sowie weitere Details zu den einzusetzenden Systemen, legen BNetzA, BSI und BfDI fest (§ 167 Abs. 1 S. 1 TKG).[294] „Kritische Komponenten" im Sinne von § 2 Abs. 13 BSIG dürfen Telekommunikationsnetzbetreiber schließlich nur nach vorheriger Zertifizierung einsetzen (§ 165 Abs. 4 TKG). Auch wenn man sich hier über Details streiten kann, hat sich der Gesetzgeber erkennbar um eine weitgehende Vorstrukturierung der Risikobewertung bemüht und ist insoweit seiner Gewährleistungsverantwortung für die IT-Sicherheit im Telekommunikationssektor gerecht geworden.

d) Zwischenfazit

Mittels Generalklauseln oder Delegation an Verwaltung, Gerichte oder private Normungsinstanzen will der parlamentarische Gesetzgeber typischerweise nicht nur dem Wissensproblem, sondern auch der Dynamik der technologischen Entwicklung Rechnung tragen. Im Falle der IT-Sicherheit geht diese Kalkulation allerdings nur teilweise auf. Denn private Akteure haben dort typischerweise nur geringe Anreize für ein über die Sicherung des eigenen Bereichs hinausgehendes Engagement.[295] Auch das technische Normungswesen erweist sich als eher träge.

Das heißt nicht, dass das Recht nicht weiterhin die Kommunikation mit der Technik suchen sollte. Allerdings zeigt die Detailanalyse, dass die Gegenüber-

[294] Dazu im Detail *BNetzA*, Katalog von Sicherheitsanforderungen, Stand: 29.4.2020; *dies*, Liste der kritischen Funktionen, Stand: 18.8.2021.

[295] Zur IT-Sicherheit als „öffentlichem Gut" siehe § 6 II. 3. a).

stellung von technischer Dynamik und Statik des Rechts, ein alter Topos der Rechtskritik, in die Irre führt. Ohnehin ist es kein Zeichen für die Überforderung des Rechtssystems, wenn dieses zunächst abwartet, bis technische Entwicklungen negative Folgen zeitigen, die die Gesellschaft selbst nicht mehr in den Griff bekommt.[296] Vielmehr ist es das für ein freiheitliches Gemeinwesen unter üblichen Bedingungen angemessene Vorgehen.[297] Auch darf nicht übersehen werden, dass das Parlamentsgesetz als Instrument flexibel und konstitutiv auf Veränderbarkeit hin ausgelegt ist.[298]

Umgekehrt sind aber eben auch Technik und Gesellschaft nicht notwendig besonders dynamisch. Dies schließt die gesellschaftlichen Gewohnheiten im Umgang mit der Technik ein. Zahlreiche Sicherheitsprobleme der digitalen Technik rühren nicht nur daher, dass ein Großteil der digital vermittelten Kommunikation auf Architekturen basiert, die in den 1960er- bis 1980er-Jahren ohne Rücksicht auf mögliche Folgen für die Informationssicherheit implementiert wurden. Vielmehr sind bestimmte mit diesen Normen verbundene Eigenschaften des Internets – insbesondere seine Generativität, die für eine Dynamik auf der Ebene der Anwendungen sorgt[299] – so tief verwurzelt, dass rein privat, d. h. ohne rechtliche Absicherung initiierte Versuche zur Erhöhung des Sicherheitsniveaus an der Trägheit der Nutzer scheitern.[300]

Statt rechtliche Statik und gesellschaftliche Dynamik antagonistisch einander gegenüberzustellen, gilt es daher, die Wechselbezüge herauszuarbeiten. So müssen, um die gesellschaftliche Dynamik zu entfalten, vielfach auch die Mittel des vermeintlich trägen und statischen (Gesetzes-)Rechts genutzt werden. Im Recht der Informationssicherheit erfolgt dies etwa dadurch, dass der Staat selbst Normungsverfahren initiiert oder sich daran beteiligt, am klarsten wohl in dem gerade angeführten Verfahren halbstaatlicher Standardsetzung nach

[296] Klar dazu *Schulze-Fielitz*, Technik und Umweltrecht, in: Schulte/Schröder (Hrsg.), Handbuch des Technikrechts, 2011, S. 455 (463 f.), der darauf hinweist, dass Recht auch „zu früh" erlassen werden kann und dann dysfunktionale Regelungen trifft. Zur Thematik weiter bereits *W. Berg*, Vom Wettlauf zwischen Recht und Technik, JZ 40 (1985), S. 401 ff.

[297] Vgl. aber etwa *Wolf*, Der Stand der Technik, 1986, S. 265 ff.; *ders.*, Zur Antiquiertheit des Rechts in der Risikogesellschaft, Leviathan 15 (1987), S. 357 ff.

[298] Dazu im Kontext der Technikregulierung bereits *D. Murswiek*, Dynamik der Technik und Anpassung des Rechts, in: Ziemske (Hrsg.), FS Kriele, 1997, S. 651 ff.; *H. Schulze-Fielitz*, Zeitoffene Gesetzgebung, in: Hoffmann-Riem/Schmidt-Aßmann (Hrsg.), Flexibilität und Innovationsoffenheit im Verwaltungsrecht, 1994, S. 139 ff.; *Vec*, Kurze Geschichte des Technikrechts, in: Schulte/Schröder (Hrsg.), Handbuch des Technikrechts, 2. Aufl. 2011, S. 3 (80 ff.). Ein Plädoyer für die Stärkung des allgemeinen Gesetzes in Zeiten der Digitalisierung bei *H. Kube*, E-Government: Ein Paradigmenwechsel in Verwaltung und Verwaltungsrecht?, in: VVDStRL Bd. 78 (2019), S. 289 (314 ff.).

[299] Dazu nur *J. Zittrain*, The Generative Internet, Harv. L. Rev. 119 (2006), S. 1974 ff.; *B. van Schewick*, Internet Architecture and Innovation, 2010, S. 285 ff.

[300] Zu den bestenfalls gemischten Erfolgen der sicherheitsorientierten Änderungen der grundlegenden Internet-Protokolle siehe oben § 6 II. 1. b) cc).

§ 8a Abs. 2 BSIG, oder indem er auf den ohnehin stets in dynamischer Entwicklung befindlichen Stand der Technik Bezug nimmt.[301] Aber nicht nur bei der Netzwerk- und Systemsicherheit, auch bei der Komponentensicherheit sind diese Zusammenhänge zu bedenken.

6. Konkretisierung des Pflichtenprogramms für die Komponentensicherheit

a) Komponentensicherheit als neues Aufmerksamkeitsfeld des Informationssicherheitsrechts

Auch wenn DSGVO und IT-SiG 2.0 den Blick von der Netzwerk- und Systemsicherheit auf die Komponentensicherheit erweitert haben und erste Vorgaben für die Hersteller von IT-Produkten enthalten,[302] sind die entsprechenden Pflichtenprogramme nach wie vor eklektisch. So erfolgt der Zugriff auf die Hersteller im Recht der kritischen Infrastrukturen schon mit Blick auf das Regulierungsziel in erster Linie indirekt über die System- und Netzwerkbetreiber und gibt nur in Sonderkonstellationen eindeutige Lösungen vor (vgl. §§ 8b Abs. 6, 9b BSIG). Auch im Datenschutzrecht, das zwar ganz allgemein nach einer Minimierung möglicher Persönlichkeitsgefährdungen strebt und mit Art. 25 DSGVO eine Regelung mit unmittelbarem Produktbezug enthält, steht über Art. 32 DSGVO bisher der Systemschutz ganz im Vordergrund.

Die Gründe dafür, dass die Komponentensicherheit lange Zeit regulatorische *terra incognita* war, unterscheiden sich nicht grundsätzlich von jenen, die ganz allgemein für die langsame Verrechtlichung der Informationssicherheit verantwortlich sind: Unklarheit über die Verantwortlichkeiten, Unsicherheit über die Möglichkeit eines territorialen Zugriffs sowie ungenügendes Regulierungswissen. Allerdings ist das Feld der mit Fragen der Komponentensicherheit befassten Akteure nochmals größer und viel diffuser als das der Betreiber kritischer Infrastrukturen, die sich durch die Festlegungen der KritisV eindeutig definieren und zielgenau adressieren lassen. Auch dürfte die Sensibilität der Komponentenhersteller für die Risiken ihrer Tätigkeit und, damit verbunden, ihr Verständnis für regulatorische Vorgaben, deutlich geringer sein, als dies jedenfalls mittlerweile bei den für die Verarbeitung personenbezogener Daten verantwortlichen Stellen und bei KRITIS-Betreibern der Fall ist. Bevor hier ambitionierte regulatorische Agenden verfolgt werden können, muss daher

[301] Zum dynamischen Gehalt des Art. 32 Abs. 1 DSGVO, der zu einer stetigen Anpassung der geforderten technischen und organisatorischen Sicherungsmaßnahmen zwingt, siehe *Martini*, in: Paal/Pauly (Hrsg.), DS-GVO, 3. Aufl. 2021, Art. 32 Rn. 56 ff.; *Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022, Rn. 199.

[302] Siehe oben § 6 II. 4. c) bb).

zunächst einmal ein tauglicher Regulierungsrahmen etabliert werden. Dazu sind in jüngster Zeit einige wesentliche Schritte erfolgt.

b) Der EU Cybersecurity Act (CSA) als risikobasierte Rahmenregelung für Zertifizierungen

Wichtiges Vorbild für eine Regulierung, die auf Stärkung des Sicherheitsniveaus von IT-Komponenten zielt, ist das Recht der Produktsicherheit. Allerdings konzentriert sich diese Materie traditionell ganz auf physische Produkte und auf den Schutz der körperlichen Integrität.[303] Um einen Beitrag zur Informationssicherheit zu leisten, muss der Rechtsrahmen daher entsprechend fortentwickelt werden.

Das unionale Recht der Produktsicherheit, ein zentraler Pfeiler zur Sicherung der Warenverkehrsfreiheit und damit des Binnenmarktes, hat sich in drei Schritten entwickelt.[304] Zunächst wurden Anforderungen an die Sicherheit bestimmter Produkte detailliert in Rechtsakten festgelegt; für deren Durchführung und für die Konformitätsprüfung der Produkte waren die mitgliedstaatlichen Behörden zuständig. In einzelnen Sachbereichen findet sich dieses „alte Konzept" heute noch. Nach längeren Reformdebatten wurde im Jahr 1985 das sog. „neue Konzept" (New Approach) auf den Weg gebracht.[305] Danach wurden per Rechtsakt nur noch die „wesentlichen Anforderungen" für ein Produkt festgelegt; deren detaillierte Ausformung erfolgte dann in Form harmonisierter europäischer (technischer) Normen.

Im Anschluss widmete sich der Unionsgesetzgeber intensiv der Entwicklung eines Rechtsregimes für solche Konformitätsbewertungen und dem Aufbau einer leistungsfähigen europäischen Normungsinfrastruktur.[306] In den 2000er-Jahren wurde das „neue Konzept" dann zum „neuen Rechtsrahmen"

---

[303] *Leisterer*, Internetsicherheit in Europa, 2018, S. 109. Grundlegend zum Produktsicherheitsrecht *H. Weiß*, Produktsicherheit, 2008; *Röthel*, Europarechtliche Vorgaben, in: Schulte/Schröder (Hrsg.), Handbuch des Technikrechts, 2011, S. 201 ff.; *F.-J. Peine*, Gerätesicherheitsrecht, in: a. a. O., S. 405 ff.; *D. Gauger*, Produktsicherheit und staatliche Verantwortung, 2015; *T. Klindt/C. Schucht*, Technikrecht, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht, Bd. 1, 4. Aufl. 2019, § 36.

[304] Zum Folgenden detailliert *Europäische Kommission*, Bekanntmachung – Leitfaden für die Umsetzung der Produktvorschriften der EU 2016 („Blue Guide"), ABl. 2016/C 272/01, S. 5 ff.; *Klindt/Schucht*, Technikrecht, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht, Bd. 1, 4. Aufl. 2019, § 36 Rn. 48.

[305] Auslöser der Reform waren auch die Ausführungen in EuGH, 120/78 v. 20.2.1979 – Rewe-Zentral AG („Cassis de Dijon"), wonach Verbote oder Beschränkungen von Produkten aus anderen Mitgliedstaaten nur mit der mangelnden Konformität in „wesentlichen Anforderungen" begründet werden durften.

[306] Vgl. jetzt Verordnung (EU) Nr. 1025/2012 vom 25.10.2012 zur europäischen Normung.

(New Legislative Framework) weiterentwickelt.[307] Dieser verfeinerte das „neue Konzept" und enthielt umfangreiche Vorgaben zur Konformitätsbewertung, Akkreditierung und Marktüberwachung, einschließlich der Überprüfung von Produkten aus Drittländern. Geregelt wurde ferner die CE-Kennzeichnung. Umgesetzt wurden diese Rechtsakte durch das Produktsicherheitsgesetz (ProdSG), das zum 1.12.2011 das Geräte- und Produktsicherheitsgesetz (GPSG) ersetzte.

Inhaltlich gefüllt wird der „neue Rechtsrahmen" durch mehr als zwanzig darauf abgestimmte, je auf spezielle Produktarten bzw. Sektoren spezialisierte Verordnungen und Richtlinien, darunter die für IT-Produkte besonders relevanten Richtlinien 2014/35/EU (Niederspannungsrichtlinie), 2014/53/EU (Funkanlagenrichtlinie) und 2006/42/EG (Maschinenrichtlinie). Diese Rechtsakte selbst definieren wiederum nur die wesentlichen Eigenschaften, denen die Produkte genügen müssen. Die Detailausformung erfolgt durch die in den europäischen Normungsorganisationen (CEN, Cenelec, ETSI) organisierten Expertengremien im Auftrag der Kommission in einem durch Verordnung (EU) 1025/212 strukturierten Verfahren; gelingt dort eine Einigung, werden die technischen Standards als sogenannte „harmonisierte Normen" veröffentlicht.[308] Die Hersteller sind überwiegend selbst für die Konformitätsbewertung nach Maßgabe der Normen zuständig und weisen dies durch CE-Kennzeichnung nach.

Bisher nicht vollständig mit dem „neuen Rechtsrahmen" synchronisiert wurde die für die Praxis überaus bedeutsame, weil horizontal geltende Richtlinie 2001/95/EG über die allgemeine Produktsicherheit. Hier läuft seit längerer Zeit ein Gesetzgebungsverfahren; an sich war mit der Verabschiedung der nun als Verordnung gefassten Neuregelung (Produktsicherheits-VO) für Ende 2021 gerechnet worden; das Verfahren hat sich jedoch verzögert.[309] Hierfür ist auch verantwortlich, dass nach den Plänen der Kommission neu auch die Cybersicherheit als eines der bei der Beurteilung der Sicherheit von Produkten zu berücksichtigenden Merkmale aufgeführt ist.[310] Parallel dazu plant

[307] Dieser setzt sich ursprünglich aus drei Rechtsakten zusammen: der VO (EG) Nr. 764/2008, der VO (EG) Nr. 765/2008 und dem Beschluss Nr. 768/2008/EG. Die VO (EG) Nr. 764/2008 wurde durch die VO (EU) 2019/515 vom 19.3.2019 aufgehoben und die VO (EG) Nr. 764/2008 wurde durch die VO (EU) 2019/1020 vom 20.6.2019 wesentlich modifiziert worden, sodass der „neue Rechtsrahmen" heute aus der VO (EG) Nr. 765/2008, dem Beschluss Nr. 768/2008/EG und der VO (EU) 2019/1020 besteht.

[308] Zur Begrifflichkeit siehe Art. 2 Nr. 1 Verordnung (EU) Nr. 1025/2012.

[309] Dazu *T. Klindt*, in: ders. (Hrsg.), ProdSG, 2021, Einführung Rn. 37 ff. Das Verfahren zum Vorschlag der Kommission für eine General Product Safety Regulation v. 30.6.2021, COM(2021) 346, wird unter 2021/0170(COD) dokumentiert.

[310] Dazu kritisch *C. Hartmann/T. Klindt*, Kritisches zum Kommissions-Entwurf für eine Produktsicherheits-VO, ZfPC 2022, S. 73 (74 f.). Das Verfahren zum Vorschlag der Kommission für eine General Product Safety Regulation v. 30.6.2021, COM(2021) 346, wird unter 2021/0170(COD) dokumentiert.

die Kommission seit geraumer Zeit eine grundlegende Überarbeitung des legislativen Rahmens für die Konformitätsbewertung und Marktüberwachung; Teile dieser Reform wurden bereits mit der Verordnung (EU) 2019/1020 über Marktüberwachung und die Konformität von Produkten umgesetzt.

Das zentrale Instrument aus dem Recht der Produktsicherheit, an dem sich das Recht der Informationssicherheit orientieren kann, ist die Zertifizierung von Komponenten.[311] Programmatisch formuliert hierzu der aus der EU-Cybersicherheitsstrategie 2017 hervorgegangene EU Cybersecurity Act (CSA) in Erwägungsgrund 65: „Die Cybersicherheitszertifizierung spielt eine große Rolle, wenn es darum geht, das Vertrauen in IKT-Produkte, -Dienste und -Prozesse zu stärken und deren Sicherheit zu erhöhen. Die Entwicklung des digitalen Binnenmarkts und insbesondere der Datenwirtschaft und des Internets der Dinge kommt nur voran, wenn in der breiten Öffentlichkeit das Vertrauen vorhanden ist, dass diese Produkte, Dienste und Prozesse ein gewisses Maß an Cybersicherheit gewährleisten."[312]

Nach Ansicht des Verordnungsgebers fehlt es bislang an branchenübergreifenden und unionsweit anerkannten Zertifizierungsangeboten, worunter das Vertrauen in die Informationstechnologie leidet. Nicht alle Mitgliedstaaten hatten bereits wie Deutschland mit dem BSI eine nationale Zertifizierungsstelle errichtet (vgl. § 9 Abs. 2 BSIG). Informelle Initiativen zur gegenseitigen Anerkennung von Cybersicherheits-Zertifikaten konnten sich zudem am Markt nicht durchsetzen.[313] Hier soll der CSA mit seinem horizontalen Ansatz Abhilfe schaffen und einen unionsweiten Zertifizierungsrahmen für Cybersicherheit errichten (Art. 46 ff. CSA). Anliegen des CSA ist generell eine Erhöhung des IT-Sicherheitsniveaus. Dementsprechend soll sich seine Umsetzung und Anwendung an den dem Datenschutzrecht (vgl. Art. 25 Abs. 2 DS-GVO) nachempfundenen Prinzipien von „security by design" und „security by default" orientieren (vgl. ErwGr 12, 13 CSA).

Auf der Grundlage des CSA kann ENISA nun im Auftrag der Kommission oder der als „Europäische Gruppe für die Cybersicherheitszertifizierung" organisierten Fachbehörden der Mitgliedstaaten (Art. 62 CSA) sowie in Konsul-

[311] Speziell zur Zertifizierung siehe neben den in der vorigen Fußnote genannten Texten auch *H. Pünder*, Zertifizierung und Akkreditierung, ZHR 170 (2006), S. 567 ff.; *G. Dimitropoulos*, Zertifizierung und Akkreditierung, 2012.

[312] Die Verordnung hat zwei Schwerpunkte. Zum einen wird ENISA organisatorisch und finanziell gestärkt und der Agentur werden weitere Aufgaben übertragen (Art. 5–12 CSA); ihre Rolle innerhalb der Union ist nun der des BSI vergleichbar. Zum anderen errichtet der CSA ein Zertifizierungsregime für Informationssicherheit; eben dieses wird hier näher betrachtet.

[313] Zu erwähnen ist in diesem Zusammenhang insbes. die von der „Gruppe hoher Beamter für die Sicherheit der Informationssysteme" (SOG-IS) getroffene Vereinbarung über die gegenseitige Anerkennung (MRA), an der jedoch nicht alle EU-Mitgliedstaaten beteiligt sind, vgl. https://www.sogis.org.

tation mit dieser Gruppe und weiteren Stellen (vgl. Art. 49 CSA) für konkrete IT-basierte Produkte, Dienstleistungen und Prozesse sogenannte „Zertifizierungs-Schemata" verabschieden (Art. 49 CSA).[314] Nach der Legaldefinition des Art. 2 Nr. 9 CSA bezeichnet ein „europäisches Schema für die Cybersicherheitszertifizierung" ein „umfassendes Paket von Vorschriften, technischen Anforderungen, Normen und Verfahren, die auf Unionsebene festgelegt werden und für die Zertifizierung oder Konformitätsbewertung von bestimmten IKT-Produkten, -Diensten und -Prozessen gelten". Gemäß Art. 54 CSA umfasst ein Schema also unter anderem folgende Arten von Informationen: die konkreten Produkte oder Dienste, auf die es Anwendung findet; die Normen oder technischen Standards, die beachtet werden müssen; die Art der Überprüfung der Anforderungen (Selbstbewertung oder Fremdzertifizierung); sowie gegebenenfalls die Vertrauenswürdigkeitsstufen.

Die Schemata werden durch die Kommission per Durchführungsakt angenommen (Art. 49 Abs. 7 CSA).[315] Sie dienen unionsweit (Art. 57 CSA) als Grundlage für Cybersicherheitszertifizierungen (Art. 56 CSA). Sofern das Unionsrecht oder das Recht der Mitgliedstaaten nicht anders bestimmen, bleibt die Zertifizierung allerdings freiwillig (Art. 56 Abs. 2 CSA). Im Rahmen der Zertifizierung richtet sich die Qualität der geforderten Sicherungsmaßnahmen ebenso wie die Art der geforderten Evaluation nach dem Risikoniveau[316] des Produkts oder Systems bzw. nach der in Anspruch genommenen „Vertrauenswürdigkeitsstufe", die als „niedrig", „mittel" und/oder „hoch" angeben werden kann.[317] Je nach Vertrauenswürdigkeitsstufe unterscheidet sich das Verfahren der Zertifikatsausstellung. Diese kann in den Stufen „niedrig" und „mittel" in Übereinstimmung mit den Grundsätzen des New Legislative Framework nach Richtlinie (EU) 2008/765 durch alle den Anforderungen des Art. 60 CSA und dem Anhang zur CSA genügenden Konformitätsbewertungsstellen ausgestellt werden (Art. 56 Abs. 4 CSA); üblicherweise sind dies Private wie der TÜV e. V. Für die Vertrauenswürdigkeitsstufe „hoch" kann die Bescheinigung der Zertifizierung hingegen einer Behörde vorbehalten werden (Art. 56 Abs. 5, 6 CSA i. V. m. Art. 58 CSA). Im Falle eines „niedrigen" Risikos kann der Hersteller oder Anbieter nach den Maßgaben des

[314] Zum Governance-Modell näher *Fischer/Kipker/Voskamp*, Internationaler Rahmen, in: Kipker (Hrsg.), Cybersecurity, 2020, Kap. 16 Rn. 14 ff. Die aktuellen Bemühungen dokumentiert ENISA unter https://www.enisa.europa.eu/topics/standards/certification.

[315] Zu diesem Prozess *B. Kowalski/M. Intemann/T. Mühlenbruch*, Bedeutung des Cybersecurity Acts für die IT-Sicherheitszertifizierung in Deutschland und Europa, DuD 2021, S. 244 ff.

[316] Zum Risikobegriff des CSA *S. Fritsch/D. Bremser*, Europäische Zertifizierungsschemata, BSI Forum in der <kes> 2020, S. 44 ff.

[317] Näher dazu *D. Bremser/S. Fritsch*, Europäische Cybersicherheitszertifizierung, BSI Forum in der <kes> 2020, S. 35 ff.

Art. 53 CSA eine Selbstbewertung der Konformität vornehmen und sich die EU-Konformitätserklärung ausstellen.

Insgesamt will der CSA also erneut nicht selbst konkrete IT-Sicherheitsstandards definieren. Vielmehr schafft der Rechtsakt Rahmenbedingungen für ein spezifisch IT-sicherheitsbezogenes Zertifizierungswesen in den Mitgliedstaaten. ENISA und den zuständigen nationalen Behörden obliegt es, entsprechende Zertifizierungsschemata zu entwerfen. Die konkreten Zertifizierungsentscheidungen erfolgen hingegen überwiegend durch Private, wobei die Behörden der Mitgliedstaaten im Falle „hoch"-riskanter Systeme eine wichtige Rolle spielen.

Kern des CSA-Systems ist der Freiwilligkeitsgedanke. Der Erfolg der Verordnung setzt damit voraus, dass am Markt ein Bedarf nach entsprechenden Zertifizierungen entsteht. Angesichts der Erkenntnisse der ökonomischen Forschung ist dies keineswegs gewiss.[318] Art. 56 Abs. 2 CSA sieht zwar die Möglichkeit vor, entsprechende Zertifizierungen verpflichtend zu verlangen. Hierzu trifft der CSA jedoch keine weitergehenden Festlegungen.

c) Der CSA im Kontext weiterer Zertifizierungsregime

Die Attraktivität einer Zertifizierung nach CSA hängt nicht nur von den Erwartungen des Marktes ab. Geklärt werden muss auch, wie sich das Zertifizierungsregime nach CSA zu vergleichbaren Regimen verhält. Dies betrifft zum einen die datenschutzrechtliche Zertifizierung nach Art. 42 DSGVO, die sich gemäß Art. 32 Abs. 3 DSGVO auch auf Aspekte der Informationssicherheit erstrecken und zum Nachweis der Erfüllung der Anforderungen des Art. 32 Abs. 1 DSGVO dienen kann.[319] Hierfür enthält ErwGr 74 CSA den Hinweis, wonach das Zertifizierungssystem der DSGVO von den Vorschriften des CSA „unberührt" bleiben soll. Gleichwohl stellen sich hier in der Praxis weitgehend identische Fragen.[320] Inwieweit eine „Doppelzertifizierung" nachgefragt wird, bleibt abzuwarten. Gleiches gilt für das Verhältnis des CSA zu den nach § 8a Abs. 2 BSIG für KRITIS-Betreiber verpflichtenden Standards und vor allem zu der seit 2009 existierenden Möglichkeit zur Zertifizierung durch das

[318] Siehe oben § 6 Fn. 142.

[319] Die Leistungsfähigkeit von Art. 42 DSGVO wird unterschiedlich beurteilt, vgl. nur die zurückhaltende Einschätzung bei *F. Richter*, Zertifizierung unter der DS-GVO, ZD 2020, S. 84 ff.; optimistischer hingegen *N. Maier/I. M. Pawlowska/S. Lins/A. Sunyaev*, Die Zertifizierung nach der DS-GVO, ZD 2020, S. 445 ff. Siehe auch die Beiträge in Heft 10/2020 der DuD, insbes. *H. Krasemann*, Der aktuelle Stand der Datenschutz-Zertifizierung und Akkreditierung in Deutschland und Europa, DuD 2020, S. 645 ff.

[320] Vgl. *Martini*, in: Paal/Pauly (Hrsg.), DS-GVO, 3. Aufl. 2021, Art. 32 Rn. 17 ff.

BSI nach § 9 BSIG bzw. zum – gänzlich überflüssigen – freiwilligen IT-Sicherheitskennzeichen nach § 9c Abs. 1 BSIG.[321]

Gewichtiger ist die Frage, wie sich der CSA zum unionalen Produktsicherheitsrecht verhält, das bei der Ausarbeitung des CSA ersichtlich als Vorbild diente. Dieses kennt bereits seit langem jene Mechanismen, die der CSA erst schaffen will. Das allein heißt jedoch noch nicht, dass der CSA obsolet wäre, solange sich die Konformitätsprüfungen nicht überschneiden. Wie erwähnt erfassen sowohl die sektoralen Rechtsakte als auch die horizontale allgemeine Produktsicherheits-Richtlinie (bzw. das ProdSG) die IT-Sicherheit bisher nicht – jedenfalls nicht direkt.[322] Grund hierfür ist neben der erwähnten Fokussierung des Produktsicherheitsrechts auf physische Schäden auch, dass sich das Produktsicherheitsrecht traditionell ganz am *safety*-Konzept orientiert, während Gefährdungen der IT-Sicherheit eben nicht nur durch das Produkt selbst, sondern auch durch Dritte drohen, also Fragen von *security* aufwerfen.[323] Da allerdings wiederum gerade bei cyber-physischen Systemen sowohl *safety*- wie *security*-bezogene Risiken zu Schäden an Leben und Gesundheit von Personen (vgl. § 3 Abs. 2 S. 1 ProdSG) führen können,[324] läge es alles andere als fern, die Konformitätsprüfungen des Produktsicherheitsrechts auch auf Fragen der IT-Sicherheit zu erstrecken.[325] Dementsprechend wird derzeit im Rahmen der turnusmäßigen Überarbeitung mehrerer sektoraler Produktsicherheitsrichtlinien diskutiert, ob die gesetzlichen Zielvorgaben um Aspekte der Informationssicherheit erweitert werden sollen; geplant ist dies insbesondere für die Maschinen-Richtlinie (umgesetzt durch ProdSG und die 9. ProdSV – Maschinenverordnung) und die Funkanlagen-Richtlinie (umgesetzt im FUAG).[326] Im Unterschied zu den freiwilligen Sche-

[321] Umgesetzt durch die Verordnung zum IT-Sicherheitskennzeichen des Bundesamtes für Sicherheit in der Informationstechnik (BSI-ITSiKV) v. 24.11.2021 (BGBl. I S. 4978). Die Funktion dieses Zeichens neben den in § 9a BSIG 2021 i. V. m. dem CSA geregelten Zertifizierungen und der Zertifizierung nach Art. 42, 43 DSGVO bleibt unklar. Hier droht nicht nur eine weitere Zersplitterung des ohnehin schon unübersichtlichen Zertifikatmarktes, sondern auch die Bindung wichtiger Ressourcen der Behörde. Kritisch daher zurecht *Hornung*, Das IT-Sicherheitsgesetz 2.0, NJW 2021, S. 1985 (1989), vgl. weiter *Paschke*, in: Ritter (Hrsg.), Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2022, § 9c BSIG Rn. 668 f.

[322] *C. Schucht*, Safety & Security bei smarten Produkten, NVwZ 2021, S. 532 ff.; *G. Wiebe*, IT-sicherheitsbezogene Pflichten von Herstellern smarter Produkte, InTeR 2021, S. 66 f. Vgl. allerdings die Hinweise in *Europäische Kommission*, Bericht über die Auswirkungen künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung, 19.2.2020, COM(2020) 64, S. 7.

[323] Umfassend dazu oben § 4. II. 2. c).

[324] Hierzu auch *Schucht*, Safety & Security bei smarten Produkten, NVwZ 2021, S. 532 ff.

[325] *Wiebe*, IT-sicherheitsbezogene Pflichten von Herstellern smarter Produkte, InTeR 2021, S. 66 (67). Kritischer *Hartmann/Klindt*, Kritisches zum Kommissions-Entwurf für eine Produktsicherheits-VO, ZfPC 2022, S. 73 (74 f.).

[326] Vgl. *BDI/DIN/DKE*, Europaweite Cyberregulierung, 1.2.2021.

mata nach CSA wären derartige Anforderungen in den genannten Rechtsakten dann für alle Marktteilnehmer verbindlich. Noch fehlen allerdings vielfach technische Standards, die eine rechtssichere Bewertung der Produkte erlauben würden.

Die Popularität des Zertifizierungskonzepts – so erfolgreich das System Zertifizierung an sich sein mag – ist aus Sicht der Marktteilnehmer nicht uneingeschränkt zu begrüßen. Für Verbraucher, deren „Vertrauen" in die Sicherheit von IT-Produkten durch die Zertifizierung an sich gestärkt werden soll,[327] verringert die große Zahl konkurrierender Zertifizierungsregime (DSGVO, BSIG, CSA etc.) die Markttransparenz eher, als dass sie sie stärkt. Während das hergebrachte Produktsicherheitsregime mit dem CE-Kennzeichen ein universelles und eingängiges Label hervorgebracht hat, existiert für IT-Sicherheitsprodukte (noch) nichts Vergleichbares. Aus Sicht der Wirtschaft geht eine regulatorische Fragmentierung der Zertifizierungsanforderungen mit einer erheblichen Kostenbelastung einher. Auf mittlere Sicht ist daher eine deutlich engere Koordinierung oder sogar eine Konsolidierung der Zertifizierungsregime erforderlich. Verschiedene Konstruktionen sind hier denkbar, etwa eine Integration des CSA in das New Legislative Framework oder aber ein eigenständiger horizontaler, auf dem New Legislative Framework basierender Rechtsakt zur Cybersicherheit.[328]

d) Produktwarnungen, -empfehlungen und -untersuchungen

Während das Zertifizierungsregime nur in Sonderfällen eine Beteiligung administrativer Stellen vorsieht, kennt das Technikrecht noch direkte Interventionen der Behörden in den Markt. Diese finden sich auch im Recht der Informationssicherheit. So gestattet § 7 Abs. 1 S. 1 Nr. 1 BSIG dem BSI, wie bereits erwähnt, Warnungen vor Sicherheitslücken auszusprechen; die Behörde darf dabei nach § 7 Abs. 2 BSIG auch öffentlich Hersteller und Produkt benennen, „wenn hinreichende Anhaltspunkte dafür vorliegen, dass Gefahren für die Sicherheit in der Informationstechnik hiervon ausgehen".[329] Einen ähnlichen Eingriff in die Grundrechte der Unternehmen stellt die an gleicher Stelle geregelte Befugnis zur Empfehlung konkreter IT-Sicherheitsprodukte dar. Eine Befugnis zur Produktwarnung (bisher nicht zur -empfehlung) neh-

[327] Vgl. oben § 6 Fn. 312.

[328] Vgl. *Europäischer Rat*, Schlussfolgerungen zur Cybersicherheit vernetzbarer IT-Produkte (13629/20), 2.12.2020.

[329] Zu den grundrechtlichen Grenzen für amtliche (Produkt-)Warnungen siehe jüngst ausführlich BVerfGE 148, 40; vgl. weiter nur *A.-S. Landwers*, Behördliche Öffentlichkeitsarbeit im Recht, 2019, S. 114 ff.; *B. Paal*, Sanktion durch behördliche Öffentlichkeitsinformation, K&R 2020, S. 8 ff. Für einen aktuellen Anwendungsfall des § 7 BSIG siehe BVerfG (K), 1 BvR 1071/22 v. 2.6.2022.

men auch die Datenschutzbehörden – nicht unumstritten[330] – auf der Grundlage des Art. 57 Abs. 1 lit. b i. V. m. Art. 58 Abs. 3 lit. b DSGVO für sich in Anspruch.[331]

Allerdings ist der Spielraum für behördliche Warnungen im Feld der IT-Sicherheit eher klein. So hat die Rechtsprechung aus Art. 12 Abs. 1 GG strenge Vorgaben für Warnungen in bloßen Verdachtsfällen entwickelt und erkennbar Sympathien für die Regelung des § 40 Abs. 1a LFGB gezeigt, mit der der Gesetzgeber die dort zuständige Behörde zu einer abschließenden Ermittlung der Tatsachen verpflichtet hat.[332] Bei komplexen IT-Produkten stoßen behördliche Ermittlungen allerdings rasch an Kapazitätsgrenzen; hinzu kommt erneut, dass jedenfalls dort, wo noch kein hinreichend konkreter Stand der Technik definiert ist, der Behörde ein eindeutiger Maßstab zur Durchführung der Prüfung oft fehlt. Schließlich erschwert die typischerweise hohe Dynamik der IT-Produktentwicklung den aus Verhältnismäßigkeitsgründen stets zur Prüfung der je aktuellen Produktversion verpflichteten Behörden die Arbeit.[333]

Anlass für eine Warnung kann eine nach § 7a BSIG zulässige Untersuchung von IT-Produkten und -Systemen, die entweder bereits auf dem Markt bereitgestellt oder zur Bereitstellung auf dem Markt vorgesehen sind, sein.[334] Hierbei kann das BSI nicht nur im Einzelfall gegen potenziell unsichere Produkte ermitteln, sondern etwa auch durch eine gezielte Sektorenermittlung Absprachen zur Blockade von Zertifizierungen brechen. Für die Erkenntnisse aus solchen Untersuchungen besteht eine strikte Zweckbindung, § 7a Abs. 4 BSIG.[335] Allerdings gilt erneut, dass die Behörden nur im Rahmen ihrer Kapazitäten tätig werden können; will der Gesetzgeber im Rahmen seiner Gewährleistungsverantwortung entsprechend invasive Untersuchungen bestimmter Produktgruppen bis hin zum Quellcode bzw. zur Basisarchitektur ermöglichen, muss er hierfür auch ausreichende Haushaltsmittel zur Verfügung stellen.[336]

---

[330] Kritisch etwa *R. Gerling/S. Gerling/S. Hessel/R. Petrlic*, Stand der Technik bei Videokonferenzen, DuD 44:11 (2020), S. 740 (746 f.); *S. Hessel/M. Schneider*, Inspector Gadget ermittelt?, K&R 2022, S. 82 ff.

[331] Siehe zur Position der Datenschutzbehörden: *AK Grundsatz der DSK*, ohne Titel, 9.11.2020.

[332] BVerfGE 148, 40 (56, Rn. 44). Zu Haftungsrisiken der Behörde siehe *Schulte*, in: Ritter (Hrsg.), Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2022, § 7 BSIG Rn. 321 ff.

[333] Zur Bedeutung des Zeitfaktors BVerfGE 148, 40 (60 ff., Rn. 56 ff.).

[334] Zu den erweiterten Untersuchungsrechten nach § 7a BSIG 2021 *Hornung*, Das IT-Sicherheitsgesetz 2.0, NJW 2021, S. 1985 (1989 f.).

[335] Zu den Implikationen siehe § 7 II. 3. b) bb).

[336] Dazu bereits *Wischmeyer*, Informationssicherheitsrecht, DV 50 (2017), S. 155 (170). Dem BSI stehen für diese Aufgabe jedoch nur sehr geringe Personalkapazitäten zur Verfügung, vgl. *Deutscher Bundestag*, Gesetzesentwurf der Bundesregierung zum IT-SiG 2.0, BT-Drs. 19/26106, S. 37; kritisch dazu *Keppeler*, in: Ritter (Hrsg.), Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2022, § 7a BSIG Rn. 330.

e) Zwischenfazit

Erkennbar ist, dass der Informationssicherheitsgesetzgeber der Komponentensicherheit mittlerweile große Aufmerksamkeit widmet. Die bisherigen Initiativen sind allerdings noch nicht in jeder Hinsicht zielführend. Nachvollziehbar ist, dass der Aufbau einer entsprechenden Zertifizierungsinfrastruktur Zeit benötigt. Auch wenn die im allgemeinen Produktsicherheitsrecht gesammelten Erfahrungen eine gewisse Beschleunigung gestatten mögen, bleibt es dennoch eine komplexe Aufgabe, IT-Sicherheit umfassend im sehr diffusen und dynamischen Markt der IT-Komponenten zu implementieren. Erneut kann nicht darauf gehofft werden, dass allein durch die Institutionalisierung eines Rechtsregimes und die Einräumung einzelner behördlicher Interventionsrechte eine grundlegende Verbesserung erfolgt, wenn diese Maßnahmen nicht hinreichend fiskalisch unterlegt werden.

7. Internetsicherheit als terra incognita des Informationssicherheitsrechts

Während sich der Informationssicherheitsgesetzgeber jedenfalls in Ansätzen der Risiken von IT-Komponenten angenommen hat, wird das Feld der Internetsicherheit nach wie vor regulatorisch vernachlässigt. Dies gilt sowohl für die Risiken für die Sicherheit und Stabilität des Internets selbst, die oben unter Verweis auf das BGP Highjacking illustriert wurden,[337] als auch für jene Risiken, die Schwachstellen der Internetarchitektur ausnutzen, um auf diese Weise die an das Internet angebundenen IT-Systeme und Netzwerke zu beeinträchtigen.[338] Neben den nun schon mehrfach angeführten Gründen, die für die verzögerte Reaktion des Gesetzgebers verantwortlich sind, ist es im Fall der Internetsicherheit auch die Sorge vor eine Verstärkung der rechtlichen und technischen Fragmentierung des Internet, die hemmend wirkt.[339]

Die Thematik hat dennoch mittlerweile immerhin den politischen Raum erreicht. So hat die Kommission in der Europäischen Cybersicherheitsstrategie 2020 angekündigt, Schutzpläne für einen Ausfall des globalen DNS Routing zu entwickeln, und will sich zudem an der Entwicklung und Verbreitung sicherer Internetstandards beteiligen:

„The Commission will also, in liaison with Member States and industry, accelerate the uptake of key internet standards including IPv6 and well-established internet security standards and good practices for DNS, routing, and email security, not excluding regu-

[337] Vgl. oben § 6 Fn. 91.
[338] Dazu im Einzelnen § 6 II. 1. b) cc).
[339] Zur Fragmentierung des Internets siehe § 6 Fn. 132.

latory measures like a European sunset clause for IPv4 to steer the market if there is insufficient progress towards their adoption."[340]

Erste Schritte dazu finden sich bereits im Verordnungsrecht. So hat der deutsche Verordnungsgeber bereits die Betreiber zentraler Internet-Infrastrukturdienste, insbesondere Anbieter von DNS-Dienstleitungen und sog. Top Level Domain (TLD)-Registern, den KRITIS zugeordnet und so in die Regulierung des BSIG einbezogen,[341] um den durch die Übernahme oder Kompromittierung des DNS-Systems für die Integrität des Internetverkehrs drohenden Gefahren zu begegnen. Während diese Regelung im deutschen Recht im Anhang zur KritisV „versteckt" ist, spricht der europäische Gesetzgeber im Entwurf zur NIS 2-RL die entsprechenden Betreiber direkt als Regulierungsadressaten an (Art. 3 Abs. 1 lit. b NIS 2-RL)[342] und belegt sie in Art. 26 Abs. 3; 27 Abs. 2 NIS 2-RL mit Sorgfaltspflichten für die Registrierung und Pflege ihrer Einträge.[343] Flankiert wird dies durch eine breite Jurisdiktionsregelung in Art. 26 Abs. 1 NIS 2-RL für die häufig in mehreren Mitgliedstaaten der Union oder ganz außerhalb der Union angesiedelten Betreiber. Das Parlament hat zusätzlich vorgeschlagen, dass die Mitgliedstaaten Internetprovidern und anderen die Einführung sicherer Routing-Protokolle und einer DNS Resolution Diversification-Strategie vorschreiben, unter anderem um BGP Highjacking zu verhindern.[344] Diese Vorschläge haben (auch wegen weiterer damit verbundener Vorhaben) Kritik auf sich gezogen.[345] Als erster Schritt hin zu einer aktiven Befassung mit der Problematik kommt ihnen dennoch eine Vorbildfunktion zu.

---

[340] *Europäische Kommission/Hoher Vertreter der Union für Außen- und Sicherheitspolitik*, Die Cybersicherheitsstrategie der EU für die digitale Dekade, JOIN(2020) 18 final, S. 10 f.

[341] Siehe Anhang 4 Nr. 2 lit. c, d und e BSI-KritisV.

[342] Vgl. auch ErwGr 32 NIS 2-RL: „Upholding and preserving a reliable, resilient and secure domain name system (DNS) are key factors in maintaining the integrity of the internet and are essential for its continuous and stable operation, on which the digital economy and society depend. Therefore, this Directive should apply to top-level-domain (TLD) name registries, and DNS Service providers […]. This Directive should not apply to root name servers."

[343] Ergänzt wird dies durch die verschärfte Regulierung entsprechender Anbieter von Internet-Infrastrukturdienstleistungen durch den ebenfalls im Gesetzgebungsverfahren befindlichen Digital Services Act (oben § 6 Fn. 122).

[344] Vgl. ErwGr 100 NIS 2-RL.

[345] *M. Reuter*, EU will eigenen DNS-Server mit Filterlisten und Netzsperren, Netzpolitik.org, 24.1.2022.

8. Durchsetzung und Kontrolle

a) Allgemeine ordnungsrechtliche Durchsetzungs- und Kontrollbefugnisse

Zur Durchsetzung und Kontrolle der informationssicherheitsbezogenen Pflichtenprogramme sehen die einschlägigen Rechtsakte weitgehend klassische Mechanismen der Wirtschaftsaufsicht vor. So stehen den Datenschutzaufsichtsbehörden bei Verstößen gegen Art. 32 DSGVO die allgemeinen Befugnisse des Art. 58 DSGVO zu.[346] Im KRITIS-Recht sieht § 8a Abs. 3 BSIG vor, dass die – registrierungspflichtigen (§ 8b Abs. 3 BSIG) – KRITIS-Betreiber die Erfüllung aller Sicherheitsstandards mindestens alle zwei Jahre nachzuweisen haben, wobei der Nachweis durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen kann.[347] Das BSI hat Informationsrechte und kann, gegebenenfalls im Benehmen mit den sonst zuständigen Aufsichtsbehörden, die Beseitigung von Sicherheitsmängeln verlangen. Gemäß § 8a Abs. 4 BSIG darf das BSI die Einhaltung der Anforderungen zudem umfassend überprüfen und hat zu diesem Zweck unter anderem das Recht zur Nach- und Umschau in den Geschäfts- und Betriebsräumen während der üblichen Betriebszeiten. Schließlich tragen auch die oben analysierten Melde- und Informationspflichten ihren Teil zur Ermöglichung und Erleichterung der behördlichen Kontrolltätigkeit bei. Bereits erwähnt wurde, dass das BSI bei konkreten Störfällen auch die Hersteller der betroffenen Produkte und Systeme in Anspruch nehmen kann (§ 8b Abs. 6 Satz 1 BSIG). Auskunftspflichten und Beseitigungsrechte bestehen gemäß § 8c Abs. 4 BSIG auch gegenüber den Anbietern digitaler Dienste. Für „Unternehmen im besonderen öffentlichen Interesse" bestehen hingegen gemäß § 8f BSIG nur (allerdings weitreichende) Berichtspflichten und Informationsansprüche. Ähnlich verhält es sich im sektorspezifischen Informationssicherheitsrecht. So finden sich im Telekommunikationsrecht entsprechende Kontrollrechte und korrespondierende Informations- und Mitwirkungspflichten in den §§ 165 ff. TKG.[348] Auch die durch das IT-SiG 2.0 geschaffenen, im Gesetzgebungsverfahren sehr umstrittenen Ermittlungs- und Anordnungsbefugnisse des BSI nach §§ 7b, 7c und 7d BSIG sind in diesem Zusammenhang zu nennen.[349]

---

[346] Näher hierzu *Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022, Rn. 232 ff.

[347] Zu den Optionen externer und interner Nachweisverfahren siehe *A. Woitke*, Prüfgrundlagen nach § 8a, DuD 2021, S. 584 ff.; *C. Stradomsky*, KRITIS – Der Weg zum Audit, DuD 2021, S. 589 ff.

[348] Beachte in diesem Zusammenhang auch, dass den Telekommunikationsunternehmen in § 169 Abs. 4 bis 7 TKG zu Beschränkungen der Nutzer ermächtigt.

[349] § 7b BSIG gestattet dem BSI, in Form sog. Portscans eigenständig die Netzwerk- und Systemsicherheit von Unternehmen und Behörden zu überprüfen, vgl. zu den technischen Details die ausführliche Begründung *Deutscher Bundestag*, Gesetzesentwurf der Bundesregierung zum IT-SiG 2.0, BT-Drs. 19/26106, S. 60 ff. Zur Kritik vgl. *Kipker/Scholz*, Das IT-Sicherheitsgesetz 2.0, MMR 2019, S. 431 (433). Zur fehlenden Praktikabilität der Neure-

Auf die grundrechtliche Dimension all dieser Rechte wurde bereits ausführlich eingegangen. Ein Verstoß gegen die genannten Pflichten ist rechtsgebietsübergreifend mit Bußgeldern bewehrt; Art. 34 Abs. 4 und 5 NIS 2-RL führt hier jetzt zu einer empfindlichen Verschärfung, indem die Höhe der Bußgelder am Unternehmensumsatz orientiert wird, und nähert damit das KRITIS-Recht der DSGVO an.[350]

b) Operative Tätigkeiten: CSIRT/CERT und MIRTs

Unter bestimmten Bedingungen und in begrenztem Umfang dürfen hoheitliche Stellen bei IT-Sicherheitsvorfällen auch operativ tätig werden. Entsprechende Stellen in der Verwaltung werden nach internationalem Vorbild als Computer Emergency Response Teams (CERTs) oder auch Computer Security Incident Response Teams (CSIRTs) bezeichnet.[351] In Deutschland übernimmt das BSI diese Aufgabe in erster Linie in seiner Funktion als die für die Abwehr von Gefahren für die Sicherheit der Bundes-IT zuständige Stelle (§ 3 Abs. 1 S. 2 Nr. 1 BSIG).[352] Als CERT-Bund ist es ausweislich seiner Selbstbeschreibung die zentrale Anlaufstelle für präventive und reaktive Maßnahmen bei IT-sicherheitsrelevanten Vorfällen in der Bundesverwaltung.[353]

Darüber hinaus geht die durch das NIS-RL-Umsetzungsgesetz eingeführte und durch das IT-SiG 2.0 nicht wesentlich veränderte operative Gefahrenabwehrbefugnis des BSI nach § 5b BSIG.[354] Danach stellt die Behörde sog. Mo-

---

gelung siehe *Keppeler*, in: Ritter (Hrsg.), Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2022, § 7b BSIG Rn. 355, 374. Allgemein zu Portscans siehe *F. Grieger*, Portscans im Lichte des Rechts, Int'l Cybersecurity L. Rev. 2021, S. 297 ff.

§§ 7c und 7d BSIG, die dem BSI erstmals – und beschränkt auf Anbieter von Telekommunikationsdiensten und Telemedien – eigenständige operative Befugnisse zur Gefahrenabwehr einräumen, gestatten dem BSI, die Anbieter zu den ihnen nach § 169 Abs. 6 und 7 TKG möglichen Beschränkungen der Nutzer (vgl. dazu oben § 6 Fn. 199 und 348) bzw. zur Umsetzung der von § 19 Abs. 4 TTDSG geforderten Sicherheitsvorkehrungen behördlich zu verpflichten. Zu Unschärfen des § 7c BSIG, zur notwendigen Koordination zwischen BSI und BNetzA und zur grundrechtlichen Dimension siehe *Keppeler*, a. a. O., § 7c BSIG Rn. 401, 404 ff.

[350] Vgl. bisher § 14 BSIG, der wegen des Verweises auf § 30 Abs. 2 S. 3 OWiG für Unternehmen Bußgelder von bis zu 10 Millionen Euro vorsieht.

[351] Zur Definition siehe § 4 Fn. 111.

[352] Die Einrichtung von CSIRTs verlangen Art. 1 Abs. 2 lit. c und Art. 9 NIS-RL; Anhang I der Richtlinie präzisiert die Anforderungen und Aufgaben der CSIRTs und beschreibt, wie sie Risiken überwachen, analysieren und auf Vorfälle reagieren sollen. Die NIS-Richtlinie unterscheidet allgemein zwischen der nationalen „competent authority" und dem nationalen CERT/CSIRT, erlaubt jedoch die Ansiedlung von letzterem in ersterem.

[353] Vgl. die Darstellung unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html.

[354] Allerdings wurde der Anwendungsbereich auch der Norm auf Unternehmen im besonderen öffentlichen Interesse erweitert; hierfür wurden dem BSI 41 zusätzliche Planstellen bewilligt, vgl. *Deutscher Bundestag*, Gesetzesentwurf der Bundesregierung zum IT-SiG 2.0, BT-Drs. 19/26106, S. 37.

bile Incident Response Teams (MIRTs) auf, um Bundesbehörden, KRITIS-Betreiber sowie in begründeten Einzelfällen auch weitere Stellen (§ 5b Abs. 7 BSIG) bei besonders komplexen oder schwerwiegenden Cyber-Angriffen vor Ort bei der Bewältigung zu unterstützen („Cyber-Feuerwehr"). Da dieser Einsatz nach der Gesetzeslage nur auf der Grundlage eines Ersuchens der Betreiber gestattet ist,[355] liegt insoweit kein Eingriff in die Grundrechte betroffener Unternehmen vor. Allerdings beeinträchtigen die Untersuchungen und Abhilfemaßnahmen der MIRTs regelmäßig das Recht auf informationelle Selbstbestimmung und das Fernmeldegeheimnis Dritter, sodass es der jetzt mit § 5b BSIG geschaffenen Ermächtigungsgrundlage samt der dortigen Eingriffsbeschränkungen bedurfte. Unter den in § 5b Abs. 4 S. 1 BSIG i. V. m. § 5 Abs. 5 und 6 BSIG definierten Umständen dürfen im Zuge eines Einsatzes gesammelte Daten auch an Polizei- und Nachrichtendienste weitergegeben werden.

c) Haftung

Eine Sonderstellung im Recht der Informationssicherheit kommt dem Haftungsrecht zu. Als alleiniges Instrument hat es sich aus den oben genannten Gründen als weitgehend wirkungslos erwiesen.[356] Seine Wirkung konnte bzw. kann es erst jetzt im Zusammenwirken mit einem regulatorischen Regime entfalten, das für Netzwerk- und Systembetreiber ebenso wie für Komponentenhersteller konkrete Handlungs-, Duldungs- und Unterlassungspflichten definiert, Meldepflichten vorsieht und zum Aufbau und zur Pflege hinreichend bestimmter Standards motiviert. Die Aktivierung des zivilen Haftungsrechts verlangt nämlich, dass recht konkret feststeht, was ein sicheres System oder Programm leisten muss – und wer dafür verantwortlich ist.[357]

Die weitergehenden gesellschafts-, zivil- und zivilprozessrechtlichen Fragen, die sich bei der Anwendung und Durchsetzung der Haftungsnormen stellen, sprengen den Rahmen der vorliegenden Arbeit. Hingewiesen sei nur darauf, dass das Haftungsrecht sich der Thematik heute in ihrer ganzen

[355] Zur diesbezüglichen Motivationslage der Betreiber siehe *Schallbruch*, IT-Sicherheitsrecht (Folge 3), CR 2018, S. 215 (219).

[356] Siehe § 6 II. 4. b).

[357] Siehe § 6 II. 3. a). Dies gilt gerade für die dogmatisch bereits überzeugend begründeten, in der Praxis bisher allerdings gänzlich vernachlässigten vertraglichen Nebenpflichten zur IT-Sicherheit, vgl. *Rafsendjanim/Bomhard*, IT-Sicherheit im Zivilrecht und in der Vertragsgestaltung, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 9 Rn. 77; *Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022, Rn. 134 ff. Umgekehrt gilt, dass die sonstigen Pflichten des Informationssicherheitsrechts an Effektivität einbüßen, wenn sie nicht auch im Wege des Haftungsrechts (privat) durchgesetzt werden können. Zum Zusammenspiel von Haftungsrecht und Meldepflichten aus der Sicht des insoweit defizitären kalifornischen Rechts *S. Park*, Why Information Security Law Has Been Ineffective in Addressing Security Vulnerabilities, International Review of Law and Economics 58 (2019), S. 132 ff.

Breite annimmt.[358] Stand traditionell die deliktische Haftung im Vordergrund, sei es nach § 823 Abs. 1 BGB in der Form der Verletzung des eingerichteten und ausgeübten Gewerbebetriebs oder von Verkehrssicherungspflichten oder nach § 823 Abs. 2 BGB i. V. m. einem Schutzgesetz,[359] rücken heute mehr und mehr Compliance-Vorgaben in den Vordergrund.[360] Auch im verschuldensunabhängigen Produkthaftungsrecht wird mittlerweile über eine Weitung des traditionell engen Produktbegriffs nachgedacht, der jedenfalls für sog. „stand alone"-Software lange Zeit verhindert hat, dass Fragen der IT-Sicherheit effektiv adressiert werden konnten.[361] Jüngst ist auch das vertragliche Haftungsrecht dort, wo es um die Bereitstellung digitaler Dienste geht, in Sachen IT-Sicherheit gestärkt worden.[362] Hierzu trägt insbesondere

[358] Zur Diskussionsentwicklung siehe *Schallbruch*, IT-Sicherheitsrecht (Folge 3), CR 2018, S. 215 (221 f.). Im Überblick nun *T. Lapp*, Ziviles Haftungsrecht, in: Kipker (Hrsg.), Cybersecurity, 2020, S. 231 ff.; *Rafsendjanim/Bomhard*, IT-Sicherheit im Zivilrecht und in der Vertragsgestaltung, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 9; *G. Spindler*, Grundlagen deliktsrechtlicher Sicherheitspflichten, in: a. a. O., § 10; *ders.*, Verantwortung der IT-Hersteller (produktbezogene Pflichten), in: a. a. O., § 11. Zur Durchsetzungsperspektive insbes. *T. Riehm/S. Meier*, Rechtliche Durchsetzung von Anforderungen an die IT-Sicherheit, MMR 2020, S. 571 ff. Siehe weiter bereits die Nachweise oben § 6 Fn. 143.

[359] Den Normen des BSIG wird ein drittschützender Charakter weithin abgesprochen, vgl. nur *Spindler*, IT-Sicherheitsgesetz und zivilrechtliche Haftung, CR 2016, S. 297 (306); *von dem Bussche/Schelinski*, Rechtsgrundlagen und Haftungsfolgen in der IT-Sicherheit, in: Leupold/Wiebe/Glossner (Hrsg.), IT-Recht, 4. Aufl. 2021, Teil 7.1 Rn. 38; teilweise anders *P. Roos*, Das IT-Sicherheitsgesetz, MMR 2015, S. 636 (641); unklar *Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022, Rn. 301 ff., 381, 542, 583 ff. Zur Frage, ob sich die Regeln der Produzentenhaftung über Art. 25 DSGVO gegenüber den Herstellern unsicherer IT-Produkte zur Anwendung bringen lassen, siehe *L. Specht-Riemenschneider*, Herstellerhaftung für nichtdatenschutzkonform nutzbare Produkte – Und er haftet doch!, MMR 2020, S. 73 ff.; *Martini*, in: Paal/Pauly (Hrsg.), DS-GVO, 3. Aufl. 2021, Art. 32 Rn. 27a.

[360] Dazu allgemein *D.-K. Kipker*, Grundlagen und Strukturen, in: ders. (Hrsg.), Cybersecurity, 2020, Kap. 1 Rn. 17, 24 m. w. N.; *T. Thalhofer*, Rechtliche Regeln für die IT-Sicherheit in Organisationen, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 16 Rn. 4 ff. Siehe weiter bereits die Nachweise oben § 6 Fn. 260.

[361] Grundlegend *A. Günther*, Produkthaftung für Informationsgüter, 2001. Siehe weiter *Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022, Rn. 590 ff. Offener *Europäische Kommission*, Bericht über die Auswirkungen künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung, 19.2.2020, COM (2020) 64 final, S. 17. Vom Produktbegriff dürfte bereits jetzt sog. „embedded" Software erfasst sein, etwa in das Endprodukt integrierte „Firmware" (siehe oben § 4 II. 2. b). Umstritten ist die Einordnung, wenn sich die Software auf einem Datenträger befindet. Vgl. weiter *G. Wiebe*, Produktsicherheitsrechtliche Pflicht zur Bereitstellung sicherheitsrelevanter Software-Updates, NJW 2019, S. 625 (626 m. w. N.). Zu aktuellen Entwicklungsperspektiven siehe etwa *L. Joggerst/J. Wendt*, Die Weiterentwicklung der Produkthaftungsrichtlinie, InTeR 2021, S. 13 ff.

[362] Vgl. dazu nur *S. Rockstroh/C. Peschel*, Sicherheitslücken als Mangel, NJW 2020, S. 3345 ff.; *D.-K. Kipker/M. Walkusz*, Mehr verbraucherbezogene IT-Sicherheit durch die Umsetzung der Digitale-Inhalte-Richtlinie?, RDi 2021, S. 30 ff.; *N. Böck/J. Theurer*, Herstellerpflichten und Haftungsrisiken bei IT-Sicherheitslücken vernetzter Produkte, BB 2021, S. 520 ff.

die für Verbraucherverträge eingeführte Pflicht zur Aktualisierung (Update-Pflicht) bei, vgl. § 327f BGB.[363]

d) Strafrechtliche Sanktionen

Als ultima ratio muss auch das Recht der Informationssicherheit Straf- und Bußgeldnormen für die Verletzungen der Verfügbarkeit, Unversehrtheit und Vertraulichkeit von informationstechnischen Systemen vorsehen.[364] Der Gesetzgeber hat vergleichsweise früh zu diesem Mittel gegriffen, erstmals im Zweiten Gesetz zur Bekämpfung der Wirtschaftskriminalität v. 15.5.1986, das die §§ 202a, 263a, 269, 270 ins StGB eingefügt hat. Eigentliche praktische Bedeutung bekam die Materie dann mit dem Aufstieg von Cybercrime zu einem Massenphänomen um die Jahrtausendwende,[365] auf den der Gesetzgeber mit dem Einundvierzigsten Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (41. StrÄndG) v. 7.8.2007 reagiert hat (vgl. §§ 202a, 202b, 202c, 303a, 303b StGB).[366] Die deutsche Gesetzgebung wurde hierbei stark durch das Völker- und Unionsrecht beeinflusst – namentlich die Convention on Cybercrime des Europarats vom 23.11.2001 und den EU-Rahmenbeschluss 2005/222/JI vom 24.2.2005 über Angriffe auf Informationssysteme.[367]

Seither sind größere Reformen ausgeblieben.[368] Erst jüngst ist der Vorschlag, die Ausbreitung von „Bot-Netzen" durch die Pönalisierung des „digitalen

[363] Dazu näher *S. Hessel/K. Potel*, Update qua Gesetz, RDi 2022, S. 25 ff.; *K. Schreiber/J. Esser*, Einheitliche Update-Zyklen im Spannungsfeld der §§ 327f, 327r BGB, RDi 2022, S. 317.

[364] Grundlegend *Kochheim*, Cybercrime und Strafrecht, 2. Aufl. 2018; *T. Singelnstein/L. Zech*, Schutz der IT-Sicherheit durch das Strafrecht, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 20 Rn. 9 ff.

[365] Begriff und Umfang des Phänomenbereichs „Cybercrime" sind umstritten. Für die Praxis maßgeblich: *BKA*, Bundeslagebild Cybercrime 2021, 2022, S. 4. Siehe vertiefend *D. Brodowski/F. Freiling*, Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, 2011, S. 27 ff.; *Singelnstein/Zech*, Schutz der IT-Sicherheit durch das Strafrecht, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 20 Rn. 5 ff.

[366] Zur Geschichte des IT-Strafrechts *K. Altenhain*, IT-Strafrecht – Entstehung eines Rechtsgebiets, in: Weiß (Hrsg.), Rechtsentwicklungen im vereinten Deutschland, 2011, S. 117 ff.; *Kochheim*, Cybercrime und Strafrecht, 2. Aufl. 2018, Rn. 311 ff.

[367] Zur Cybercrime Convention siehe oben § 4 Fn. 146. Der Rahmenbeschluss 2005/222/JI wurde mittlerweile durch die Richtlinie 2013/40/EU vom 12.8.2013 über Angriffe auf Informationssysteme ersetzt. Zum Unionsrecht umfassend *Haase*, Computerkriminalität im Europäischen Strafrecht, 2017.

[368] Zum weithin als misslungen angesehenen § 202d StGB (BGBl. I 2015 S. 2218) siehe nur kritisch *T. Singelnstein*, Predictive Policing, NStZ 2018, S. 1 ff.; *S. Golla/S. Thess*, Das Strafrecht als schlechtes Vorbild, in: Hennemann/Sattler (Hrsg.), Immaterialgüter und Digitalisierung, 2018, S. 9 ff.

Hausfriedensbruchs" einzudämmen, (erneut) gescheitert.[369] Dies trägt der Einsicht Rechnung, dass das Strafrecht aus strukturellen Gründen nur einen geringen Beitrag zur Verbesserung der Informationssicherheitslage leisten kann. Zwar spricht aus Sicht des Gesetzgebers für die Wahl des Instruments Strafrecht dessen (potenzielle) Befriedigungsfunktion.[370] Allerdings leidet das Strafrecht mit seinen hohen verfahrensrechtlichen Anforderungen und seiner Fokussierung auf personale Verantwortlichkeit noch stärker als das Verwaltungs- und das zivile Haftungsrecht unter dem Attributionsproblem, das gerade bei nicht-standardisierten Angriffsformen jenseits der Kleinkriminalität die Ermittlung der Angreifer erschwert.[371] Die sonst zur Bewältigung des Territorialitäts- und des Attributionsproblems gewählte Strategie der Inpflichtnahme der Nichtstörer scheidet hier weitgehend aus. In der weitgehenden Anonymität des Internets verliert schließlich auch die strafrechtliche Sanktionsdrohung ihre motivierende Wirkung. So waren die Effekte der teils erheblichen Strafrechtsverschärfungen von 2007 auf die Informationssicherheitslage insgesamt minimal.

Nicht ignoriert werden dürfen zudem die unter IT-Sicherheitsgesichtspunkten kontraproduktiven Effekte einer Pönalisierung der Materie.[372] Gerade § 202c StGB, der bestimmte Vorbereitungshandlungen für die Begehung von Taten nach §§ 202a, 202b StGB, insbesondere die Erstellung von Programmen, deren Zweck die Begehung einer solchen Tat ist (§ 202c Abs. 1 Nr. 2 StGB), unter Strafe stellt, ist sehr weit formuliert und erfasst prima facie auch Handlungen bzw. Programme, die zu Ausbildungs- und Übungszwecken in der IT-Sicherheitspraxis Verwendung finden.[373] Zwar kann die Norm nach Auffassung des BVerfG restriktiv und damit verfassungskonform ausge-

[369] Ein entsprechender § 202e StGB war Teil des ersten Referentenentwurfs des BMI aus dem März 2019 zum IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0-RefE). Danach sollte bestraft werden, wer sich unbefugt Zugang zu einem informationstechnischen System verschafft (Nr. 1), dieses in Gebrauch nimmt (Nr. 2) oder einen Datenverarbeitungsvorgang oder einen informationstechnischen Ablauf auf einem informationstechnischen System beeinflusst oder in Gang setzt (Nr. 3). 2016 war bereits eine weitgehend analoge Bundesratsinitiative gescheitert. Zur Thematik näher *U. Buermeyer/S. Golla*, „Digitaler Hausfriedensbruch", K&R 2017, S. 14 ff.; *F. Stam*, Die Strafbarkeit des Aufbaus von Botnetzen, ZIS 2017, S. 547 ff.; *Singelnstein/Zech*, Schutz der IT-Sicherheit durch das Strafrecht, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 20 Rn. 30 ff.

[370] Abwägend zur Funktion des IT-Strafrechts *D. Brodowski*, Cybersicherheit durch Cyber-Strafrecht?, in: Lange/Bötticher (Hrsg.), Cyber-Sicherheit, 2015, S. 249 (250 ff.).

[371] Siehe oben § 4 II. 2. b). Dazu speziell aus strafrechtlicher Sicht *Singelnstein/Zech*, Schutz der IT-Sicherheit durch das Strafrecht, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 20 Rn. 34.

[372] Ausführlich *Golla*, IT-Sicherheit und Strafrecht, JZ 76 (2021), S. 985 ff.

[373] Der Gesetzgeber hat auch aus diesem Grund die Forschungsaktivitäten und bestimmte Untersuchungsmethoden des BSI nach § 7a und § 7b BSIG spezialgesetzlich abgesichert, vgl. näher *Keppeler*, in: Ritter (Hrsg.), Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2022, § 7a BSIG Rn. 331 ff., § 7b BSIG 382 f.

legt werden.[374] Dennoch wird sie „mit einem Rückzug der IT-Security-Szene aus der Öffentlichkeit in Verbindung gebracht, da die Motivation gesunken sei, öffentlich auf neuartige Sicherheitslücken hinzuweisen".[375] Auch § 206 StGB wird teilweise als Hindernis für den Einsatz bestimmter zur operativen Bekämpfung von IT-Sicherheitsvorfällen hilfreicher (Filter-)Technologien kritisiert.[376]

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

In der Tradition des Technikrechts setzt das Informationssicherheitsrecht in erster Linie auf Verfahrens- und Organisationsregeln, die auf die Generierung, Implementierung und Distribution technischen Wissens zielen, und lenkt die Aufmerksamkeit und Investitionen innerhalb von Organisationen. Statt selbst technische Standards zu definieren, schafft der Informationssicherheitsgesetzgeber Anreize, beseitigt Barrieren für sicherheitsorientierte Ansätze und stellt Infrastrukturen für die wechselseitige Kommunikation bereit. Allerdings kann das Recht der Informationssicherheit die tradierten Instrumente und Verfahren des Technikrechts nicht einfach übernehmen, sondern muss diese im Lichte der neuen Herausforderungen weiterentwickeln. Die Analyse der zu diesem Zweck vom Gesetzgeber unternommenen Schritte bildet den Kern dieses Kapitels. Sie hat gezeigt, welcher Weg in den vergangenen zwei Dekaden zurückgelegt worden ist und welche Lücken nach wie vor bestehen.

Die hier als maßgeblich identifizierten Grundstrukturen des Informationssicherheitsrechts dürfen daher nicht als abschließende Antwort auf das Informationssicherheitsproblem verstanden werden, sondern stellen den aktuellen Stand der Regulierung dar, die ihrerseits auf den gegenwärtigen Stand der Technik reagiert – und sich mit diesem fortentwickeln muss. Allerdings deuten die Rechtsetzungsakte der jüngsten Zeit darauf hin, dass das regulatorische „patchwork of confusion" allmählich einem strukturierteren, integrativen

[374] Zur Verfassungskonformität des § 202c siehe BVerfG, 2 BvR 2233/07 u. a. v. 18.5.2009. Pointiert *C.-F. Stuckenberg*, Viel Lärm um nichts?, wistra 2010, S. 41 (46): „Übrig bleibt eine Norm von zweifelhaftem praktischen Nutzen und beschämender Systematik, die zudem ein Lehrbuchbeispiel für gescheiterte Kommunikation zwischen dem Gesetzgeber und den von der Regelung Betroffenen darstellt".

[375] *Deutscher Bundestag*, Neunter Zwischenbericht der Enquete-Kommission „Internet und digitale Gesellschaft" – Zugang, Struktur und Sicherheit im Netz, 19.3.2013, BT Drs. 17/12541, S. 65. Vertiefend *D. Böhlke/Ö. Yilmaz*, Auswirkungen von § 202c StGB auf die Praxis der IT-Sicherheit, CR 2008, S. 261 ff.

[376] *Golla*, IT-Sicherheit und Strafrecht, JZ 76 (2021), S. 985 (986). Auch hier verfolgt § 5b BSIG für die „Bundes-MIRTs" das Ziel, eine Strafbarkeit sicher auszuschließen, vgl. *Keppeler*, in: Ritter (Hrsg.), Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2022, § 4b BSIG Rn. 254.

Vorgehen weicht. Fünf übergreifende Entwicklungstrends, die die Heterogenität der Materie nicht überwinden, aber doch einhegen und handhabbar machen,[377] sollen hier herausgehoben werden.

Erstens hat sich bestätigt, dass sich die regulatorische Dynamik in Sachen Cybersicherheit von der nationalstaatlichen auf die europäische Ebene verlagert.[378] Dies ist begrüßenswert, sorgt es doch im Verhältnis der Mitgliedstaaten für ein höheres Maß an Integration und stärkt vor allem die Effektivität der Regulierung in den für den digitalen Raum typischen grenzüberschreitenden Konstellationen. Während im Verhältnis von IT-SiG (2015) und NIS-Richtlinie (2016) zumindest in zeitlicher Hinsicht noch die Rede davon sein konnte, dass das deutsche Vorbild den europäischen Rechtsetzungsakt motiviert und inspiriert hat, geht der CSA nun dem IT-SiG 2.0 zeitlich voraus. Aber auch inhaltlich ist das IT-SiG 2.0 vergleichsweise wenig ambitioniert. Dies beruht auch darauf, dass verschiedene der im Gesetzgebungsverfahren zum IT-SiG 2.0 erwogenen und von Sachverständigen für sinnvoll befundenen Modifikationen in der endgültigen Fassung nicht enthalten waren.[379] Teilweise findet sich im IT-SiG 2.0 zudem unter IT-Sicherheitsaspekten Fragwürdiges[380] bis Kontraproduktives[381], was die Überzeugungskraft des Gesetzes schwächt. Nach wie vor wirft zudem die Stellung des BSI als eine auf Stärkung der zivilen IT-Sicherheit zielende „Ordnungsbehörde" in einem von sicherheitsbehördlichen Interessen an der Verwertung von IT-Sicherheitslücken für eigene Zwecke mitgeprägten Umfeld Fragen auf.[382] Auch wenn das IT-SiG 2.0 durch Integration von regulatorischen Ideen aus anderen Rechtsbereichen und durch „Schlüsselnormen" wie § 9a BSIG 2021, die eine Verbindung zu anderen Rechtsakten herstellen, zu einer Arrondierung des regulatorischen Terrains beiträgt, setzt es insgesamt doch (zu) wenig Impulse für eine Fortentwicklung der Materie. Demgegenüber schlagen der CSA, die NIS 2-RL sowie die weiteren angekündigten oder schon im Gesetzgebungsverfahren befindlichen Rechtsakte der Union zahlreiche neue Wege ein, die vom Zertifizierungswe-

[377] Hierzu oben § 6 I.

[378] Für einen Überblick über die gegenwärtigen Aktivitäten der Union siehe § 1 Fn. 30 sowie umfassend https://www.consilium.europa.eu/de/policies/cybersecurity/.

[379] Bemängelt wird beispielsweise verbreitet die Streichung einer in der zweiten Entwurfsfassung noch enthaltenen Pflicht des BBK zur Aufstellung von Krisenreaktionsplänen für IT-Katastrophen.

[380] Hierzu zählt auch das in § 9c BSIG 2021 eingeführte „freiwillige IT-Sicherheitskennzeichen", siehe oben § 6 Fn. 321.

[381] Kritisiert wird neben dem bereits erwähnten § 9b BSIG 2021 insbes. auch der neue § 7c Abs. 1 S. 1 Nr. 2 BSIG 2021, auf dessen Grundlage das BSI bestimmte TK-Anbieter dazu verpflichten kann, zur Abwehr von Gefahren „technische Befehle zur Bereinigung von einem konkret benannten Schadprogramm an betroffene informationstechnische Systeme" zu verteilen, vgl. *Keppeler*, in: Ritter (Hrsg.), Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2022, § 7c BSIG Rn. 387, 411 m. w. N.

[382] Siehe oben § 5 III. 2. a).

sen bis hin zur Integration der Internetsicherheit in die Informationssicherheitsregulierung reichen. Diese Relevanzsteigerung der Union bzw. des Unionsrechts spiegelt sich auch im Aufbau neuer Institutionen auf Unionsebene, darunter zuletzt das Europäische Kompetenzzentrum für Cybersicherheit sowie das Netzwerk nationaler Koordinierungszentren.

Der Bedeutungsgewinn des Unionsrechts steht nur scheinbar im Widerspruch zum *zweiten* Entwicklungstrend: Der Pluralisierung des Informationssicherheitsrechts. Gezeigt hat sich, dass die Aufgabe zu vielschichtig ist, als dass sie „aus einer Hand" geregelt werden könnte. Vielmehr ist mit ihrer Bewältigung notwendig eine Vielzahl von staatlichen und nichtstaatlichen Akteuren befasst. Dies ist nicht nur Folge der (prinzipiell änderbaren) verfassungsrechtlichen Kompetenzordnung, sondern vor allem den begrenzten Problemlösungskapazitäten funktional differenzierter Verwaltungen und Gesellschaftsordnungen geschuldet. Eine Zentralisierung der Rechtsetzung und -durchsetzung – auf welcher Ebene auch immer – ist daher kein erstrebenswertes Ziel. Vielmehr ist für jede Regulierungsebene der sachangemessene Bezugsrahmen zu wählen. Welcher dies ist, wird für unionsweit zirkulierende Produkte regelmäßig anders zu bewerten sein als für ortsfeste Betreiber kritischer Infrastrukturen.

Das leitet zum *dritten* Entwicklungstrend über: der Institutionalisierung des Informationssicherheitsrechts. Auch hier ist zu beachten, dass Institutionalisierung nicht Zentralisierung bedeutet. Letzteres allein wäre keine nachhaltige Strategie. Fraglos ist der Auf- und Ausbau spezialisierter Fachbehörden unabdingbar, um informierte und effektive Informationssicherheitsregulierung betreiben zu können. Diese dürfen jedoch nicht als Solitäre agieren, sondern müssen zu Ankerpunkten der Kooperation und Kommunikation sowohl innerhalb der Verwaltung als auch im Verhältnis zwischen hoheitlichen Stellen und Privaten werden. Stärkere Institutionalisierung bedeutet also immer auch stärkere Koordination und Kooperation. Der deutsche und der Unionsgesetzgeber haben beide diese zweispurige Entwicklung vorangetrieben, d. h. sowohl BSI bzw. ENISA gestärkt als auch deren Koordinations- und Kooperationspflichten ausgebaut.[383] Die NIS 2-RL setzt dies fort, indem sie die Rolle von ENISA nochmals stärkt und zugleich mittels des auf die Bekämpfung akuter IT-Sicherheitskrisen größeren Ausmaßes ausgelegten CyCLONe (vgl. Art. 16 NIS 2-RL) den Kooperationsgedanken stärkt. Wieder aufgenommen werden zudem einige schon in den Entwürfen zur ersten NIS-Richtlinie enthaltene Ideen, namentlich die Einrichtung eines Systems für den sicheren Informationsaustausch Art. 29 f. NIS 2-RL sowie – wenn auch zurückhaltend – eines Frühwarnsystems, das koordinierte Reaktionen ermöglicht (Art. 15

[383] Zu den entsprechenden Regelungen im IT-SiG, in der NIS-RL und im IT-SiG 2.0 siehe § 6 II. 2. c) und 3. c) und f).

Abs. 15 lit. j ii) NIS 2-RL). Dass der Grat zwischen Spezialisierung und Zersplitterung schmal und das Austarieren jeder komplexen geschaffenen Verbundstruktur überaus schwierig ist, versteht sich von selbst.[384]

Viertens setzt der Gesetzgeber die sektoralen Regime zur Informationssicherheit – Datenschutzrecht, Recht kritischer Infrastrukturen, Produktsicherheitsrecht etc. – auch bei der Aufstellung und Konkretisierung der materiellen Vorgaben zur IT-Sicherheit zunehmend miteinander in Beziehung. Beispielhaft zeigt sich das daran, dass die ursprünglich in ihrem Anwendungsbereich und in ihrem Regelungsanspruch eng begrenzten Normen zur IT-Sicherheit bei kritischen Infrastrukturen nun zu horizontalen Rechtsakten fortentwickelt werden, die zumindest alle „großen" Unternehmen adressieren[385] und zudem mehr und mehr auch Aspekte der Komponentensicherheit („Sicherheit der Lieferkette") sowie, eingeschränkt, der Internetsicherheit integrieren[386]. Diese horizontalen Rechtsakte werden dann weiter mit sektoralen Regelungen gekoppelt, sei es über Vorgaben zur Koordination der Erstellung von Sicherheitskatalogen oder über Vorschriften wie den durch das IT-SiG 2.0 eingefügten § 9a BSIG 2021, der das BSI zur Nationalen Behörde für die Cybersicherheitszertifizierung im Sinne des CSA macht (vgl. auch § 3 Abs. 1 S. 2 Nr. 5a BSIG). Hierdurch werden BSIG bzw. BSI zur Schnittstelle zwischen dem Schutz kritischer Infrastrukturen und dem Wirtschaft und Verbrauchern allgemein dienenden Recht der Cybersicherheitszertifizierung. Diese Funktion tritt neben die schon nach § 9 Abs. 1 BSIG bestehende Aufgabe des BSI als nationale Zertifizierungsstelle der Bundesverwaltung für IT-Sicherheit. Über das gemeinsame Instrument der Zertifizierung, dessen Handhabung einer Stelle – dem BSI – zugewiesen wird, erfolgt sowohl auf der Ebene der Regelsetzung wie der Regeldurchsetzung eine allmähliche Integration der unterschiedlichen regulatorischen Handlungslogiken. Ganz entsprechend koppelt auch Art. 24 NIS 2-RL an das Zertifizierungsregime des CSA an und erlegt den Mitgliedstaaten mit Blick auf die von den regulierten Entitäten einzuhaltenden technischen Standards Förderpflichten für die technische Normung auf. In diesem Sinne überbrückt das Informationssicherheitsrecht als „Querschnittsgebiet" nicht nur zahlreiche Rechtsgebiete, sondern sorgt rechtsgebietsübergreifend für einheitlicher werdende Regelungsstrukturen.[387] Den differenzierten Anforderungen der Rechtsordnung entsprechend gelten in den einzelnen Teilbereichen jedoch weiterhin unterschiedliche Maßstäbe. Konkret: Vorgaben zur Informationssicherheit für die Betreiber kritischer Infra-

[384] Siehe § 6 II. 3. c).
[385] Siehe § 6 II. 4. c) aa).
[386] Siehe § 6 II. 6 und 7.
[387] Analog zur Querschnittsnatur des Datenschutzrechts respektive des Informationsrechts *Kingreen/Kühling*, Der überspannte Parlamentsvorbehalt im Datenschutzrecht, JZ 70 (2015), S. 213; *M. Kloepfer*, Informationsrecht, 2002, § 1 Rn. 67.

strukturen lassen sich nicht ohne weiteres auf (nicht-kritische) Telemedienanbieter übertragen. Ein risikobasierter Ansatz, der funktional und sektoral genau differenziert, ist vielmehr im Informationssicherheitsrecht alternativlos.[388]

Fünftens und letztens ist es insbesondere für die europäische Ebene bemerkenswert, dass die maßgeblichen Rechtsakte konsequent einem rein defensiven IT-Sicherheitsverständnis verpflichtet sind. So sieht Art. 7 Abs. 2 lit. c NIS 2-RL eine auf nationaler Ebene bisher vergeblich geforderte Maßnahme vor, nämlich die Koordinierung der Offenlegung sogenannter „Schwachstellen"; ferner wird die Einrichtung eines bei ENISA als ziviler Behörde angesiedelten „europäisches Schwachstellenregisters" gefordert.[389] In einer primär auf Stärkung der Resilienz orientierten Cybersicherheitspolitik nimmt ein solches Transparenzregister eine wichtige Rolle ein, wird so doch gesichert, dass die – unvermeidbaren – Lücken, sobald sie aufgedeckt wurden, auch rasch behoben werden können. Ähnlich konsequent agiert die europäische Gesetzgebung beim zentralen Thema der Verschlüsselung. Deren Bedeutung wird in der NIS 2-RL mehrfach betont (ErwGr 98; Art. 21 Abs. 2 lit. h NIS 2-RL). Vor allem aber sieht der Entwurf keinerlei auf die Beeinträchtigung der Integrität von Verschlüsselungstechnologien zielende Maßnahmen vor.[390]

Dieser klare und aus Sicht der staatlichen Gewährleistungsverantwortung für die Risiken der Informationstechnik begrüßenswerte Ansatz ist angesichts der Ambivalenzen, mit denen die IT-Sicherheitspolitik allgemein konfrontiert ist, bemerkenswert.[391] Auf die größeren Unschärfen, die der deutsche Gesetzgeber hier eingeht, wurde bereits verschiedentlich hingewiesen. Und auch an anderen Stellen der Unionspolitik finden sich Aussagen, die deutlich die Kritik der Sicherheitsbehörden an starker Verschlüsselung und das Interesse an der Nutzung von Schwachstellen für eigene Zwecke reflektieren.[392] Auf die hier berührte hochkomplexe Spannungslage der staatlichen IT-Sicherheitspolitik wird jetzt einzugehen sein.

---

[388] Siehe § 6 II. 5. c).

[389] Siehe § 6 II. 3. 3).

[390] Allerdings weist ErwGr 98 NIS 2-RL für den Fall sog. Ende-zu-Ende-verschlüsselter Kommunikation auf die Spanungslage zwischen der – für den Schutz der Privatheit und die Sicherheit der Kommunikation essenziellen – Wirksamkeit der Verschlüsselung einerseits und dem Bedürfnis der Strafverfolgung nach einem Zugriff auf diese Kommunikationen hin. Auch auf dieses Problem wird unter § 7 III noch zurückzukommen sein.

[391] Siehe oben § 1 III.

[392] Vgl. nur *Europäische Kommission/Hoher Vertreter der Union für Außen- und Sicherheitspolitik*, Die Cybersicherheitsstrategie der EU für die digitale Dekade, JOIN(2020) 18 final, S. 16. Auch der NIS 2-RL-E lässt im Übrigen offen, inwieweit CSIRTs zu sogenannten Hackbacks ermächtigt werden dürfen, vgl. die nach wie vor unklare Formulierung in Art. 11 Abs. 3 lit. c NIS 2-RL; dazu *Kipker/Birreck/Niewöhner/Schnorr*, NIS-Richtlinie und der Entwurf der NIS-2-Richtlinie, MMR 2021, S. 214 (215).

§ 7 Sicherheitsgewährleistung durch Manipulation der Informationstechnik?

> „States can and do control cyberspace when it suits them – and often with a heavy hand."[1]
>
> „The rapidly growing and highly dynamic mobile communications market – characterized by the introduction of new devices, operating systems and applications on virtually a daily basis – requires a rethinking of the traditional intelligence paradigm. These changes in the communications landscape pose real challenges and obstacles that must be overcome by intelligence organizations and law enforcement agencies worldwide."[2]

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

Staatliche Maßnahmen, die die Schutzziele der Informationssicherheit aushebeln oder kompromittieren, sind in der Öffentlichkeit weit präsenter als die Bemühungen hoheitlicher Stellen um eine Verbesserung der IT-Sicherheitslage. Aus rechtlicher Sicht müssen jedoch beide Handlungsperspektiven zusammengedacht werden, schon weil die Verantwortung des Staates für sichere Informationsinfrastrukturen die wichtigste Grenze für staatliche Eingriffe in die IT-Sicherheit ist. Tatsächlich aber sind staatliche Akteure heute neben Hackern, Hacktivisten und Kriminellen die wichtigsten „Autoren" von Cyber-Unsicherheit.[3] Im globalen Zusammenhang lässt sich beobachten, dass Staaten aus ganz unterschiedlichen innen- oder außenpolitischen Motiven letztlich alle technisch möglichen Angriffsvektoren ausnutzen, d. h. sich der Schwachstellen von Komponenten, Systemen, Netzwerken und der Internetinfrastruktur bedienen, um Systeme zu infiltrieren, Malware zu verbreiten, Botnetze zu

---

[1] *Finnemore/Hollis*, Constructing Norms for Global Cybersecurity, AJIL 110 (2016), S. 425 (460).

[2] *NSO*, Pegasus – Product Description, 2019, S. 7.

[3] So *Finnemore/Hollis*, Constructing Norms for Global Cybersecurity, AJIL 110 (2016), S. 425 (434 f.). Hierzu bereits oben im Kontext des Attributionsproblems unter § 4 II. 2. b).

betreiben etc.[4] Dank ihrer Ressourcen verfügen staatliche Akteure im wissensintensiven Geschäft der Cybergefährdung oft sogar über besonders potente technische Instrumente. Darüber hinaus haben staatliche Akteure die einzigartige Möglichkeit, mittels ihrer Rechtsmacht das eigene Handeln zu legalisieren und – noch wichtiger – private Verteidigungsmaßnahmen erschweren oder sogar untersagen zu können.

Im europäischen Kontext nutzen Staaten derartige Maßnahmen bisher meist zum Zweck der Gefahrenabwehr oder zur Strafverfolgung. So gab das Instrument der Online-Durchsuchung bereits 2007 Anlass zur Selbstvergewisserung des Verfassungsrechts über die grundrechtliche Dimension der IT-Sicherheit. Wachsende Bedeutung haben Manipulationen der IT-Sicherheit auch für die Gewinnung nachrichtendienstlicher Erkenntnisse im Rahmen der sogenannten Informationsvorsorge erlangt. Eine besondere Zuspitzung erfährt die Problemstellung bei zwischenstaatlichen Konfrontationen.[5]

In demokratischen Gemeinwesen stehen derartige staatliche Handlungen unter genauer Beobachtung. Dies betrifft in erster Linie ihre Vereinbarkeit mit den Vorgaben des Verfassungsrechts. Wie bei allen eingriffsintensiven Maßnahmen muss geprüft werden, ob sich die konkreten Maßnahmen in dem oben aufgezeigten grund- und kompetenzrechtlichen Rahmen bewegen.[6] Die fachwissenschaftliche Debatte über einzelne Instrumente wie die Online-Durchsuchung, die Quellen-TKÜ oder die Quellen-TKÜ Plus wird insoweit intensiv geführt. Allerdings stellt sich hierbei rasch die grundsätzlichere Frage, ob staatliche Beeinträchtigungen der Informationssicherheit überhaupt möglich sind, ohne dass die gleichzeitigen Bemühungen um eine Stärkung der Informationssicherheit nicht nur relativiert, sondern konterkariert werden. Kritisiert wird also nicht (nur), dass der Staat mit dem Einsatz entsprechender Instrumente übermäßig in Freiheitsrechte eingreift bzw. für spezifische Konstellationen falsche Abwägungen trifft. Befürchtet wird vielmehr, dass der Staat, indem er die IT-Sicherheit kompromittiert und Sicherheitslücken ausnutzt,

[4] Zum Panorama möglicher Angriffshandlungen siehe oben § 6 II. 1. b). Prominentes Beispiel für einen hoheitlichen Eingriff deutscher Stellen in die System- und Netzwerksicherheit Privater ist die durch Medienberichte dokumentierte Nutzung des Überwachungsprogramms „Pegasus" durch das BKA; siehe dazu *H. Stark*, BKA kaufte heimlich NSO-Spähsoftware, Die Zeit, 7.9.2021, sowie aus technischer Sicht *Amnesty International*, Forensic Methodology Report, 18.7.2021. Das Europäische Parlament hat zur Nutzung der von der in Israel ansässigen Firma NSO Group Technologies entwickelten Software durch zahlreiche Mitgliedstaaten der Union am 10.3.2022 einen Untersuchungsausschuss eingesetzt (2022/2586(RSO)). Als Beispiel für einen staatlichen Eingriff in die Internetsicherheit in Gestalt des BGP-Highjacking (siehe § 6 Fn. 91) wurden jüngst die Bemühungen Russlands, den Internetverkehr der Ukraine zu Überwachungszwecken über eigene Server umzuleiten, beschrieben; siehe dazu *Federal Communications Commission*, Notice of Inquiry, In the matter of Secure Internet Routing, FCC 22–18 v. 28.2.2022.

[5] Siehe oben § 2 I. 4.

[6] Siehe oben § 5 I. 2.

das Fundament der Digitalisierung beschädigt – mit unübersehbaren Folgen für Staat und Gesellschaft.

Damit drängt sich die Frage auf, ob der demokratische Verfassungsstaat tatsächlich auf Dauer eine Doppelrolle als Garant und als Gefährder der Informationssicherheit spielen kann oder ob er sich für eine Seite entscheiden muss. Diese Frage soll im Folgenden im Mittelpunkt stehen. Es geht also nicht darum, einzelne gesetzliche Verbots- oder Eingriffsnormen auf ihre Verfassungsmäßigkeit hin zu prüfen. Herauszuarbeiten ist vielmehr, ob und inwieweit solche Maßnahmen strukturell die staatliche Gewährleistungsverantwortung für die Informationssicherheit unterminieren. Dies betrifft allgemein all jene staatlichen Maßnahmen, die IT-Schwachstellen für eigene Zwecke nutzen (II.), sowie speziell solche Vorhaben, welche die Integrität von Verschlüsselungsverfahren – Fundament jeder sicheren IT-Architektur – beeinträchtigen (III.).

II. Staatliche Governance von IT-Schwachstellen

Überall dort, wo IT-Sicherheit mit der Verfolgung staatlicher Interessen kollidiert, steht im Raum, dass der Staat erstere opfert, um letztere zu realisieren. Angesichts der Ubiquität informationstechnischer Systeme gibt es wenige Bereiche, die den damit einhergehenden Abwägungen von vornherein entzogen sind. In der Praxis beschränkt sich das Interesse staatlicher Stellen hierzulande allerdings meist noch auf solche technischen Maßnahmen, die den Schutz, den IT-basierte Kommunikation vor einer Kenntnisnahme durch Dritte gewährt, überwinden können.[7] So werden staatliche Eingriffe in die IT-Sicherheit aktuell primär im Zusammenhang mit dem verfassungsrechtlichen Schutz der Privatheit diskutiert. Im Zuge der Analyse der für das Recht der Informationssicherheit prägenden Grundrechtsgarantien wurde allerdings bereits darauf hingewiesen, dass die Problematik potenziell weit über Beeinträchtigungen der Privatheit hinausweist.[8]

Ungeachtet der Vielzahl möglicher Einsatzkontexte und -motive eint die Maßnahmen auf technischer Ebene, dass staatliche Stellen mit IT-Schwachstellen operieren müssen, um in die Zielsysteme eindringen und dort ihre Späh- oder sonstigen Schadprogramme einbringen zu können. Anders als bei den im vorigen Kapitel geschilderten hoheitlichen Interventionen wird das staatliche Know-how also nicht dafür eingesetzt, erkannte Schwachstellen zu beherrschen und zu beseitigen. Vielmehr verschafft sich der Staat Kenntnis

[7] Siehe oben § 5 I. 2.

[8] Zur „Kehrseite", d. h. den grundrechtlich geschützten Belangen, die bei entsprechenden staatlichen Handlungen aktiviert werden, siehe oben § 5 Fn. 37.

von Schwachstellen,[9] sieht dann jedoch – abweichend von den Grundregeln des IT-Sicherheitsrechts[10] – von deren Veröffentlichung ab, was Dritten die Möglichkeit zur Beseitigung oder zum Ergreifen vorbeugender Maßnahmen gäbe, sondern nutzt diese Schwachstellen für eigene Zwecke. Hierdurch werden nicht nur jene Rechtsgüter gefährdet, die unmittelbares Ziel der staatlichen Maßnahmen sind, etwa die Privatheit, sondern auch die IT-Sicherheit (1.). Diese IT-sicherheitsspezifischen Risiken werden in der rechtlichen Diskussion bisher nicht angemessen verarbeitet, wie hier am Beispiel der sogenannten Quellen-Telekommunikationsüberwachung (TKÜ) – aktuell wohl der „Standardmaßnahme" für Eingriffe in die IT-Sicherheit – erläutert werden soll (2.). Es ist daher geboten, im Lichte der staatlichen Gewährleistungsverantwortung für die IT-Sicherheit einerseits und der für die Nutzung von Schwachstellen streitenden Gründe andererseits allgemein tragfähige Leitlinien für die staatliche „Governance" von IT-Schwachstellen[11] zu entwickeln (3.).

1. Implikationen der Nicht-Offenlegung und Nutzung von Schwachstellen für die IT-Sicherheit: Kollisions-, Proliferations- und Einsatzrisiken

Die Nutzung von Kenntnissen über informationssicherheitsrelevante Schwachstellen von Programmen, Systemen, Netzwerken etc. kann einzelne staatliche Akteure – vor allem solche des Sicherheitssektors – in bestimmten Kontexten in die Lage versetzen, die ihnen zugewiesenen Aufgaben effektiver zu erfüllen.[12] Besonders hilfreich sind sogenannte Zero-day-Schwachstellen, d. h. Schwachstellen, die Herstellern und Öffentlichkeit unbekannt sind, sodass typischerweise keine Abwehrmaßnahmen in Form von Patches oder Ähnlichem zur Verfügung stehen.[13] Nutzen staatliche Akteure entsprechende Schwachstellen, erzeugt dies drei Arten IT-sicherheitsspezifischer Risiken:

[9] Wie sich der Staat diese Kenntnisse *verschafft*, soll hier nicht im Vordergrund stehen. Vgl. dazu *M. Schulze*, Governance von 0-Day-Schwachstellen in der deutschen Cyber-Sicherheitspolitik, SWP-Studie, Mai 2019, S. 14 ff. Analysiert wird hier, wie der Staat mit entsprechenden Kenntnissen über Schwachstellen *umgeht*. Als „Vehikel" zur Akquise von Schwachstellen ist insbes. die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) konzipiert, siehe dazu oben § 1 Fn. 23.

[10] Siehe oben § 6 II. 3. e) m. w. N. zu den Informations- und Warnbefugnissen des Staates.

[11] Zur Forderung nach einer staatlichen Schwachstellen-Governance programmatisch *Schulze*, Governance von 0-Day-Schwachstellen in der deutschen Cyber-Sicherheitspolitik, SWP-Studie, Mai 2019.

[12] Für Schätzungen zur Größenordnung der Problematik siehe *J. Healey*, The U.S. Government and Zero-Day Vulnerabilities, Journal of International Affairs 67:11 (2016), S. 1 ff.

[13] Zum Begriff näher *Schulze*, Governance von 0-Day-Schwachstellen in der deutschen Cyber-Sicherheitspolitik, SWP-Studie, Mai 2019, S. 7. Das Spektrum der 0-Day-Schwachstellen reicht von solchen, die zwar bekannt, aber noch in keinem der dafür geschaffenen Re-

Erstens kann oft nicht sicher ausgeschlossen werden, dass die von staatlichen Stellen gefundenen oder erworbenen Schwachstellen Dritten bereits bekannt sind und von diesen genutzt werden. Unterlässt der Staat die Veröffentlichung der Schwachstellen, um sie für eigene Zwecke zu nutzen, führt dies daher unter Umständen dazu, dass auch Dritte diese Lücken weiterhin ungestört ausnutzen. In Übereinstimmung mit dem in der Technik üblichen Sprachgebrauch soll dies hier als *Kollisionsrisiko* bezeichnet werden.[14] Das Risiko ist besonders hoch, wenn staatliche Stellen ihre Kenntnis von den Lücken nicht durch eigene Forschungsaktivitäten, sondern durch ausländische Partnerdienste oder auf den dafür existierenden schwarzen und grauen Märkten erworben haben.[15] In diesen Fällen liegt es auf der Hand, dass nicht nur die eigenen Behörden, sondern auch alle möglichen sonstigen staatlichen und nichtstaatlichen Akteure die Schwachstellen einsetzen – womöglich auch gegen die hiesige Bevölkerung. Entscheidet sich der Staat hier gegen eine Veröffentlichung, nimmt er die Beeinträchtigung dieser Nutzer durch Dritte jedenfalls billigend in Kauf.

Zweitens ist selbst dann, wenn staatliche Stellen ausnahmsweise über einen genuinen Forschungs- und Wissensvorsprung verfügen, das Vorhalten von Schwachstellen auf staatlichen Systemen mit Blick auf die IT-Sicherheitslage riskant, kann das behördliche Wissen doch seinerseits durch Cyberangriffe erobert oder sonst unbefugt in Verkehr gebracht werden. Die Aufmerksamkeit für dieses *Proliferationsrisiko* ist insbesondere nach dem Angriff der sogenannten „Shadow Brokers"-Gruppe auf die U. S. National Security Agency

---

positorien dokumentiert sind (vgl. dazu im Überblick https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/vulnerabilities-and-exploits), über Schwachstellen, die auf grauen oder schwarzen Märkten verfügbar, aber den Herstellern selbst noch nicht bekannt sind (sodass keine Abhilfe erfolgen kann), bis hin zu Schwachstellen, die exklusiv nur einer Instanz bekannt sind (im Jargon der NSA: „Nobody, but us", vgl. *B. Buchanan*, Nobody But Us: The Rise and Fall of the Golden Age of Signals Intelligence, Aegis Series Paper No. 1708, 30.8.2017). Einen instruktiven Gesamtüberblick bieten *L. Ablon/A. Bogart*, Zero Days, Thousands of Nights, 2017.

[14] Zum öfter zu beobachtenden Phänomen, dass mehrere Akteure eine Schwachstelle unabhängig voneinander entdecken – im Fachjargon eine sog. Kollision –, siehe *B. Schneier*, Simultaneous discovery of vulnerabilities, Februar 2016; *T. Herr/B. Schneier/C. Morris*, Taking Stock: Estimating Vulnerability Rediscovery, Revised Version, 2017; *S. Herpig*, Schwachstellen-Management für mehr Sicherheit, 27.8.2018, S. 29 f.

[15] Eine instruktive Bestandsaufnahme der „weißen" und „grauen" Märkte, die sich für Software-Schwachstellen etabliert haben, gibt *J. Meakins*, A Zero-sum Game, Journal of Cyber Policy 4:1 (2019), S. 60 ff.; siehe auch *Schulze*, Governance von 0-Day-Schwachstellen in der deutschen Cyber-Sicherheitspolitik, SWP-Studie, Mai 2019, S. 14 ff. m. w. N. Zu Vorschlägen für eine Regulierung dieses Marktes siehe *P. Stockton/M. Golabek-Goldman*, Curbing the Market for Cyber Weapons, Yale L. & Pol'y Rev. 32:1 (2013), S. 239 ff.; *J. Kesan/C. Hayes*, Bugs in the Market, Arizona L. Rev. 58:3 (2016), S. 753 ff.; *M. Wolf/N. Fresco*, Ethics of the Software Vulnerabilities and Exploits Market, The Information Society 32:4 (2016), S. 269 ff.

(NSA), bei dem Schwachstellen aus dem NSA-Arsenal entwendet wurden, in den Fokus der Öffentlichkeit gerückt.[16] Spätestens mit der Bevorratung von Schwachstellen erzeugt der Staat somit aktiv eigene Risiken für die IT-Sicherheit, die je nach Verbreitungsgrad der betroffenen Systeme oder Anwendungen eine unterschiedlich große Zahl von Akteuren in Wirtschaft und Gesellschaft betreffen. Erhöht wird damit auch das Sanktions- und Haftungsrisiko, das die Hersteller der mit Schwachstellen behafteten Komponenten bzw. die System- und Netzwerkbetreiber tragen, die die Schwachstellen mangels Kenntnis nicht beseitigen können. Gefährdet sind im Übrigen auch jene staatlichen Akteure, die keinen privilegierten Zugang zu den Kenntnissen erhalten und dementsprechend nicht präventiv mitigierend tätig werden können.

Entscheiden sich staatliche Stellen dann für die eigene Nutzung der Schwachstellen, etwa in Gestalt der Quellen-TKÜ, geht damit ein *drittes* IT-sicherheitsspezifisches Risiko einher. Denn die von staatlichen Stellen genutzten Schwachstellen können Manipulationen der Zielsysteme ermöglichen, die über das von der Maßnahme Bezweckte bzw. das von Rechts wegen Zulässige hinausgehen. Die Technik kann dann mehr als die Behörde darf. Dieses hier sogenannte *Einsatzrisiko* ist eng mit dem regelmäßig nicht-IT-sicherheitsspezifischen Zweck der Maßnahme (etwa dem Eingriff in die Privatsphäre) verbunden, muss aber separat gewürdigt werden.

Im Rahmen der Risikobewertung ist ferner zu berücksichtigen, dass Zero-day-Schwachstellen nicht der einzige Weg sind, um IT-Systeme und Netzwerke zu kompromittieren. Die ganz überwiegende Zahl von Attacken auf IT-Systeme bedient sich vielmehr bereits bekannter Schwachstellen („N-day-Schwachstellen").[17] Dies ist möglich, weil eine Vielzahl von Systemen und Diensten auch nach Veröffentlichung der Schwachstellen für diese verwundbar bleibt. Ursache dafür kann sein, dass die technische Anpassung auf sich warten lässt, dass die ursprünglich für das Produkt verantwortlichen Stellen die Unterstützung des Dienstes bereits eingestellt haben, dass die zur Verfügung gestellten Patches schlicht nicht genutzt werden etc. Aus diesen Gründen sind auch N-day-Schwachstellen für staatliche Akteure eine attraktive Ressource.[18] Die Struktur der durch die Nutzung von N-day-Schwachstellen erzeugten Risiken unterscheidet sich jedoch teilweise von den Zero-day-Risiken: So hat sich das Kollisionsrisiko von Zero-day-Schwachstellen bereits rea-

[16] Vgl. zu den „Verlusten" der NSA durch die Angriffe der sog. „Shadow Brokers"-Gruppe die Darstellung unter https://en.wikipedia.org/wiki/The_Shadow_Brokers. Siehe auch die Reportage von *E. Nakashima/C. Timberg*, NSA officials worried about the day its potent hacking tool would get loose. Then it did, Washington Post, 16.5.2017.

[17] Hierzu ausführlich *Schulze*, Governance von 0-Day-Schwachstellen in der deutschen Cyber-Sicherheitspolitik, SWP-Studie, Mai 2019, S. 20.

[18] Dazu näher *Herpig*, Schwachstellen-Management für mehr Sicherheit, 27.8.2018, S. 10 f., 24 ff. Siehe dazu auch das Beispiel bei *ders.*, Government Hacking, Juni 2017, S. 9 f.

lisiert, besteht allerdings weiterhin in geringerem Maße, wenn man davon ausgeht, dass durch staatliche Warnungen Abhilfemaßnahmen weitere Verbreitung fänden. Das Proliferationsrisiko ist ebenfalls reduziert, allerdings nicht auf Null, soweit die Erbeutung der Schwachstellen bei staatlichen Stellen geringere Kosten als der Erwerb am freien Markt verursacht. Keine wesentlichen Unterschiede bestehen hingegen beim Einsatzrisiko. Den unterschiedlichen Risikostrukturen ist bei der Ausgestaltung der Schwachstellen-Governance Rechnung zu tragen.

2. Zur staatlichen Nutzung von Schwachstellen am Beispiel der Quellen-TKÜ

Mit den Befugnisnormen zur Durchführung einer „Quellen-TKÜ" hat der Sicherheitsgesetzgeber auf die Sorge der Behörden reagiert, durch die zunehmende Verlagerung individueller Kommunikation ins Digitale von bisher zugänglichen Informationsquellen abgeschnitten zu werden („going dark").[19] Insbesondere durch den Einsatz von Ende-zu-Ende-Verschlüsselung laufen die herkömmlich beim Telekommunikationsmittler ansetzenden Überwachungsmethoden ins Leere (vgl. §§ 170 f. TKG), haben diese Mittler doch auf die auf diese Weise verschlüsselten Daten selbst unter keinen Umständen Zugriff.[20] Daher werden die Behörden nun ermächtigt, direkt auf den beteiligten Endgeräten Software zu installieren, mit deren Hilfe die Telekommunikation bereits an der „Quelle" bzw. an der „Mündung" abgeschöpft werden kann.[21]

[19] Die Prägung der Formulierung wird üblicherweise mit der „Going Dark: Lawful Electronic Surveillance in the Face of New Technologies" betitelten Anhörung eines Unterausschusses des Committee on the Judiciary des U.S.-Repräsentantenhauses am 17.2.2011 in Verbindung gebracht, dokumentiert unter https://www.govinfo.gov/content/pkg/CHRG-112hhrg64581/pdf/CHRG-112hhrg64581.pdf. Ausführlich zur Debatte in den USA sowie zur Kritik an der Plausibilität des Going Dark-Szenarios *Berkman Center for Internet & Society*, Don't Panic. Making Progress on the "Going Dark" Debate, 1.2.2016; siehe aus deutscher Sicht auch *M. Schulze*, Going Dark?, Parl Beilage, Nr. 46–47 2017, S. 23 ff. Programmatisch für die deutsche sicherheitsbehördliche Perspektive: *T. Haldenwang/R. Postberg*, „Going Dark", in: Sauerland/Leppek (Hrsg.), FS Bönders, 2019, S. 51 ff. Entsprechend auch der Vortrag von Bundes- und Landesregierung im Verfahren BVerfG, 1 BvR 2771/18 v. 8.6.2021, Rn. 12 ff. (insoweit nicht abgedruckt in NVwZ 2021, 1361). Vertiefend dazu gleich noch mit Blick auf die Rolle von Verschlüsselungstechnologien unter § 7 III.

[20] Zum Begriff sowie zur Abgrenzung von Ende-zu-Ende- und Transport-Verschlüsselung siehe *BSI*, E-Mail Verschlüsselung, ohne Datum.

[21] Aus dem Bundesrecht vgl. § 100a Abs. 1 Satz 2 und 3 StPO; § 51 Abs. 2 BKAG; § 11 Abs. 1a G 10; § 72 Abs. 3 ZfdG. Zum gescheiterten § 27d BPolG-E siehe *Guckelberger*, in: Schmidt-Bleibtreu/Hofmann/Henneke, GG, 15. Aufl. 2022, Art. 10 Rn. 59. Aus dem Landesrecht siehe nur beispielhaft Art. 42 Abs. 2 S. 1 BayPAG; § 54 Abs. 2 PolG BW; § 15b HSOG.

Die Debatte um die Zulässigkeit derartiger Maßnahmen wird in der Rechtswissenschaft intensiv geführt. Die Einsatz-, Kollisions- und Proliferationsrisiken, die sich mit dem staatlichen Schwachstelleneinsatz verbinden, werden in der bisherigen Debatte allerdings nur teilweise überzeugend adressiert.

a) Unvollständige Würdigung der Einsatzrisiken

In technischer Hinsicht verlangt die Durchführung einer Quellen-TKÜ in aller Regel, dass die Behörden Schwachstellen der Zielsysteme oder sonstige Sicherheitslücken ausnutzen.[22] Die Eingriffsnormen formulieren zu den technischen Aspekten des Eindringens in das Zielsystem allerdings meist nur ganz generisch, dass „mit technischen Mitteln in von dem Betroffenen genutzte informationstechnische Systeme eingegriffen [werden darf], wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen" (§ 100a Abs. 1 S. 2 StPO). Weitere Vorgaben zur Technik macht der Gesetzgeber nicht. Stattdessen konzentriert er sich ebenso wie die verfassungsgerichtlichen[23] und die überwiegende Zahl der rechtswis-

[22] Anschaulich dazu BVerfG, 1 BvR 2771/18 v. 8.6.2021, Rn. 5 (insoweit nicht abgedruckt in NVwZ 2021, 1361): „Die Ausnutzung von Sicherheitslücken im informationstechnischen System ist eine von mehreren Möglichkeiten, wie eine Quellen-Telekommunikationsüberwachung nach § 54 PolG BW durchgeführt werden kann. Zur Ermöglichung einer solchen Überwachung muss das Zielsystem mit einer Überwachungssoftware infiltriert werden. Auf welche Weise dies geschieht, ist gesetzlich nicht geregelt. Denkbar ist eine Infiltration auf physischem Weg. Dabei wird die Software durch einen Ermittler vor Ort auf das Zielsystem aufgespielt, etwa nach einem heimlichen Betreten der Wohnung, einem Zugang zur Wohnung durch verdeckte Ermittler oder außerhalb der Wohnung beispielsweise bei einer Zoll- oder Verkehrskontrolle. Alternativ kann das Zielsystem über einen Fernzugriff infiltriert werden. Dies kann geschehen, indem der Zielperson die Infiltrationssoftware als E-Mail-Anhang zugespielt und dann von dieser Person geöffnet wird oder indem Sicherheitslücken in der Hard- oder Software des Zielsystems ausgenutzt werden. Letzteres kann insbesondere im Vergleich zu den sich aus Art. 13 GG ergebenden Grenzen für ein physisches Betreten der Wohnung und zu Zugriffen, die ein Fehlverhalten des Nutzers voraussetzen, praktische Vorteile bieten."

Aus IT-Sicherheitsperspektive unterscheiden sich Quellen-TKÜ und Online-Durchsuchung kaum, muss doch auch erstere die Daten auf den IT-Systemen der Betroffenen vor deren Verschlüsselung, also vor Einleiten des konkreten Übertragungsvorgangs, bzw. nach Abschluss der Kommunikation, also nach der Entschlüsselung, abgreifen können, wozu typischerweise ein weitreichender Zugriff auf das IT-System selbst erforderlich ist. Dazu aus technischer Sicht näher *Hauser*, Das IT-Grundrecht, 2015, S. 32 ff.; *Freiling/Safferling/Rückert*, Quellen-TKÜ und Online-Durchsuchung, JR 2018, S. 9 (16 ff.); *A. Schlegel*, Normative Grenzen für internetbasierte Ermittlungsmethoden, 2019, S. 99 ff.

[23] Hierzu BVerfGE 120, 274 (309, Rn. 190); 141, 220 (309, Rn. 228). Gegen § 100a Abs. 1 S. 2 StPO in der Fassung des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17.8.2017 (BGBl. I S. 3202) ist derzeit eine Verfassungsbeschwerde mit dem Az. 2 BvR 897/18 anhängig.

senschaftlichen[24] Stellungnahmen auf Umfang und Grenzen der Verarbeitung der mittels solcher Eingriffe gewonnenen Daten. Diskutiert wird vor diesem Hintergrund etwa, ob der Gesetzgeber den behördlichen Zugriff auf solche Daten im Zielsystem erweitern darf, die dort auch nach Abschluss des Telekommunikationsvorgangs gespeichert bleiben.[25] Auch der Umfang des Kernbereichsschutzes ist Thema.[26]

Doch auch wenn es sich bei der Quellen-TKÜ aus Sicht der handelnden Behörden um ein funktionales Äquivalent zur hergebrachten TKÜ handeln mag, darf nicht aus dem Blick geraten, dass die eingesetzten Mittel riskanter sind als hergebrachte Überwachungsinstrumente. Dies lässt das Bundesverfassungsgericht bereits insofern außer Acht, als es den Einsatz der Quellen-TKÜ nur auf seine Vereinbarkeit mit Art. 10 GG und nicht auch mit dem IT-Grundrecht prüfen will.[27] Diese Regelung zur Grundrechtskonkurrenz ist angesichts der besonderen Schwere des gleichzeitigen Eingriffs in das IT-Grundrecht des Betroffenen nicht sachgerecht.[28] Der Eingriff in das IT-Grundrecht wird auch durch eine rechtliche Beschränkung der Zugriffsmöglichkeiten auf die laufende Kommunikation nicht aufgehoben, sondern bedarf einer eigenständigen Rechtfertigung; entsprechende rechtliche Beschränkungen sind gegebenenfalls im Rahmen der Verhältnismäßigkeitsprüfung zu berücksichtigen.

Darüber hinaus erfährt das mit dem Einsatz der Quellen-TKÜ verbundene Risiko einer „überschießenden" Überwachung keine adäquate Behandlung. Dieses Einsatzrisiko entsteht, wenn die handelnde Behörde die Funktionalitäten der Software nicht umfassend nachvollziehen und insbesondere Fehl- oder Fremdnutzungen des Einsatzes, etwa durch die damit beauftragten Dienstleister, nicht sicher ausschließen kann.[29] Das Bundesverfassungsgericht hebt insoweit zwar hervor, dass die Quellen-TKÜ auf laufende Telekommunikationsvorgänge beschränkt bleiben *muss*. Ob und wie dies technisch gesichert werden kann, will das Gericht jedoch nicht prüfen; dies betreffe nur „die Anwendung

[24] Siehe neben den bereits zitierten Beiträgen insbes. auch *Roggan*, Die strafprozessuale Quellen-TKÜ und Online-Durchsuchung, StV 2017, S. 821 *ff.*; *von zur Mühlen*, Zugriffe auf elektronische Kommunikation, 2019, S. 62 ff.; *M. Martini/S. Fröhlingsdorf*, Catch me if you can, NVwZ-Extra 24 2020, S. 1 ff.

[25] Dies dürfte auszuschließen sein. Hochproblematisch ist daher § 100a Abs. 5 Nr. 1b StPO, der aufgrund der oft längeren Frist, die zwischen rechtlicher Anordnung der Maßnahme und faktischem Zugriff liegt, die Erhebung aller Daten ab Anordnung der Maßnahme ermöglicht.

[26] Dazu oben § 5 Fn. 59.

[27] Vgl. BVerfGE 141, 220 (311, Rn. 234). Kritisch *Martini*, in: v. Münch/Kunig, GG, 7. Aufl. 2021, Art. 10 Rn. 196 f. Eine gewisse Öffnung ist jetzt erkennbar in BVerfG, NVwZ 2021, 1361, Rn. 29.

[28] Vgl. *Wischmeyer*, in: Dreier, GG, Bd. I, 4. Aufl., i. E., Art. 10 Rn. 125.

[29] Vgl. den entsprechenden Parteivortrag bei BVerfG (K), 1 BvR 1552/19 v. 20.1.2022, Rn. 7.

der Norm, nicht aber ihre Gültigkeit."[30] Dies würde überzeugen, wenn die rechtlichen Vorgaben unproblematisch technisch umgesetzt werden könnten. Das ist jedoch keineswegs der Fall. Die Einbringung von Quellen-TKÜ-Software ist kein minimalinvasiver Eingriff, sondern kompromittiert ein informationstechnisches System grundlegend;[31] es bedarf daher eines erheblichen technischen Aufwands und technisch fehlbarer Filter, um „nur" die laufende Kommunikation abzuschöpfen.[32] Vor diesem Hintergrund läge es sowohl unter Bestimmtheits- als auch unter Verhältnismäßigkeitsgesichtspunkten nahe, dass auch die Geltung einer Befugnisnorm in Frage steht, wenn diese gar keine Vorgaben zu technischen und organisatorischen Sicherungsmechanismen enthält, mit deren Hilfe die Behörden die Risiken der von ihnen eingesetzten Technik überschauen und beherrschen können.[33] Soweit das Gericht in einer jüngeren Entscheidung darauf verweist, dass das Bundeskriminalamt zur Einhegung des Einsatzrisikos einen „Gesamtabnahmeprozess" vorsehe, ist damit kein hinreichender Sicherungsmechanismus benannt.[34] Offen ist bereits, welche rechtliche Bindungswirkung dieser in Form eines auf der Homepage des Bundeskriminalamts veröffentlichten Schreibens dokumentierte „Prozess" überhaupt erzeugt.[35] Auch inhaltlich enthält das referenzierte Dokument nur wenige belastbare Ausführungen und misst zudem an entscheidenden Punkten den Eigenerklärungen der externen Dienstleister ein hohes Gewicht bei. Angesichts des erheblichen Kompetenzgefälles zwischen staatlichen Behörden und privaten Dienstleistern sowie der spezifischen Marktdynamiken im Bereich IT-basierter Überwachungsdienstleistungen erscheint das Vertrauen des BVerfG auf die grundrechtssichernde Funktion dieses „Gesamtabnahmeprozesses" daher nicht gerechtfertigt.[36] Insgesamt werden die IT-sicherheitsbezogenen Einsatzrisiken der Quellen-TKÜ bisher nur unvollständig gewürdigt.

---

[30] Vgl. BVerfGE 141, 220 (311, Rn. 234).

[31] Siehe hierzu die instruktive Aufbereitung des „Telegram"-Falls bei *Herpig*, Government Hacking, Juni 2017, S. 7 ff.

[32] Siehe oben § 7 Fn. 22.

[33] Vgl. für eine entsprechende Argumentation mit dem Bestimmtheitsgebot und dem Verhältnismäßigkeitsgrundsatz im Kontext der Erhebung von Kommunikationsdaten oben § 5 Fn. 56 ff.

[34] Vgl. BVerfG (K), 1 BvR 1552/19 v. 20.1.2022, Rn. 19. Gemeint ist wohl *BKA*, Standardisierende Leistungsbeschreibung für Software zur Durchführung von Maßnahmen der Quellen- Telekommunikationsüberwachung und der Online- Durchsuchung, 5.10.2018.

[35] Schwer nachvollziehbar ist auch, weshalb die Auseinandersetzung mit diesem Dokument Gegenstand des Begründungserfordernisses nach § 23 Abs. 1 Satz 2, § 92 BVerfGG sein soll; so aber BVerfG (K), 1 BvR 1552/19 v. 20.1.2022, Rn. 19.

[36] Dies drängt sich jedenfalls mit Blick auf den Fall „Pegasus" auf, vgl. oben § 7 Fn. 4.

b) Vernachlässigung der Kollisions- und Proliferationsrisiken

Gleiches gilt für die mit der staatlichen Verwertung von Schwachstellen verbundenen Kollisions- und Proliferationsrisiken. Diese wurden zwar jüngst vor dem Bundesverfassungsgericht erstmals thematisiert.[37] Gegenstand des einschlägigen Verfassungsbeschwerdeverfahrens war § 54 Abs. 2 PolG BW, eine in ihren Grundstrukturen § 100a Abs. 1 S. 2 StPO stark angenäherte Ermächtigungsgrundlage, die den Einsatz der Quellen-TKÜ für Zwecke der Gefahrenabwehr gestattet. Die Beschwerdeführer hatten in ihrer Gesetzesverfassungsbeschwerde ausdrücklich eine Verletzung der aus dem IT-Grundrecht rührenden Schutzpflicht gerügt und dies damit begründet, dass die Norm einen Anreiz für Behörden und Sicherheitsforschung setze, entdeckte Schwachstellen nicht den jeweiligen Herstellern bzw. Betreibern zu melden, sondern für eigene Zwecke zu nutzen bzw. an die Behörden zu veräußern. Darin liege eine wenigstens mittelbare Beeinträchtigung des durch Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG gewährleisteten IT-Grundrechts. Notwendig sei daher mit Blick auf den Vorbehalt des Gesetzes eine formell-gesetzliche Grundlage für die Nicht-Veröffentlichung, die zudem organisatorische und prozedurale Mindeststandards für den Erwerb und den weiteren Umgang mit Schwachstellen sowie zum Schutz vor einer Proliferation der Schwachstellen an nicht autorisierte Dritte enthalte.[38] Angegriffen wurde also die nur auf den ersten Blick „technikneutrale" Regelungskonzeption des Gesetzgebers, die sich bei genauerer Betrachtung als Delegation grundrechtlich sensibler Entscheidungen an die Exekutive erweist. Denn ebenso wie die sonstigen, weitgehend analog strukturierten Ermächtigungen zur Quellen-TKÜ im Bundes- und im Landesrecht beschränkt die Norm die Exekutive in keiner Weise darin, sich in großem Umfang hochpotente Sicherheitslücken zu verschaffen und diese zu „bevorraten"; auch für die Sicherung vor Verlust und die Weitergabe werden weder hier noch an anderer Stelle spezifische Vorkehrungen getroffen.

Das Bundesverfassungsgericht hat sich in seiner Entscheidung die Argumentation der Beschwerdeführer im Ausgangspunkt durchaus zu eigen gemacht. So verlangt das Gericht, gestützt auf die das IT-Grundrecht und die daraus resultierende Pflicht des Staates zum Schutz der IT-Sicherheit eine „Regelung zur grundrechtskonformen Auflösung des Zielkonflikts zwischen dem Schutz informationstechnischer Systeme vor Angriffen Dritter mittels unbekannter Sicherheitslücken einerseits und der Offenhaltung solcher Lücken zur Ermöglichung einer der Gefahrenabwehr dienenden Quellen-Tele-

[37] BVerfG, NVwZ 2021, 1361. Zu dieser Entscheidung siehe bereits oben § 5 I. 3. Weitgehend analog nun auch zu §§ 15b, 15c HSOG: BVerfG (K), 1 BvR 1552/19 v. 20.1.2022.

[38] BVerfG, 1 BvR 2771/18 v. 8.6.2021, Rn. 10 (insoweit nicht abgedruckt in NVwZ 2021, 1361).

kommunikationsüberwachung andererseits."[39] Dabei übersieht das Gericht jedoch, dass die Entscheidung über die Nichtveröffentlichung und Bevorratung von Schwachstellen nicht nur unter Schutzpflichtgesichtspunkten grundrechtsrelevant werden kann. Zwar erleichtert das Unterlassen einer Veröffentlichung in erster Linie privaten Dritten Angriffe auf die IT-Sicherheit. Insofern ist durch das Kollisionsrisiko primär die Schutzdimension betroffen. Erhält der Staat allerdings durch Dritte Kenntnis von der Schwachstelle, muss er damit rechnen, dass jedenfalls diese Akteure die Schwachstelle ausnutzen; hier kommt die Entscheidung zur Nichtveröffentlichung einer aktiven Billigung des Risikos gleich, das mit der Qualifikation als Unterlassen einer eigenen Eingriffshandlung nicht mehr adäquat beschrieben erscheint. Jedenfalls aber mit der Bevorratung schafft der Staat selbst aktiv ein Proliferationsrisiko und erhöht damit durch eigenes Tätigwerden die Gefährdungslage für die IT-Sicherheit, was auch aus abwehrrechtlicher Sicht die Frage nach der Grundrechtsverantwortlichkeit aufwirft. Auf die Konsequenzen wird noch näher einzugehen sein.[40]

Darüber hinaus lehnt es der Senat dann jedoch aus prozessualen Gründen ab zu prüfen, ob der Gesetzgeber seine grundrechtliche Schutzpflicht tatsächlich verletzt habe, da die Beschwerdeführer den Anforderungen an die Darlegungslast nicht genügt hätten.[41] Insbesondere hätten einschlägige Schutzvorgaben des Gesetzgebers diskutiert werden müssen, konkret die Vorschrift des § 54 Abs. 3 PolG BW, die Vorgaben zur Datenschutz-Folgenabschätzung (§ 80 PolG BW i. V. m. Art. 27 DSRL-JI), das baden-württembergische Gesetz zur Verbesserung der Cybersicherheit vom 17.2.2021 (CSG BW)[42] sowie der untergesetzliche „Meldestandard" des IT-Planungsrats vom 5.10.2017[43].

Für eine restriktive Handhabung der Zulässigkeitsanforderungen bei Gesetzesverfassungsbeschwerden sprechen gute verfassungsrechtliche Gründe.[44] Im konkreten Fall erweisen sich die vom Gericht genannten Normen jedoch als Nebelkerzen. Denn auch wenn man § 54 Abs. 3 S. 2 PolG BW – trotz der vom Gericht selbst artikulierten Zweifel an der Reichweite der Norm – als

[39] BVerfG, NVwZ 2021, 1361, LS 2b. Zurückhaltender nun BVerfG (K), 1 BvR 1552/19 v. 20.1.2022, Rn. 17: „Zwar kann […] sich hieraus eine konkrete Schutzpflicht des Gesetzgebers ergeben, den Umgang mit Sicherheitslücken zu regeln".

[40] Siehe § 7 II. 3. b).

[41] BVerfG, NVwZ 2021, 1361, Rn. 48 ff. Entsprechend BVerfG (K), 1 BvR 1552/19 v. 20.1.2022, Rn. 16 ff.

[42] Gesetz zur Verbesserung der Cybersicherheit und Änderung anderer Vorschriften, GBl 2021, S. 182.

[43] *IT-Planungsrat*, Standard zum Verbindlichen Meldeverfahren zum Informationsaustausch über IT-Sicherheitsvorfälle im VerwaltungsCERT-Verbund (Meldestandard), Beschluss 2017/35 v. 5.10.2017.

[44] *J. Buchheim*, Die Grenzen des „entgrenzten Gerichts", VerfBlog, 27.7.2021, unter Verweis auf *C. Möllers*, Funktionen des Verfassungsprozessrechts, in: Münch/Thiele (Hrsg.), GS Heun, 2019, S. 149 ff.

Vorgabe an die Behörde versteht, die Sicherheitslücke selbst (und nicht nur die Infiltrationssoftware) vor „unbefugter Nutzung" zu schützen,[45] wäre damit allenfalls das Proliferationsproblem, nicht aber die fortbestehenden Kollisionsrisiken für die Nutzer infolge des Offenhaltens der Lücke adressiert. Entsprechendes gilt für die Datenschutz-Folgenabschätzung. Schon die Ausführungen des Senats dazu, weshalb bereits das Verschaffen und Offenhalten einer Sicherheitslücke eine datenschutzrechtlich relevante „Verarbeitung" personenbezogener Daten darstelle, erscheinen – wie vom Gericht selbst eingeräumt – spekulativ, würde dies doch eine erhebliche Vorverlagerung des ohnehin schon weiten Begriffs der Verarbeitung nach Art. 3 Nr. 2 DSRL-JI erfordern.[46] Zudem ist die Datenschutz-Folgenabschätzung konzeptionell auf die Rechte aus Art. 7 und Art. 8 GRCh fokussiert.[47] Wie gezeigt lässt sich das Informationssicherheitsproblem jedoch nicht allein und auch nicht primär auf das Datenschutz- bzw. Persönlichkeitsrecht zurückführen. Die Schutzpflichtfrage stellt sich vielmehr auch dort, wo Sicherheitslücken nicht für die Infiltration persönlichkeitsrelevanter IT-Systeme, sondern etwa gegen KRITIS-Einrichtungen genutzt werden können. Dementsprechend kann selbst dann, wenn die Datenschutz-Folgenabschätzung greifen würde, diese ein gesetzliches Schwachstellenmanagement nicht vollständig ersetzen. Auch die Vorschriften des baden-württembergischen CSG, das für die Landesverwaltung Vorgaben zur Informationssicherheit macht, die im Wesentlichen den Vorgaben des BSIG für den Bund entsprechen, können nicht als hinreichende Antwort auf das Informationssicherheitsproblem gelten. So gestattet die maßgebliche Norm, die der zuständigen Landesbehörde die Warnung vor Sicherheitslücken erlaubt, auch deren Nichtoffenlegung, soweit die Lücken „staatlichen Geheimhaltungserfordernissen unterliegen", ohne letztere näher zu definieren oder den darauf bezogenen Verwaltungsprozess zu erläutern.[48] Diese Einschränkung ist zwar in der ansonsten wortgleichen Vorschrift des § 7 Abs. 2

[45] § 54 Abs. 3 PolG BW in der angegriffenen Fassung lautet: „Bei Maßnahmen nach Absatz 2 ist sicherzustellen, dass
1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und
2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist gegen unbefugte Nutzung zu schützen."

[46] BVerfG, NVwZ 2021, 1361, Rn. 58.

[47] Allerdings sind gem. Art. 27 Abs. 2 i.Vm. ErwGr 51 DSRL-JI analog zu Art. 35 Abs. 1 i. V. m. ErwGr 75 DSGVO bei den Folgen der Verarbeitung physische, materielle und immaterielle Beeinträchtigungen mit in Betracht zu ziehen. Dies setzt allerdings immer noch voraus, dass jedenfalls auch eine Verarbeitung personenbezogener Daten durch die Schadsoftware erfolgt. Das ist zwar bei der Quellen-TKÜ der Fall, erfasst allerdings (siehe oben) nicht alle potenziellen Konstellationen des Schwachstelleneinsatzes.

[48] Vgl. zu § 8 Abs. 2 CSG die kritische Stellungnahme von *Chaos Computer Club*, Stellungnahme v. 3.11.2020.

BSIG nicht enthalten. Letzteres wird relevant, weil das BSI gemäß den Anforderungen des vom Gericht erwähnten Meldestandards des IT-Planungsrats von den Landesbehörden über allgemein bedeutsame Sicherheitslücken informiert werden muss und dann seinerseits gem. § 7 Abs. 1 BSIG die Öffentlichkeit oder betroffene Kreise warnen muss. Doch ist eine derartige Warnung ein Aliud zur eigentlich notwendigen Schwachstellen-Governance, wird der Konflikt zwischen IT-Sicherheit und den behördlichen Interessen an einer Offenhaltung der Lücke hier letztlich einseitig zugunsten ersterer aufgelöst. Das mag für viele Fälle die richtige Lösung sein. Die eigentliche Frage, die eine gesetzliche Regelung der Schwachstellen-Governance beantworten soll, ist damit jedoch nicht geklärt.

Festhalten lässt sich, dass es aus prozessrechtlichen Gründen notwendig gewesen sein mag, den Beschwerdeführern diesen Vortrag abzuverlangen. Belastbare Lösungen für das vom Gericht präzise rekonstruierte Problem finden sich jedoch weder in den genannten Normen noch an anderer Stelle. Im Ergebnis muss daher konstatiert werden, dass es bisher an einer Regelung zur grundrechtskonformen Auflösung des Zielkonflikts, den der Umgang mit Sicherheitslücken bzw. Schwachstellen aufwirft, fehlt.

3. Grundzüge einer staatlichen Schwachstellen-Governance

Um ein hohes Schutzniveau für die IT-Sicherheit und die mit der Nutzung von Schwachstellen verfolgten Ziele in Ausgleich zu bringen, genügt es nach dem gerade Gesagten nicht, staatlichen Stellen den Umgang mit Schwachstellen für einzelne Zwecke zu erlauben. Vielmehr gilt es, technische, organisatorische und prozedurale Fragen zu klären und Kriterien dafür zu definieren, welche Art von Sicherheitslücken unter welchen Bedingungen wann und wem gegenüber offengelegt werden dürfen bzw. müssen.[49] Auch die Frage, wie staatliche Stellen Schwachstellen erwerben sollen, muss geregelt werden.[50] Idealerweise erfolgt zudem eine Anbindung der Vorgaben an das allgemeine Informationssicherheitsrecht.[51] Orientierungspunkte für ein solches Regelwerk gibt das U.S.-Recht, das aus diesem Grund hier vorab dargestellt werden soll.

[49] Instruktiv zu den verschiedenen Zeitpunkten, an denen eine Veröffentlichung erfolgen kann, und den damit verbundenen „Philosophien" einer Veröffentlichung *N. Weaver*, The GCHQ's Vulnerabilities Equities Process, Lawfare v. 3.6.2019.

[50] Zu dieser hier ausgeklammerten Frage (vgl. oben § 7 Fn. 9) siehe vertiefend *Schulze*, Governance von 0-Day-Schwachstellen in der deutschen Cyber-Sicherheitspolitik, SWP-Studie, Mai 2019.

[51] Dies wird insbesondere durch die jetzt durch die NIS 2-RL anstehende Einbindung staatlicher Stellen in das KRITIS-Regime relevant; hiernach greifen für staatliche Stellen grundsätzlich dieselben Informationspflichten wie für private Betreiber. Art. 2 Abs. 6 bis 8 NIS 2-RL sieht hier allerdings eine recht weit gefasste Bereichsausnahme für die Sicherheitsbehörden vor.

a) Orientierungspunkte: Der Vulnerabilities Equities Process

Ein international viel diskutiertes Vorbild für ein Regime zum Umgang *staatlicher* Stellen mit Schwachstellen[52] stellt der in den USA seit rund 15 Jahren etablierte „Vulnerabilities Equities Process" (VEP) dar. Dieses Programm wurde zuletzt 2017 in Reaktion auf die Entwendung wertvoller Zero-day-Schwachstellen bei der NSA[53] überarbeitet und als „Vulnerabilities Equities Policy and Process" (VEP 2017) teilweise veröffentlicht.[54] Verschiedene Länder haben seither ähnliche Regularien verabschiedet.[55] Für Deutschland enthält der Koalitionsvertrag 2021 eine entsprechende Absichtserklärung.[56] Auch die Europäische Union befasst sich mit dieser Thematik.[57] Normhierarchisch handelt es sich beim VEP 2017 um Innenrecht[58]; einer gesetzlichen Festschreibung der dortigen Kernaussagen, wie sie für Deutschland aus Schutzpflichtgesichtspunkten jedenfalls teilweise geboten sein dürfte, stehen jedoch keine prinzipiellen Gründe entgegen.

Zentrales Anliegen des VEP 2017 ist die klare Etablierung eines Regel-Ausnahme-Verhältnisses und die Beschränkung auf bestimmte Sachbereiche: Nur dort, wo ein „demonstrable, overriding interest in the use of the vulnerability for lawful intelligence, law enforcement, or national security purposes" vor-

[52] Für den Umgang Privater mit Schwachstellen finden sich ähnliche Grundregeln in ISO/IEC 30111:2013 Information technology – Security techniques – Vulnerability handling processes. Hier greifen aber vor allem die oben dargestellten Informations- und Meldepflichten, vgl. § 6 II. 3. e).

[53] Siehe § 7 Fn. 16.

[54] Vgl. die veröffentlichte Fassung *White House*, Vulnerabilities Equities Policy and Process for the United States Government v. 15.11.2017. Zur Erläuterung siehe *R. Joyce*, Improving and Making the Vulnerability Equities Process Transparent is the Right Thing to Do, 15.11.2017. Die Vorgängerfassung – *White House*, Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process v. 16.2.2010 – ist durch ein Informationsfreiheitsbegehren der Electronic Frontier Foundation 2016 publik geworden, vgl. die Darstellung unter https://archive.epic.org/privacy/cybersecurity/vep/. Instruktiv auch die Einblicke bei *M. Daniel*, Heartbleed: understanding when we disclose cyber vulnerabilities, 28.4.2014.

[55] Siehe für Großbritannien: *GCHQ*, The Equities Process, 2018. Für Australien: *Australian Signals Directorate*, Responsible Release Principles for Cyber Security Vulnerabilities, 2022. Für die Union siehe *ENISA*, Coordinated Vulnerability Disclosure Policies in the EU, April 2022.

[56] *SPD/Bündnis 90/Die Grünen/FDP*, Mehr Fortschritt wagen, 2021, S. 16: „Wir führen […] ein wirksames Schwachstellenmanagement, mit dem Ziel Sicherheitslücken zu schließen, […] ein".

[57] *European Parliament, Directorate-General for Internal Policies*, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, Study for the LIBE Committee, 2017.

[58] Als Grundlage des 2017 veröffentlichten VEP werden die National Security Policy Directive-54 (zugleich veröffentlicht als Homeland Security Policy Directive-23) angegeben. Zur Rechtsnatur der (nur teilweise öffentlichen) Presidential Policy Directives siehe die Nachweise bei *T. Wischmeyer*, Überwachung ohne Grenzen, 2017, S. 110.

liegt, dürfen Schwachstellen geheim gehalten werden; Ziel sei hingegen „to prioritize the public's interest in cybersecurity and to protect core Internet infrastructure, information systems, critical infrastructure systems, and the U. S. economy through the disclosure of vulnerabilities discovered by the [United States Government]".[59]

Im Kern installiert der VEP 2017 dann ein komplexes inneradministratives Kommunikations- und Entscheidungssystem, das die Ziele der verschiedenen Sicherheitsbehörden ausbalancieren soll.[60] Angesiedelt ist der Prozess daher nicht bei einer einzelnen Behörde, sondern in dem unter Vorsitz des Präsidenten tagenden National Security Council (NSC); allerdings stellt die National Security Agency (NSA) das Executive Secretariat, das Koordinationsaufgaben übernimmt und Expertise bereitstellt. An dem mehrstufigen Prozess sind jedoch auch Vertreter von Behörden beteiligt, die nicht zum engeren Kreis der „Intelligence Community" zählen. Die Abwägung, ob eine Veröffentlichung erfolgt oder unterbleibt, ist dementsprechend breit angelegt und berücksichtigt folgende Gesichtspunkte: „defensive, military, intelligence and operational, commercial, international relationships, and law enforcement".[61] Allerdings werden die Interessen von Militär und Nachrichtendiensten an verschiedenen Stellen im Prozess priorisiert und in Teilbereichen auch vom VEP ausgenommen.[62] Subjektiv-rechtliche Interessen derjenigen, die von der staatlichen Nutzung der Lücken betroffen sind, spielen demgegenüber allenfalls mittelbar eine Rolle.

Während die durch den VEP 2017 vorgenommene Institutionalisierung des Schwachstellenmanagements weithin begrüßt wird, bemängeln Kritiker das geringe Maß an Formalisierung, die fortbestehenden Ausnahmen, die relative Trägheit des Prozesses aus Sicht der unmittelbar betroffenen Unternehmen, den Mangel an Beteiligungsmöglichkeiten des Privatsektors und allgemein an Öffentlichkeit, die unzureichende parlamentarische Kontrolle sowie den übermäßigen Einfluss des Militärs und der Nachrichtendienste.[63] Inwieweit

[59] *White House*, Vulnerabilities Equities Policy and Process for the United States Government v. 15.11.2017, S. 1.

[60] Zum Folgenden *White House*, Vulnerabilities Equities Policy and Process for the United States Government v. 15.11.2017, S. 3 ff.

[61] *White House*, Vulnerabilities Equities Policy and Process for the United States Government v. 15.11.2017, S. 8 f. Die Kategorien werden in Annex B (a. a. O., S. 13 f.) weiter charakterisiert.

[62] *White House*, Vulnerabilities Equities Policy and Process for the United States Government v. 15.11.2017, S. 9.

[63] Siehe die konkreten Monita bei *M. Ambashta*, Taking a Hard Look at the Vulnerabilities Equities Process and its National Security Implications, Berkeley Tech. L. J. Blog v. 22.4.2019; *A. Gaudion*, It's Time to Reform the U.S. Vulnerabilities Equities Process War Room, 2.9.2021; *A. Thompson*, Assessing the Vulnerabilities Equities Process, Three Years After the VEP Charter, Lawfare v. 13.1.2021. Vgl. auch allgemein *R. Knake*, Internet Governance in an Age of Cyber Insecurity, 2010; *T. Caulfield/C. Ioannidis/D. Pym*, The U.S. Vul-

die von der aktuellen Präsidentschaft geplanten Reformen des VEP diese Punkte berücksichtigen, ist derzeit nicht absehbar. Sie müssen jedenfalls bei der Orientierung nationaler und europäischer Ansätze am U.S.-Vorbild mitbedacht werden.

b) Gestaltungselemente

Anders als in den USA liegt derzeit weder auf nationaler noch auf unionsrechtlicher Ebene ein vollzugsfähiger Vorschlag für ein dem VEP entsprechendes Regime vor. Auch in den rechtspolitischen Debatten um die Zulässigkeit staatlicher Maßnahmen, die die IT-Sicherheit kompromittieren, wird die Problematik selten erörtert.[64] Das Bundesverfassungsgericht hat die von ihm selbst konstatierte gesetzgeberische Pflicht zum „Schutz informationstechnischer Systeme vor Angriffen Dritter mittels unbekannter Sicherheitslücken“[65] – wie erwähnt – ebenfalls nicht in diese Richtung konkretisiert. Dem Verfassungsrecht lassen sich allerdings durchaus Eckpunkte entnehmen, die den staatlichen Umgang mit Schwachstellen anleiten. Das Unionsprimärrecht ist hier weniger direktiv; soweit die im Sicherheitsrecht beschränkten Kompetenzen der Union reichen,[66] dürfte sich der Unionsgesetzgeber jedoch zweckmäßigerweise für analoge Vorgaben entscheiden.

aa) Ziele und gesetzliche Grundlagen

Für die deutsche Rechtsordnung ergibt sich das im VEP 2017 festgeschriebene Regel-Ausnahme-Verhältnis mit einer klaren Priorisierung der Pflicht zur Veröffentlichung von Schwachstellen aus der staatlichen Gewährleistungsverantwortung für die IT-Sicherheit.[67] Die Entscheidung zur Nichtveröffentlichung einer Schwachstelle erhöht, wie gezeigt, das Kollisionsrisiko und gefährdet damit die IT-Sicherheit. Die anschließende Bevorratung und Nutzung bringt zudem Proliferations- und Einsatzrisiken mit sich. Nur in Ausnahmefällen darf daher eine Veröffentlichung unterbleiben. Bereichsausnahmen vom Vorrang der Veröffentlichung, wie sie der VEP 2017 für bestimmte Kontexte faktisch vorsieht, sind nicht anzuerkennen. Entsprechenden Geheimhaltungsinteressen ist vielmehr im Einzelfall Rechnung zu tragen.

---

nerabilities Equities Process: An Economic Perspective, in: Rass/An et al. (Hrsg.), Decision and Game Theory for Security, 2017, S. 131 ff.; *S. Bradford Franklin*, The Need for Countries to Establish Robust and Transparent Vulnerabilities Equities Processes, Fletcher Security Rev. 6:1 (2019), S. 45 ff.; sowie die Reformvorschläge der *Cyberspace Solarium Commission*, Report, März 2020, S. 96 ff.

[64] Die Ausnahme bildet: *Herpig*, Schwachstellen-Management für mehr Sicherheit, 27.8.2018.

[65] BVerfG, NVwZ 2021, 1361, LS 2b.

[66] Siehe oben § 5 II.

[67] Siehe oben § 5 III. 1.

Ob für die Entscheidung über die Zurückhaltung von Schwachstellen eine gesetzliche Regelung erforderlich ist oder ob eine untergesetzliche Festlegung ausreicht, hängt davon ab, inwieweit hierin eine *wesentliche* Entscheidung für die durch die Nichtoffenlegung berührten Grundrechte zu erkennen ist.[68] Das Bundesverfassungsgericht hat, wie dargestellt, eine entsprechende Pflicht zur gesetzlichen Regelung bereits aus der grundrechtlichen Schutzpflicht des Staates für das Fernmeldegeheimnis und die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme hergeleitet.[69] Entsprechendes muss für die weiteren durch eine Nichtoffenlegung potenziell betroffenen Grundrechte gelten.[70] Da sich die Gefährdungen einer Sicherheitslücke in aller Regel nicht „grundrechtsspezifisch" manifestieren, sondern alle von den betroffenen Diensten oder Systemen erfassten Aktivitäten beeinträchtigen können, ist von einer umfassenden Regelungspflicht auszugehen. Diese gilt unabhängig davon, ob die Schwachstellen anschließend für sicherheitsbehördliche Eingriffe oder für sonstige Zwecke genutzt werden sollen. Hinzu kommt, dass der Staat jedenfalls durch die Bevorratung von Schwachstellen aktiv das (Proliferations-)Risiko erhöht, sodass auch aus abwehrrechtlicher Sicht ein gesetzgeberisches Tätigwerden geboten ist.[71] Gleiches gilt nach hiesigem Verständnis für die aktive Billigung einer fortbestehenden Grundrechtsgefährdung durch Dritte, die jedenfalls dann vorliegt, wenn der Staat die Kenntnis von der Sicherheitslücke nicht durch eigene Forschung, sondern durch eben diese Dritten erlangt hat.

Soweit eine gesetzliche Regelungspflicht besteht, ist dieser nicht bereits dadurch genügt, dass in Ermächtigungsgrundlagen, etwa für die Quellen-TKÜ, die Bevorratung oder sonstige Nutzung von Schwachstellen durch staatliche Stellen schlicht vorausgesetzt wird. Vielmehr ist mit Blick auf die durch die Nichtveröffentlichung erzeugte spezifische Gefährdungssituation der Erlass einer speziellen Rechtsgrundlage geboten. Nicht unähnlich dem vom Bundesverfassungsgericht für die Informationsweiterverwendung entwickelten „Doppeltür-Modell"[72] bedarf es also des Zusammenspiels zweier Befugnisnormen – der die Geheimhaltung der Schwachstelle legitimierenden und der ihren Einsatz rechtfertigenden –, um Eingriffe wie die Quellen-TKÜ verfassungsfest vorzunehmen.

---

[68] Siehe dazu nur BVerfGE 134, 141 (184, Rn. 126); 139, 148 (174 f., Rn. 51); 141, 143 (170, Rn. 59 ff.) m. w. N.

[69] BVerfG, NVwZ 2021, 1361, Rn. 26 f.

[70] Nochmals: Dies betrifft nicht nur das sogenannte IT-Grundrecht, sondern alle Grundrechte, deren Realisierung auf sichere IT angewiesen ist, vgl. oben § 5 I. 3.

[71] Siehe § 7 II. 2. b).

[72] Siehe zu diesem vor allem auch unter kompetenzrechtlichen Gesichtspunkten wichtigen Modell näher BVerfGE 125, 260 (312, Rn. 194); 130, 151 (184 f., Rn. 123 ff.); 150, 244 (278, Rn. 80); 150, 309 (335, Rn. 68); 155, 119 (167, Rn. 93 ff.; 179, Rn. 130; 209, Rn. 201).

bb) Maßstäbe für die (Nicht-)Veröffentlichung

Um den Ausnahmecharakter der Nichtveröffentlichung zu sichern und die dadurch erzeugten Risiken zu rechtfertigen, muss die gesetzliche Regelung restriktiv gefasst sein. Der Gesetzgeber sollte daher anordnen, dass die durch die Geheimhaltung verfolgten verfassungsrechtlich radizierten Interessen in der Abwägung die gleichfalls grundrechtlich radizierten Interessen an der Veröffentlichung *wesentlich* überwiegen müssen. Um eine möglichst umfassende Interessenabwägung zu gewährleisten, sollte die Abwägung darüber hinaus jedenfalls in Grundzügen gesetzlich vorstrukturiert werden und die Berücksichtigung der folgenden Faktoren verlangen[73]:

(1) Ein wesentliches Überwiegen der Interessen der Nichtveröffentlichung kommt nur dann in Betracht, wenn sich mit Hilfe der Lücke besonders wichtige Zwecke erreichen lassen; hierunter dürften die Landesverteidigung, die nachrichtendienstliche Aufklärung sowie jedenfalls die Verfolgung bestimmter schwerer Deliktstypen fallen.[74] Allerdings lassen sich Schwachstellen aus sich heraus kaum „thematisch" zuordnen. Ein und dieselbe Sicherheitslücke wird sich regelmäßig in den Systemen von qualifiziert Verdächtigen ebenso wie von gänzlich Unbeteiligten finden. Das Gewicht des Interesses an einer Nichtveröffentlichung lässt sich daher nur ganz abstrakt bestimmen. Vor diesem Hintergrund dürfte es sich als sinnvoll erweisen, die Nichtveröffentlichung daran zu knüpfen, dass jedenfalls ein klarer operativer Nutzen der Lücke für die genannten Zwecke dargelegt werden kann. Inwieweit dieses Kriterium die Geheimhaltung von Schwachstellen effektiv beschränkt, hängt davon ab, wie umfangreich und konkret begründet werden muss, dass die Lücke einen echten operativen Mehrwert gerade in Bezug auf potenzielle (geeignete) Einsatzziele verspricht. Im Lichte seiner Verantwortung für die IT-Sicherheit ist der Gesetzgeber hier zu einer restriktiven Fassung angehalten.

(2) Zweiter abwägungsrelevanter Gesichtspunkt ist die Schwere der Sicherheitslücke. Diese gibt Auskunft über das Gewicht des Informationssicherheitsinteresses. Eine Veröffentlichung muss umso eher erfolgen, je größer die Schäden sind, die bei einem Ausnutzen der Schwachstelle durch Dritte drohen. Für die Bemessung der Schwere einer Schwachstelle stehen etablierte Metriken bereit, die zwar nicht wertungsfrei sind, aber doch eine allgemeine Orientierung bieten.[75] Faktoren, die insoweit berücksichtigt werden müssen, sind

[73] Die im Folgenden entwickelten Kriterien orientieren sich am Annex B zu *White House*, Vulnerabilities Equities Policy and Process for the United States Government v. 15.11.2017, S. 9, und an *Herpig*, Schwachstellen-Management für mehr Sicherheit, 27.8.2018, S. 23 ff.

[74] Vgl. ähnlich zur Abwägung von staatlichen Eingriffsmaßnahmen in die kommunikative Privatheit: BVerfGE 129, 208 (243 f., Rn. 203 ff.); 141, 220 (270, Rn. 106 ff.); 155, 119 (190, Rn. 154).

[75] Vgl. oben § 6 II. 3. e).

der Verbreitungsgrad der fehlerbehafteten Komponente, die system- oder netzwerkinterne Kritikalität der Schwachstelle, die Art der Nutzer (Private, KRITIS-Unternehmen, staatliche Stellen etc.), die Kritikalität der konkret betroffenen Produkte oder Dienste[76] und ihre „Patchbarkeit" bzw. die Verfügbarkeit sonstiger den potenziellen Schaden verhindernder oder zumindest mitigierender Mittel. In Bezug auf letzteres ist zu berücksichtigen, dass die Effektivität von Patches nicht überschätzt werden darf.[77] Im IT-Sektor wird oft keine langjährige Produktpflege betrieben; werden Schwachstellen in älteren Produkten entdeckt, kann eine Offenlegung unter Umständen sogar kontraproduktiv sein, weil die Kenntnis der Schwachstelle verbreitet wird, aber Abhilfe nicht ersichtlich ist.

(3) Die Gewährleistung von Informationssicherheit dient, wie dargelegt, all jenen verfassungsrechtlich relevanten Interessen, deren Realisierung auf die digitale Technik angewiesen ist.[78] Einzelne Gesichtspunkte können in der Abwägung über die (Nicht-)Veröffentlichung dennoch gesondert gewichtet werden. So hält beispielsweise das VEP 2017 nochmals ausdrücklich zur Berücksichtigung der ökonomischen Folgen bei Realisierung des Kollisionsrisikos sowie der außenpolitischen Implikationen einer (Nicht-)Veröffentlichung an. Gerade letzteres ist bedeutsam, muss doch auch unter menschenrechtlichen Gesichtspunkten die Möglichkeit der (kollidierenden) Nutzung einer Sicherheitslücke durch nicht-demokratische Drittstaaten stets mitbedacht werden.[79]

(4) Viertens sind Grenzen der Abwägung zu definieren. So muss eine Veröffentlichung unabhängig vom strategischen Wert der Schwachstelle stets erfolgen, wo staatliche Stellen im Zuge der gesetzlich angeordneten Informations- und Meldepflichten – etwa auf Grundlage von Art. 33 DSGVO oder der entsprechenden Normen im BSIG – von der Existenz von Schwachstellen Kenntnis erlangt haben.[80] Müssten die Meldepflichtigen befürchten, dass staatliche Stellen ihre Meldungen sicherheitsbehördlich instrumentalisieren, könnte dies negative Effekte auf die Meldebereitschaft haben und damit die Wirksamkeit dieses für das Informationssicherheitsrecht zentralen Instrumentes kompromittieren.[81] Aus dem gleichen Grund ist daran festzuhalten, dass das BSI Erkenntnisse, die es im Zuge von Produktuntersuchungen gewonnen hat, nur für die Erfüllung seiner Aufgaben verwerten darf, vgl. § 7a Abs. 4 BSIG.

---

[76] Vgl. *Herpig*, Schwachstellen-Management für mehr Sicherheit, 27.8.2018, S. 29, mit dem Beispiel des (gegebenenfalls nur selten eingebauten) Herzschrittmachers.

[77] Siehe § 7 Fn. 18.

[78] Siehe oben § 5 II.

[79] Hierzu instruktiv am Fall „Pegasus" (§ 7 Fn. 4): *G. Mascolo*, Die gefährlichste Waffe unserer Zeit, SZ, 11.2.2022.

[80] Vgl. oben § 6 II. 3. e).

[81] Ebenso *Herpig*, Schwachstellen-Management für mehr Sicherheit, 27.8.2018, S. 18.

(5) Im Übrigen muss der Gesetzgeber den über eine Veröffentlichung entscheidenden Stellen Spielräume belassen, damit den Besonderheiten des Einzelfalls Rechnung getragen werden kann. Dies gilt etwa mit Blick auf den Zeitpunkt sowie auf Art und Umfang der Veröffentlichung. So trägt es regelmäßig zur Gewährleistung eines hohen Informationssicherheitsniveaus bei, wenn zunächst nur die für die Behebung der Schwachstelle zuständige Instanz, etwa der Produkthersteller, informiert wird, sofern auf diese Weise absehbar Abhilfe geschaffen werden kann. Erst wenn sich dieser Weg als fruchtlos erweist, bietet sich eine Veröffentlichung der Sicherheitslücke in Gestalt einer Warnung an alle Nutzer an. Anders kann dies jedoch sein, wenn Dritte die Sicherheitslücke aktuell nutzen. Hier ist unter Umständen eine sofortige und umfassende Publikation geboten, damit Betroffene rasch Selbstschutzmaßnahmen ergreifen können. Denkbar ist aber auch, dass im Einzelfall nur bestimmte, besonders sensible Stellen über die Existenz der Schwachstelle informiert werden, damit diese Schutzmaßnahmen gegen die Bedrohung durch Dritte ergreifen können, wodurch das Kollisionsrisiko gemindert wird, ohne dass der operative Wert der Schwachstelle entfällt. Auch kann es bei laufenden Angriffen sinnvoll sein, von einer Veröffentlichung der aufgedeckten Lücke vorübergehend abzusehen, um den Verursacher eines Angriffs zu identifizieren. Diese Überlegungen sind nicht abschließend und dienen nur zur Illustration des Punktes, dass eine umfassende gesetzliche Festschreibung der Abwägungskriterien kontraproduktiv wäre. Ein weiteres Instrument zur Flexibilisierung ist die Befristung von Nichtveröffentlichungsentscheidungen, wobei die Dauer der Frist mit Blick auf die operativen Interessen einerseits und die dadurch erzeugten Risiken andererseits zu bemessen ist. Auch hierfür kann der Gesetzgeber entsprechende Begründungserfordernisse vorsehen. Längere Befristungen sind gegebenenfalls mit einer Pflicht zur Zwischenevaluation zu versehen.

(6) Oben wurde bereits darauf hingewiesen, dass sich die mit der Nutzung von Zero-day-Schwachstellen und N-day-Schwachstellen verbundenen Risiken unterscheiden. Dem muss im Rahmen der Abwägung ebenfalls Rechnung getragen werden: Je weiter die Kenntnis einer Sicherheitslücke verbreitet ist, desto geringer ist ihr strategischer Nutzen und desto größer ist ihr Schadenspotenzial, jedenfalls solange die für eine Behebung der Lücke verantwortlichen Stellen keine Kenntnis davon haben. Dies spricht für eine Veröffentlichung. Allerdings hat diese Abwägung Grenzen: Sind beispielsweise ältere N-day-Schwachstellen bereits weithin bekannt, haben die Lücken aber nach wie vor einen strategischen Wert, weil Patches nicht zur Verfügung gestellt oder nicht implementiert werden, reduziert eine zusätzliche Veröffentlichung durch die Behörde das Proliferations- und das Kollisionsrisiko nicht. Die strukturellen Auswirkungen der Nicht-Veröffentlichung und auch der anschließenden Nutzung dieser Schwachstelle durch die Behörden sind daher gering. Auch insoweit ist festzuhalten, dass die gesetzlichen Vorgaben zur Ab-

wägung hinreichend flexibel gehalten sein müssen, damit den Besonderheiten des Einzelfalls Rechnung getragen werden kann.

cc) Informationssicherheit

Bereits mehrfach wurde auf das Proliferationsrisiko hingewiesen, dass mit jeder Hortung von Schwachstellen einhergeht und das, wie die Erfahrung zeigt, nicht nur theoretischer Natur ist. Jede gesetzliche Regelung eines Schwachstellenmanagements muss daher vorsehen, dass ein am jeweiligen Stand der Technik gemessen besonders hoher Informationssicherheitsstandard gewährleistet ist.[82] Dies muss durch transparente inneradministrative Kontrollmechanismen abgesichert werden.[83]

dd) Organisation und Verfahren der Schwachstellen-Governance

Nicht anders als in anderen Gebieten des Verwaltungsrechts haben die institutionelle Verortung und die prozedurale Ausgestaltung wesentlichen Einfluss auf die Anwendung und die Effektivität der materiell-rechtlichen Vorgaben zur Schwachstellen-Governance.[84] Dies zeigt auch der VEP 2017, der mit seinem Bemühen um eine Verankerung der Schwachstellen-Governance in einer die einzelnen Zweige der staatlichen Sicherheitsverwaltung mit ihren je partikularen Sicherheitslogiken überwölbenden Institution – dem NSC – zugleich Vorbild und Warnung ist, wird den Interessen von Militär und Nachrichtendiensten doch durch die dortigen Entscheidungen zur nachgeordneten Organisation und zum Ablauf des Entscheidungsprozesses faktisch wieder ein Vorrang eingeräumt.[85]

Das Grundgesetz gibt für konkrete Organisations- und Verfahrensfragen der Schwachstellen-Governance keine näheren Hinweise und erfasst darüber hinaus nur die Bundesebene. Die folgende Darstellung muss sich daher auf einige allgemeine Erwägungen beschränken.

(1) Wenig Erfolg verspricht es, der Frage nachzugehen, ob es sich bei der Entscheidung über die Nichtveröffentlichung einer Schwachstelle um Regierungs- oder Verwaltungshandeln handelt, um daraus Rückschlüsse auf die organisatorische Primärverortung des Prozesses zu ziehen. Denn eine eindeutige Trennung von Regierungs- und Verwaltungsfunktionen ist jedenfalls inner-

[82] Vgl. hierzu in einem anderen Kontext BVerfGE 125, 260 (325 ff., Rn. 221 ff.); 155, 119 (205, Rn. 188).

[83] Vgl. BVerfGE 125, 260 (327, Rn. 225).

[84] Zur Relevanz von Organisationsfragen im Informationssicherheitsrecht bereits § 5 III. 1. b). Dazu auch allgemein *C. Möllers*, Materielles Recht – Verfahrensrecht – Organisationsrecht, in: Trute/Groß et al. (Hrsg.), Allgemeines Verwaltungsrecht, 2008, S. 489 ff.

[85] Siehe § 7 Fn. 63.

halb der obersten Bundes- bzw. Landesbehörden kaum möglich.[86] Angesichts der großen und zudem ressortübergreifenden Bedeutung der Materie dürfte es sich allerdings anbieten, den Prozess hierarchisch zu strukturieren und verschiedene Instanzen der Exekutive, bis hin zu deren Spitze, zu involvieren. In der „Sicherheitsarchitektur" des Bundes und der Länder drängt sich keine Instanz auf, die diese *Gesamtsteuerung* übernehmen könnte. Die rein begrifflich naheliegende Übertragung der Aufgabe auf den als Kabinettsausschuss verfassten Bundessicherheitsrat (BSR) würde eine grundlegende Anpassung von dessen Mandat und Zusammensetzung voraussetzen. Mit seinem Fokus auf der ressortübergreifenden Koordinierung der Verteidigungs- und Außenpolitik, einschließlich der Außenwirtschaftspolitik (Rüstungskontrolle und -export), fehlt es dem BSR bisher an hinreichender Expertise in Sachen Cybersicherheit.[87] Darüber hinaus leidet die Institution in Sachen Transparenz und parlamentarischer Kontrolle unter erheblichen Defiziten, die verfassungsrechtlich gerade noch hinnehmbar sein mögen,[88] insgesamt aber eher für eine alternative institutionelle Lösungen sprechen. Denkbar wäre die Errichtung eines neuen Kabinettsausschusses, was dem Querschnittscharakter der Materie Rechnung trüge; hier stellt sich allerdings die – wohl negativ zu beantwortende – Frage, inwieweit Kabinettsausschüssen die für die Schwachstellen-Governance erforderliche eigenständige Entscheidungsmacht übertragen werden darf.[89] Alternativ bietet es sich an, die Entscheidung auf der Leitungsebene des Bundeskanzleramts anzusiedeln, das ohnehin in zahlreichen Feldern Koordinierungsaufgaben zwischen den Einzelressorts sowie zwischen Bund und Ländern übernimmt.[90]

---

[86] Dazu näher *M. Schröder*, Regierung und Verwaltung, in: Isensee/Kirchhof (Hrsg.), HStR, Bd. V, 3. Aufl. 2007, § 106, Rn. 29 ff. Vgl. auch die grundlegenden Beiträge von *H. Jarass*, Politik und Bürokratie als Element der Gewaltenteilung, 1975; *A. von Bogdandy*, Gubernative Rechtsetzung, 2000; *W. Hoffmann-Riem/A. Pilniok*, Die Eigenständigkeit der Verwaltung, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 1, 3. Aufl. 2022, § 12 Rn. 90 ff.

[87] Zur Institution allgemein *R. Glawe*, Der Bundessicherheitsrat als sicherheits- und rüstungspolitisches Koordinationselement, DVBl. 2012, S. 329 ff.; *K. Zähle*, Der Bundessicherheitsrat, Der Staat 44 (2005), S. 462 ff.; *R. Glawe*, Der Geheimrat, NVwZ 2014, S. 1632 ff.

[88] So jedenfalls BVerfGE 137, 185. Kritisch *J. von Achenbach*, Anmerkung zu BVerfG, 21.10.2014 – 2 BvE 5/11, JZ 70 (2015), S. 96 ff.; *F. Meinel*, Organisation und Kontrolle im Bereich der Regierung, DÖV 2015, S. 717 ff.

[89] Offengelassen in BVerfGE 137, 185 (238 f., Rn. 147). Allgemein zu den verfassungsrechtlichen Anforderungen an die Einrichtung von Kabinettsausschüssen und deren Handlungsmacht *E.-W. Böckenförde*, Die Organisationsgewalt im Bereich der Regierung, 2. Aufl. 1998, S. 243 ff.; *V. Busse*, Kabinettsausschüsse der Bundesregierung, DVBl. 1993, S. 413 ff.; *F. Meinel*, Selbstorganisation des parlamentarischen Regierungssystems, 2019, S. 389 ff. m. w. N. Vgl. zu dem ebenfalls als Kabinettsausschuss organisierten „Digitalkabinett" *A. Guckelberger*, Öffentliche Verwaltung im Zeitalter der Digitalisierung, 2019, S. 291 ff.

[90] Einer Übertragung der Entscheidung an ein vom Politikbetrieb gänzlich unabhängiges Gremium nach Art des neu eingerichteten „Unabhängigen Kontrollrats" (§ 40 ff. BNDG) dürfte entgegenstehen, dass die durchzuführende Prüfung eine deutlich breitere Form der

(2) Das zuständige Gremium wird die Entscheidungen über die Veröffentlichung nicht allein auf Grundlage einer technischen Dokumentation der Sicherheitslücke treffen können. Vielmehr müssen die Entscheidungen durch eine nachgeordnete Stelle (*Sekretariat*) vorbereitet werden, insbesondere auch mit Blick auf die Beurteilung des operativen Potenzials, die Schwere der Lücke und die weiteren abwägungsrelevanten Gesichtspunkte. Dies setzt ein hohes Maß an Expertise voraus. Aus den bekannten Gründen[91] bietet es sich an, diese Aufgabe nicht innerhalb der für diese Fragen gewiss qualifizierten nachrichtendienstlichen Bürokratie anzusiedeln, sondern der „Zivilverwaltung" zuzuweisen. Hierfür böte sich naturgemäß das BSI an.[92] Allerdings wird in der Literatur darauf hingewiesen, dass die an der Schnittstelle von defensiver und offensiver Cyberpolitik angesiedelte Entscheidung über die (Nicht-)Veröffentlichung schwer mit der Funktion des BSI als rein „defensiver" Behörde vereinbar wäre.[93] Gerade dann, wenn man – wie hier – das allgemeine informationssicherheitsrechtliche Meldeverfahren vom Schwachstellenmanagement strikt isolieren möchte,[94] erscheint das BSI in der Tat nicht als idealer Kandidat. Das spräche für die Ansiedelung der Sekretariatsfunktion auf „neutralem" Terrain, etwa erneut im Bundeskanzleramt.

Dem Regel-/Ausnahmecharakter des Verfahrens kann im Übrigen durch eine mehrstufige Organisation des Entscheidungsverfahrens Rechnung getragen werden.[95] Danach darf die Entscheidung *für* eine Veröffentlichung bereits durch das Sekretariat getroffen werden, während die Entscheidung *gegen* eine Veröffentlichung nur durch die höchste involvierte Instanz getroffen werden kann.[96]

(3) Wie bei jedem bedeutsamen und grundrechtsrelevanten exekutiven Entscheidungsverfahren stellt sich auch bei der Entscheidung über die Nichtveröffentlichung einer Schwachstelle die Frage nach der *Kontrolle*.[97] Bei deren Ausgestaltung ist zu bedenken, dass die sensitive Natur des Verfahrensgegen-

---

Expertise verlangt, als sie jedenfalls das gerichtsähnliche Kontrollorgan des § 42 BNDG aufweist. Soll sich die letztinstanzliche Prüfung über die *Nicht*veröffentlichung allerdings im Wesentlichen auf Rechtsfragen beschränken und können die weiteren zu berücksichtigenden Erwägungen in einer „administrativen" Vorinstanz angestellt werden (vgl. §§ 51 ff. BNDG), könnte sich auch dieser Weg anbieten.

[91] Siehe oben § 4 II. 1. b).

[92] Siehe oben § 6 II. 3. c).

[93] *Herpig*, Schwachstellen-Management für mehr Sicherheit, 27.8.2018, S. 20 f.

[94] Siehe § 7 II. 3. b) bb) (4).

[95] Vgl. *White House*, Vulnerabilities Equities Policy and Process for the United States Government v. 15.11.2017, S. 6.

[96] Siehe hierzu die detaillierten Vorschläge von *Herpig*, Schwachstellen-Management für mehr Sicherheit, 27.8.2018, S. 19 ff.

[97] Zu den verfassungsrechtlichen Grundlagen der (Verwaltungs-)Kontrolle siehe nur *W. Kahl*, Kontrolle der Verwaltung und des Verwaltungshandelns, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 2, 3. Aufl. 2022, § 45 Rn. 66 ff.

standes Geheimschutzmaßnahmen erforderlich macht, was die Kontrollmöglichkeiten einschränkt.[98] Dies ist jedoch nicht die einzige Herausforderung, die die Schwachstellen-Governance unter dem Gesichtspunkt der Kontrolle bereitet. Unterscheidet man im Lichte der etablierten Kontrollrelationen zwischen inneradministrativer, gerichtlicher, parlamentarischer und Öffentlichkeitskontrolle,[99] sind zudem folgende Punkte zu bedenken:

(a) Innerhalb der Exekutive können Geheimschutzfragen typischerweise gut bewältigt werden, sodass *inneradministrative* Kontrollverfahren in sicherheitssensiblen Bereichen oftmals ein hohes Maß an Kontrolleffektivität aufweisen. Allerdings ist das Potenzial für inneradministrative Kontrollen im Fall der Schwachstellen-Governance begrenzt, je höher die grundrechtsrelevante Entscheidung über die Nichtveröffentlichung innerhalb der exekutiven Hierarchie angesiedelt ist. Wird der Entscheidungsprozess, wie gerade angedacht, zweistufig ausgestaltet und kann nur die höhere Ebene eine Veröffentlichung untersagen, stellt dies zwar unter prozeduralen Gesichtspunkten einen Gewinn an Grundrechtseffektivität dar. Ist diese zweite Stufe jedoch auf Kabinettsebene angesiedelt, beschränkt dies zugleich die inneradministrativen Kontrollmöglichkeiten. Allenfalls die Kontrollrechte unabhängiger Stellen, wie sie im Sicherheitsrecht etwa für den Bundesdatenschutzbeauftragen bestehen, können hier noch für einen Ausgleich sorgen.[100] Kompensiert wird ein etwaiges inneradministratives Kontrolldefizit teilweise durch die enge personale Rückbindung der Kabinettsebene an das Parlament.

(b) Auch die nachträgliche *gerichtliche* Kontrolle fällt im vorliegenden Zusammenhang weitgehend aus.[101] Von der konkreten Nichtveröffentlichung einer Sicherheitslücke erhält die betroffene Öffentlichkeit naturgemäß keine Kenntnis. Der Rechtsweg kann daher nicht beschritten werden. Darüber hinaus ist eine solche Entscheidung dem individuell spürbaren Eingriff weit vor-

[98] Hier sind gleichermaßen strategische, institutionelle und treuhänderische Geheimhaltungsgründe einschlägig; dazu und zur notwendigen Engführung dieser Gründe ausführlich *T. Wischmeyer*, Formen und Funktionen des exekutiven Geheimnisschutzes, DV 51:3 (2018), S. 393 ff.

[99] Zu den Grundformen der Kontrolle differenziert *Kahl*, Kontrolle der Verwaltung und des Verwaltungshandelns, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 2, 3. Aufl. 2022, § 45 Rn. 79 ff. Zu den einzelnen Bausteinen von Kontrollrelationen *S. Kempny*, Verwaltungskontrolle, 2017, S. 16 ff.

[100] Hierzu im anderen Kontext BVerfGE 141, 220 (284 ff., Rn. 140 ff.); 155, 119 (227, Rn. 247). Zur Reform des VEC 2017 wurde vorgeschlagen, den zuständigen Inspector Generals Kontrollrechte in Form eines jährlichen Audits einzuräumen, vgl. *Gaudion*, It's Time to Reform the U.S. Vulnerabilities Equities Process War Room, 2.9.2021. Zur Stellung dieser Akteure und generell zur großen Bedeutung inneradministrativer Kontrollen im U.S.-Recht siehe *Wischmeyer*, Überwachung ohne Grenzen, 2017, S. 92.

[101] Zur zentralen Bedeutung gerichtlicher Kontrollen im System des Grundgesetzes siehe nur *J. Buchheim/C. Möllers*, Gerichtliche Verwaltungskontrolle als Steuerungsinstrument, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 2, 3. Aufl. 2022, § 46 Rn. 188 ff.

gelagert; potenzielle Kläger könnten daher selbst bei grober Kenntnis von der Schwachstelle die ihnen durch die Bevorratung konkret drohenden Nachteile kaum präzise genug bezeichnen und daher nach allgemeinen Regeln keinen Rechtsschutz erlangen.[102] Damit stellt sich die Frage nach Alternativen zur „normalen" gerichtlichen Befassung.

In einer ähnlich gelagerten Situation – der Auslands-Auslands-Fernmeldeerklärung – hat das Bundesverfassungsgericht jüngst die Einrichtung von Sondergremien verlangt, um einen weitgehenden Ausfall der justiziellen und inneradministrativen Kontrolle zu kompensieren. Konkret hat das Gericht eine „unabhängige Rechtskontrolle administrativen Charakters" sowie ein gerichtsähnliches Kontrollorgan gefordert, die den Prozess kontinuierlich begleiten und auch Einzelfallentscheidungen überprüfen sollen.[103] Der Gesetzgeber hat diesen Vorgaben mit der Errichtung des „Unabhängigen Kontrollrats", der administratives und gerichtsähnliches Kontrollorgan in sich vereint, Rechnung getragen (vgl. §§ 40 ff. BNDG). Die Institutionalisierung eines analogen Modells wäre auch für das Schwachstellenmanagement denkbar. Der damit verbundene Aufwand wäre allerdings, insbesondere wenn man sich die Besetzung des Unabhängigen Kontrollrats vor Augen führt (vgl. §§ 43 Abs. 1, 46 BNDG), sehr hoch.[104] Sofern die Entscheidung über die Nichtveröffentlichung auf Kabinettsebene getroffen würde, erscheint die Einrichtung eines derart hochrangigen Kontrollorgans jedoch nicht zweckwidrig.

Weit einfacher wäre demgegenüber der Rückgriff auf die etablierte Figur des präventiven Richtervorbehalts.[105] Dessen Ziel ist ebenfalls die „vorbeugende Kontrolle [exekutiver] Maßnahme durch eine unabhängige und neutrale Instanz".[106] Der Richtervorbehalt folgt dem „Vier-Augen-Prinzip" und soll verhindern, dass besonders intensive Eingriffsmaßnahmen allein von der „weisungsabhängigen und in der Sache selbst engagierten Exekutive" getroffen werden; er verlangt eine Bestätigung des exekutiven Handelns durch den

[102] Vgl. zur restriktiven Haltung der Fachberichtsbarkeit bei der ähnlich gelagerten Problematik bei Abhörmaßnahmen: BVerwGE 157, 8 (12 f., Rn. 16 ff.); 161, 76 (78, Rn. 14). Die Verfassungsgerichtsbarkeit hat hierauf zwar reagiert, ermöglicht jedoch ebenfalls keine Kontrolle von Einzelmaßnahmen, sondern nur die Überprüfung der gesetzlichen Grundlagen, vgl. BVerfGE 154, 152 (212 f., Rn. 79 f.).

[103] BVerfGE 154, 152 (290 ff., Rn. 272 ff.).

[104] Zur Forderung des BVerfG nach einer effektiven institutionellen Eigenständigkeit des für die Kontrolle der Ausland-Ausland-Fernmeldeaufklärung zuständigen Kontrollorgans, die insbesondere durch ein eigenes Budget, Personalhoheit sowie Verfahrensautonomie gesichert werde, ausführlich BVerfGE 154, 152 (290 ff., Rn. 272 ff.).

[105] Zu den geschriebenen und ungeschriebenen verfassungsrechtlichen Richtervorbehalten *A. Voßkuhle*, Präventive Richtervorbehalte, in: Merten/Papier (Hrsg.), HGR, Bd. V, 2013, § 131 Rn. 35 ff.

[106] BVerfGE 139, 245 (265, Rn. 57); st. Rspr.

persönlich und sachlich unabhängigen Richter.[107] Allerdings dürfte diese Figur, die ursprünglich für Einzelmaßnahmen nachgeordneter Behörden von geringer tatsächlicher und rechtlicher Komplexität wie Durchsuchungen entworfen wurde – und bereits hier regelmäßig überfordert ist[108] –, im Falle der Schwachstellen-Governance endgültig an ihre Grenzen stoßen. Wenn, wie hier vorgeschlagen, die Entscheidung über die Nichtveröffentlichung in einem stark wissensgetriebenen, inneradministrativ intensiv koordinierten und hochrangig angesiedelten Verfahren getroffen wird, stellt jedenfalls der Richtervorbehalt in seiner typischen Form (vgl. etwa §§ 100, 100e StPO) unter Kontrollgesichtspunkten keinen Mehrwert dar.

(c) Darüber hinaus kann grundsätzlich auch die *Öffentlichkeit* Kontrollfunktionen wahrnehmen.[109] Angesichts der strategischen Sensibilität der Materie und der notwendigen Geheimschutzmaßnahmen ist von einer Öffentlichkeitskontrolle im Falle der Schwachstellen-Governance jedoch wenig zu erwarten. Gestalt und Umfang der Schwachstellen-Governance können aber durch nachgelagerte (jährliche) Berichte, die statistische Informationen aggregieren, dokumentiert werden; diese tragen zur allgemeinen Transparenz des Verfahrens bei.[110]

(d) Umso dringender erscheint vor diesem Hintergrund, dass jedenfalls eine hinreichende *parlamentarische Kontrolle* gewährleistet wird, damit die Schwachstellen-Governance nicht zum „schwarzen Loch" der Staatsverwaltung wird.[111] Hierbei kommt den parlamentarischen Informationsrechten und damit der Ausbalancierung von parlamentarischen Informationsinteressen einerseits und exekutiven Geheimhaltungsinteressen andererseits eine bedeutende Rolle zu.[112] Geht man davon aus, dass das Grundgesetz keine „Regie-

[107] *Voßkuhle*, Präventive Richtervorbehalte, in: Merten/Papier (Hrsg.), HGR, Bd. V, 2013, § 131 Rn. 3 ff.

[108] Hierzu ausführlich *Voßkuhle*, Präventive Richtervorbehalte, in: Merten/Papier (Hrsg.), HGR, Bd. V, 2013, § 131 Rn. 114 ff. m. w. N.

[109] Grundlegend hierzu *H. Rossen-Stadtfeld*, Kontrollfunktion der Öffentlichkeit, in: Schmidt-Aßmann/Hoffmann-Riem (Hrsg.), Verwaltungskontrolle, 2001, S. 117; vgl. auch *A. Scherzberg*, Öffentlichkeitskontrolle, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR, Bd. 3, 2. Aufl. 2012, § 49; *Kahl*, Kontrolle der Verwaltung und des Verwaltungshandelns, in: Voßkuhle/Eifert/Möllers (Hrsg.), GVwR, Bd. 2, 3. Aufl. 2022, § 45 Rn. 172 ff.

[110] Vgl. etwa zur Relevanz nachgelagerter Berichtspflichten in einem anderen Kontext BVerfGE 141, 220 (285, Rn. 142 f.); zu den Grenzen dieses Instruments E 155, 119 (228, Rn. 251).

[111] Vgl. zu dieser Metapher *D. Pozen*, Deep Secrecy, Stan. L. Rev. 62 (2010), S. 257 (316).

[112] Diese Rechte und ihre Grenzen sind in der jüngeren Rechtsprechung des Bundesverfassungsgerichts detailliert aufgearbeitet worden: BVerfGE 110, 199; 124, 78; 124, 161; 137, 185; 139, 194; 140, 160; 143, 101; 146, 1; 147, 50. Vgl. dazu übergreifend *K. Hamdorf*, Auskunftsrechte des Deutschen Bundestages gegenüber der Bundesregierung, in: Scheffczyk/Wolter (Hrsg.), Linien der Rechtsprechung, Bd. 4, 2016, S. 467 ff. Kritische Perspektiven auf die Judikatur bei *J. von Achenbach*, Parlamentarische Informationsrechte und Gewaltentei-

rungsgeheimnisse, sondern nur abgestufte Veröffentlichungsverbote" kennt,[113] wird in aller Regel ein Ausgleich durch personelle und sachliche Beschränkungen der Reichweite der Informationsansprüche möglich sein.[114]

Für ersteres kann das Parlamentarische Kontrollgremium als Beispiel dienen, dessen Kontrolltätigkeit einfachrechtlich auf die Schwachstellen-Governance ausgedehnt werden könnte.[115] Sachliche Beschränkungen umfassen etwa eine Verkürzung der parlamentarischen Informationsrechte bis hin zu nachgelagerten Berichtspflichten, die auf statistische Auskünfte und die Beschreibung allgemeiner Herausforderungen beschränkt sind.

Zu berücksichtigen ist bei der Abwägung im Fall der Schwachstellen-Governance, dass zwar Interessen des sogenannten „Staatswohls" für die Geheimhaltung streiten können; das in der Regierungspraxis regelmäßig herangezogene Argument des „Kernbereichsschutzes" dürfte hingegen hier kaum je durchschlagen.[116] Denn die Kenntnis des Parlaments bzw. von Parlamentsteilen von einzelnen Schwachstellen führt unter keinen Umständen zu einem „Mitregieren" des Parlaments und schränkt den regierungsinternen Willensbildungsprozesses auch sonst nicht ein.[117] Herausfordernd ist demgegenüber der Umgang mit Informationen, die die Exekutive von Dritten – ausländischen Staaten oder Privaten – unter dem Siegel der Verschwiegenheit erhalten haben. Diese Konstellation weist Parallelen zu der aus dem Recht der Nach-

---

lung in der neueren Rechtsprechung des Bundesverfassungsgerichts, ZParl 48 (2017), S. 491 ff.; *Wischmeyer*, Formen und Funktionen des exekutiven Geheimnisschutzes, DV 51:3 (2018), S. 393 (410 ff.).

[113] So der Parteivortrag in BVerfGE 124, 161 (175).

[114] Vorschläge hierzu bei *Wischmeyer*, Formen und Funktionen des exekutiven Geheimnisschutzes, DV 51:3 (2018), S. 393 (403 ff.).

[115] Zu diesem Gremium und zu den Besonderheiten der nachrichtendienstlichen Kontrolle allgemein siehe *C. Gusy*, Kontrolle der Nachrichtendienste, VerwArch 106 (2015), S. 437 ff.; *C. Waldhoff*, Die reformierte Kontrolle der Nachrichtendienste, in: Dietrich/Gärditz et al. (Hrsg.), Nachrichtendienste in vernetzter Sicherheitsarchitektur, 2020, S. 73 ff.; *F. Bantlin*, Die G 10-Kommission, 2021, S. 107 ff. Aus politikwissenschaftlicher Sicht *A. Friedel*, Blackbox Parlamentarisches Kontrollgremium des Bundestages, 2019.

[116] Zu dieser Rechtsfigur grundlegend BVerfGE 67, 100 (139); siehe auch E 147, 50 (138 f., Rn. 229). Zur Kritik an dieser Figur *P. Cancik*, Der „Kernbereich exekutiver Eigenverantwortung" – zur Relativität eines suggestiven Topos, ZParl 45 (2014), S. 885 ff.

[117] Vgl. dazu und zu den mit dem Kernbereichskonzept verbundenen Fehlvorstellungen nur *J. Masing*, Parlamentarische Untersuchungen privater Sachverhalte, 1998, S. 320 ff.; *O. Lepsius*, Parlamentsrechte und Parlamentsverständnisse in der neueren Rechtsprechung des Bundesverfassungsgerichts, RuP 2016, S. 137 ff. Entgegen der missverständlichen Formulierung des BVerfG (vgl. etwa BVerfGE 67, 100 [139]; 147, 50 [138 f., Rn. 229] m. w. N.) sind weder „Erörterungen im Kabinett" noch „die Vorbereitung von Kabinetts- und Ressortentscheidungen" pauschal dem Kernbereich zuzuordnen; vielmehr ist stets zu prüfen, ob und inwieweit ein Informationsrecht tatsächlich die regierungsinterne Willensbildung beeinträchtigt. Vgl. hierzu insbes. BVerfGE 110, 199 (223). Siehe auch erneut *Masing*, Parlamentarische Untersuchungen privater Sachverhalte, 1998, S. 322; *Wischmeyer*, Formen und Funktionen des exekutiven Geheimnisschutzes, DV 51:3 (2018), S. 393 (419 ff.).

richtendienste bekannten „third party rule“ auf. Hier wie dort gilt jedoch, dass die verfassungsrechtlich gebotenen Kontrollrelationen nicht durch Abreden der Exekutive behindert oder gar unterlaufen werden dürfen.[118] Entsprechende Vereinbarungen können sich daher immer nur dann durchsetzen, solange und soweit sie mit den verfassungsrechtlichen Grenzen der Informations- und Kontrollrechte übereinstimmen.[119]

(4) Angesichts der Tatsache, dass Schwachstellen global genutzt werden können, sind im Rahmen der gesetzlichen Regelung des Schwachstellenmanagements auch Modalitäten der Weitergabe an Dritte zu adressieren. Auf die menschenrechtliche Dimension der Thematik wurde bereits hingewiesen.[120] Langfristig wird zudem auf der Ebene des Völkerrechts über eine Ausweitung des tradierten Systems der Rüstungskontrolle auf „Cyberwaffen“ nachzudenken sein; wann und unter welchen Bedingungen sich dies erreichen lässt, soll hier dahinstehen.[121]

c) Ausblick

Der Gesetzgeber kommt mit einer Regelung der Schwachstellen-Governance, die die gerade genannten Aspekte berücksichtigt, in erster Linie seinen verfassungsrechtlichen Pflichten nach. Der rationalisierende Einfluss, den eine solche Regelung auf die Exekutive hätte, muss allerdings nicht notwendig zu einer Einschränkung staatlicher Aktivitäten in diesem Bereich führen. Ein belastbares normatives Gerüst kann die Suche nach und das Management von Schwachstellen jedoch auch stimulieren. Nebenfolge einer Verrechtlichung wäre dann, dass die Exekutive nicht weniger, sondern mehr auf die Nutzung von Sicherheitslücken zurückgreift. Umso wichtiger ist es, an dieser Stelle daran zu erinnern, dass der Staat die Suche nach Sicherheitslücken in erster Linie zur Hebung des IT-Sicherheitsniveaus betreiben sollte. Der primäre Bezug des Staates zu entsprechenden Aktivitäten bleibt daher die Forschungsförderung.[122]

---

[118] So zur „third party rule“ BVerfGE 154, 152 (296 ff., Rn. 292 ff.). Vgl. auch allgemein BVerfGE 143, 101 (LS 2).

[119] Für ein generelles Verbot von Geheimhaltungsvereinbarungen (Non-Disclosure Agreements) beim Erwerb von Schwachstellen plädiert mit guten Gründen *Herpig*, Schwachstellen-Management für mehr Sicherheit, 27.8.2018, S. 18 f.

[120] Siehe § 7 Fn. 79.

[121] *M. Maybaum/J. Tölle*, Arms Control in Cyberspace, 8th International Conference on Cyber Conflict (2016), S. 159 ff.; *M. Schulze*, The State of Cyber Arms Control, S&F Sicherheit und Frieden 38:1 (2020), S. 17; *P. Roguski*, An Inspection Regime for Cyber Weapons, AJIL Unbound 115 (2021), S. 111 ff.

[122] Vgl. § 6 II. 3. b).

III. Regulierung von Verschlüsselung

Mit der Forderung nach der Nutzung von IT-Schwachstellen reagiert die Sicherheitspolitik darauf, dass die hergebrachten Überwachungsbefugnisse (vermeintlich) ins Leere laufen, wenn Kommunikation in digitalen Netzen heute ganz überwiegend verschlüsselt erfolgt („going dark").[123] Durch den Direktzugriff auf die Geräte von Sender oder Empfänger soll die Kommunikation vor der Ver- bzw. nach der Entschlüsselung abgefangen werden; die Verschlüsselung bleibt dadurch intakt, wird aber für die Betroffenen wertlos. Solche Maßnahmen sind jedoch technisch anspruchsvoll und, wie gezeigt, nur in engen Grenzen rechtlich zulässig. Als Alternative wird daher in jüngerer Zeit erneut diskutiert, ob die Kommunikations*mittler* zur Beschränkung des Einsatzes von Verschlüsselungstechnologien bzw. zum Einbau von „Hintertüren" verpflichtet werden sollten. Dies liegt auf den ersten Blick nahe, erfolgt doch auch der staatliche Zugriff in „analogen" Kontexten regelmäßig auf diesem Wege.[124] Allerdings kollidiert jeder regulatorische Vorstoß, der auf eine Schwächung des Verschlüsselungsniveaus zielt, unweigerlich mit dem Gebot der IT-Sicherheit, ist Verschlüsselung doch eine fundamentale Bedingung sicherer Informationstechnik.[125] Der Gesetzgeber ordnet daher im Kontext der IT-Sicherheit regelmäßig Verschlüsselungspflichten an.[126] Und selbst dort, wo sich kein ausdrückliches gesetzliches Gebot findet, gehört eine angemessene Verschlüsselung heute regelmäßig zum anerkannten Stand der (Informations-)Technik.[127]

Die Debatte um staatliche Eingriffe in die Integrität der Verschlüsselungstechnik ist nicht neu, sondern wurde bereits in den 1990er-Jahren geführt.[128]

---

[123] Siehe § 7 Fn. 19. Siehe auch speziell *C. Liguori*, Exploring Lawful Hacking as a Possible Answer to the "Going Dark" Debate, Mich. Telecomm. & Tech. L. Rev. 26 (2020), S. 317 ff.

[124] Dies gilt sowohl für die „klassische" TKÜ als auch dort, wo eine Verschlüsselung erst „netzseitig" durch das Telekommunikationsunternehmen erfolgt, also keine „Ende-zu-Ende-Verschlüsselung" (siehe § 7 Fn. 20) vorliegt. Dort muss der Anlagenbetreiber gemäß § 8 Abs. 3 TKÜV die Schlüssel aufheben und gegebenenfalls an die Behörden herausgeben.

[125] Vgl. die Aufbereitung verschiedener Verschlüsselungsmethoden bei *Gerhards*, (Grund-)Recht auf Verschlüsselung?, 2010, S. 29 ff.; *J. Müller-Quade/M. Huber/T. Nilges*, Daten verschlüsselt speichern und verarbeiten in der Cloud, DuD 39 (2015), S. 531 ff.; *H. Hagemeier*, Kryptografie – heute und zukünftig, DuD 43 (2019), S. 631 ff.; *Martini*, in: Paal/Pauly (Hrsg.), DS-GVO, 3. Aufl. 2021, Art. 32 Rn. 34 ff.

[126] Prominent insbes. Art. 32 Abs. 1 lit. a DSGVO; § 19 Abs. 4 S. 2 TTDSG. Siehe auch beispielhaft § 10 Abs. 2, 49 Abs. 2 S. 2 BMG (für die Kommunikation); § 87a Abs. 1 AO (für die Kommunikation); § 13 Abs. 1 S. 1 TPG (für Datenbanken). Bemerkenswert ist, dass das De-Mail-Gesetz in § 5 Abs. 3 auf eine Ende-zu-Ende-Verschlüsselung verzichtet und sich auf eine Transportverschlüsselung beschränkt hat.

[127] Siehe oben § 6 II. 5. b).

[128] Die damalige Debatte, die seinerzeit als „Krypto-Kontroverse" bzw. als crypto war firmierte, historisch kontextualisierend *W. Diffie/S. Landau*, Privacy on the Line (1998), 2. Aufl. 2007. Aus deutscher Sicht siehe *J. Bizer*, Die Kryptokontroverse, in: Hammer (Hrsg.), Sicherungsinfrastrukturen, 1995, S. 179 ff.

Seinerzeit wurde intensiv über die Verpflichtung von Telekommunikationsanbietern, Nachrichten nur mittels eines von den Behörden mitlesbaren „Clipper-Chips" zu verschlüsseln,[129] sowie über mögliche Exportbeschränkungen für Verschlüsselungstechnologien[130] gestritten. Seither haben sich die Ausgangsbedingungen allerdings geändert. So standen zur Zeit der ersten sogenannten „Krypto-Kontroverse" kaum nutzerfreundliche Lösungen für die Verschlüsselung von digitaler Kommunikation zur Verfügung.[131] Unter anderem in Reaktion auf die Snowden-Enthüllungen haben jedoch ab Mitte der 2010er-Jahre verschiedene Anbieter von Mobilfunk- und Internetdiensten Verschlüsselungstechniken nativ in ihre Angebote integriert, sodass mittlerweile auch technisch nicht versierte Nutzer von sogenannter Ende-zu-Ende-Verschlüsselung Gebrauch machen können; das heißt, dass ein Mitlesen der Nachrichteninhalte durch die Provider ebenso wie durch sonstige Stellen während des Übermittlungsvorgangs praktisch ausgeschlossen ist.[132] Selbst bei der Bekämpfung von Alltagskriminalität und -gefahren ist diese Form der Verschlüsselung heute zu einer Herausforderung für die Behörden geworden.[133]

Vor diesem Hintergrund wird nun teilweise eine Neubewertung der staatlichen Kryptopolitik gefordert (1.). Speziell für die Online-Kommunikation existieren auch bereits konkrete Vorschläge zur Regulierung, d. h. Beschränkung, der Verschlüsselung (2.). Aus rechtlicher Sicht gilt hier allerdings noch mehr als für die staatliche Nutzung von Schwachstellen: Die Spielräume für staatliche Eingriffe sind sehr eng limitiert (3.).

1. Ambivalenzen der Kryptopolitik: „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung"

In Reaktion auf die „Krypto-Kontroverse", in der sich letztlich in allen westlichen Demokratien die Befürworter starker Verschlüsselung gegen die sicherheitsbehördlichen Interessen durchgesetzt haben, hat die Bundesregierung am 2. Juni 1999 in Gestalt des Kabinettbeschlusses „Eckpunkte der deutschen

[129] Dazu grundlegend aus technischer Sicht *H. Abelson/R. Anderson et al.*, The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption, 27.5.1997.

[130] *W. Diffie/S. Landau*, The Export of Cryptography in the 20th Century and the 21st, in: De Leeuw/Bergstra (Hrsg.), The History of Information Security, 2007, S. 725 ff.

[131] Vgl. *Berkman Center for Internet & Society*, Don't Panic. Making Progress on the "Going Dark" Debate, 1.2.2016, S. 4, mit Verweis auf *A. Whitten/J. Tygar*, Why Johnny Can't Encrypt, in: Cranor/Garfinkel (Hrsg.), Security and Usability, 2005, S. 669 ff.

[132] Ausführlich *Berkman Center for Internet & Society*, Don't Panic. Making Progress on the "Going Dark" Debate, 1.2.2016.

[133] Zur Lagebewertung vgl. die bei *J.-H. Dietrich*, Der Einsatz von Verschlüsselungstechniken zwischen Grundrechtsschutz und staatlicher Sicherheitsgewährleistung, GSZ 2021, S. 1 (4), angeführten Einschätzungen.

Kryptopolitik" formuliert, die bis heute Gültigkeit haben.[134] Der Beschluss dokumentiert den Verzicht auf eine staatliche Reglementierung von Verschlüsselungstechnologien und formuliert ein ausdrückliches Förderungsgebot. Die Interessen der Sicherheitsbehörden werden zwar nominell anerkannt: „Durch die Verbreitung starker Verschlüsselungsverfahren dürfen die gesetzlichen Befugnisse der Strafverfolgungs- und Sicherheitsbehörden nicht ausgehöhlt werden." Diese Aussage wird jedoch nur durch eine Beobachtungs- und Berichtspflicht sowie ein Bekenntnis zur Verbesserung der technischen Kompetenzen der Sicherheitsbehörden hinterlegt. Diese oft auf die Maxime „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung" gebrachte Politik ist seither bei verschiedenen Gelegenheiten bestätigt worden[135] und hat mittlerweile auch Eingang in den Formelschatz der Europäischen Union gefunden[136].

Der Konsens, im Interesse der IT-Sicherheit auf ein hohes Maß an Verschlüsselung zu setzen, ist allerdings brüchiger geworden, seit Online-Plattformen und Messenger-Dienste zunehmend zur Planung von Straftaten und für den Austausch illegaler Inhalte genutzt werden. In Reaktion auf Terroranschläge in Deutschland und Frankreich sowie auf die massenhafte Verbreitung kinderpornographischer Darstellungen über das Internet haben beide Länder daher seit Mitte der 2010er-Jahre auf europäischer Ebene Regulierungsvorhaben vorangetrieben, die die Kommunikationsunternehmen zur Schwächung ihres Versprechens auf lückenlose Ende-zu-Ende-Kommunikation zwingen sollen.[137] Dies ist nicht ohne Widerspruch geblieben. Gegner dieses Politikwechsels haben sich unter anderem hinter dem Ruf nach einem „Recht auf Verschlüsselung" versammelt.[138]

---

[134] Der Kabinettsbeschluss ist dokumentiert im Anhang von *Bundesregierung*, Bericht zu den Auswirkungen der Nutzung kryptografischer Verfahren auf die Arbeit der Strafverfolgungs- und Sicherheitsbehörden (Ziffer 4 der Eckpunkte der deutschen Kryptopolitik vom 2.6.1999) – Verschlüsselungsbericht", 2002. Vgl. hierzu und zum Folgenden die Überblicksdarstellungen zur deutschen Kryptopolitik bei *S. Herpig/S. Heumann*, The Encryption Debate in Germany, 2019; *S. Herpig/J. Schuetze*, The Encryption Debate in Germany: Update, 2021. Für eine vergleichende Perspektive siehe die auf der Website der „Encryption Working Group" des Carnegie Endowment for International Peace an der Princeton University dokumentierten Berichte, abrufbar unter: https://carnegieendowment.org/programs/technology/cyber/encryption. Instruktiv auch der Überblick bei *D. Severson*, The Encryption Debate in Europe, 21.3.2017.

[135] Vgl. etwa *BMI/BSI*, Charta zur Stärkung der vertrauenswürdigen Kommunikation, 18.11.2015.

[136] *Rat der Europäischen Union*, Entschließung: Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung, 13084/1/20, 24.11.2020 – dort allerdings mit anderer Tendenz gebraucht, vgl. sogleich unter § 7 III. 2.

[137] Zu diesen Initiativen im Überblick: *S. Baker*, How Long Will Unbreakable Commercial Encryption Last?, 20.9.2019.

[138] Vgl. die Stellungnahmen in der Anhörung des Bundestagsausschusses für Inneres und Heimat v. 27.1.2020 und den entsprechenden Antrag der FDP-Fraktion „Recht auf Ver-

Aktuell ist ungewiss, in welche Richtung sich der Gesetzgeber hier bewegt. Bevor zwei konkrete Regulierungsvorhaben näher analysiert und auf ihre rechtliche Tragfähigkeit hin geprüft werden sollen, ist allerdings darauf hinzuweisen, dass der etablierte Konsens der Kryptopolitik (bisher) nur für bestimmte Formate digitaler Individualkommunikation, nicht allgemein in Frage gestellt wird. Betroffen ist damit ein zwar für die Gesellschaft und die Bürger höchst relevanter Sektor. Doch reicht die Bedeutung starker Verschlüsselung weit darüber hinaus und ist letztlich für alle Arten des digitalen Datenaustauschs existenziell, etwa auch für „smarte" Stromnetze.[139] Insoweit gibt es aktuell keinerlei Anzeichen für staatliche Bestrebungen zur Absenkung der Verschlüsselungsstandards. Die gegenwärtige Debatte um Verschlüsselungsregulierung ist daher in der Sache eine Debatte um die Regulierung der Vertraulichkeit bestimmter Formen der Online-Kommunikation, nicht mehr und nicht weniger.

2. Ansätze staatlicher Verschlüsselungsregulierung für Online-Kommunikation

Rechtstechnisch stehen im Fokus der Debatte um eine Regulierung von Verschlüsselung aktuell jene Over-the-top-Kommunikationsdienste (OTT-Dienste), also internetbasierte Dienste zur interpersonellen Kommunikation wie WhatsApp, Signal oder iMessage,[140] die standardmäßig Ende-zu-Ende-Verschlüsselung implementiert haben. Bei diesen Diensten dient die Design-Entscheidung für Ende-zu-Ende-Verschlüsselung keineswegs nur dazu, Kommunikationsinhalte dem staatlichen Zugriff zu entziehen. Sie trägt vielmehr in erster Linie der Tatsache Rechnung, dass über das Internet vermittelte (IP-basierte) Kommunikation über zahlreiche, von ganz unterschiedlichen Instanzen beherrschten AS vermittelt wird, ohne Verschlüsselung also weitgehend ungeschützt dem Zugriff beliebiger Dritter ausgeliefert wäre; dies unterscheidet sie von der Telekommunikation über das Festnetz oder über Mobilfunknetze, die sich jedenfalls im innerstaatlichen Bereich auf verhältnismäßig überschaubaren Bahnen bewegt.[141] Auch das BSI empfiehlt daher

schlüsselung – Privatsphäre und Sicherheit im digitalen Raum stärken" v. 13.11.2018, BT-Drs. 19/5764. Siehe auch jetzt den Koalitionsvertrag: *SPD/Bündnis 90/Die Grünen/FDP*, Mehr Fortschritt wagen, 2021, S. 13.

[139] Vgl. beispielhaft *N. Kumar/V. Mishra/A. Kumar*, Smart Grid and Nuclear Power Plant Security by Integrating Cryptographic Hardware Chip, Nuclear Engineering and Technology 53:10 (2021), S. 3327 ff.

[140] Zur Legaldefinition dieser Dienste und zu ihrer (grund-)rechtlichen Bewertung siehe § 5 Fn. 48.

[141] Diesen Punkt betont *S. Landau*, Exceptional Access: The Devil is in the Details, Lawfare v. 26.12.2018.

für IP-basierte Kommunikation standardmäßig starke Ende-zu-Ende-Verschlüsselung.[142]

Dennoch wird Verschlüsselung vielfach missbraucht, um illegale Inhalte vor staatlichem Zugriff zu verbergen. Nicht in jedem Fall führt dies dazu, dass den staatlichen Behörden durch die Verschlüsselung jeder Ermittlungsansatz verbaut ist. So verhindert die Verschlüsselung von Inhaltsdaten etwa nicht, dass durch die Analyse von Verbindungsdaten Erkenntnisse gewonnen werden; auch sogenannte „Brute Force"-Angriffe bleiben möglich.[143] Dennoch können rechtsstaatlich einwandfreie behördliche Ermittlungsbemühungen an der eingesetzten Verschlüsselungstechnik scheitern.

Aus dem Kreis der Sicherheitsbehörden sind daher in den vergangenen Jahren – alternativ zur Quellen-TKÜ etc. – verschiedene Vorschläge zum Umgang mit dieser Problematik entwickelt worden. Diese reichen von einem Verbot des Einsatzes bestimmter Verschlüsselungstechnologien durch bestimmte Kommunikationsdienstleister bis hin zur Verpflichtung, die für Kommunikationsdienste verwendeten Verschlüsselungsalgorithmen im Interesse der Behörden zu manipulieren. In der erwähnten Entschließung „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung" vom 14.12.2020 hat sich der Rat der Europäischen Union auf Vorschlag der deutschen Bundesregierung einer Position angenähert, die im Jargon der Sicherheitsbehörden oft als „Lawful Access" oder „Exceptional Access" bezeichnet wird; in der Entschließung wird dies als „[t]echnische Lösungen für den Zugang zu verschlüsselten Daten" umschrieben.[144] ErwGr 98 der NIS 2-RL nimmt diesen Gedanken auf und verlangt gleichfalls, technische Lösungen, um Sicherheits- und Freiheitsinteressen in eine Balance zu bringen: „The use of end-to-end encryption should be reconciled with the Member States' powers to ensure the protection of their essential security interests and public security, and to allow for the prevention, investigation, detection and prosecution of criminal offences in accordance with Union law." Er setzt dann jedoch mit einem starken Bekenntnis zur Verschlüsselung fort: „However, this should not weaken end-to-end encryption, which is a critical technology for effective protection of data and privacy and the security of communications."[145]

---

[142] *BSI*, Verschlüsselt kommunizieren im Internet, ohne Datum.

[143] Hierzu und zu weiteren Angriffsmöglichkeiten über die Supply Chain und über Zertifikate *B. Mitchell/K. Kaul et al.*, Going Dark: Impact to Intelligence and Law Enforcement and Threat Mitigation, 2017, S. 8 ff.

[144] *Rat der Europäischen Union*, Entschließung: Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung, 13084/1/20, 24.11.2020, Ziff. 5.

[145] Der ursprüngliche Kommissionsentwurf hatte hier aus Sicht der Kritiker starker Verschlüsselung noch weit großzügiger formuliert: „Solutions for lawful access to information in end-to-end encrypted communications should maintain the effectiveness of encryption in protecting privacy and security of communications, while providing an effective response to crime."

Aus technischer Sicht kann dieser „besondere" bzw. „rechtmäßige" Behördenzugang auf unterschiedliche Art und Weise implementiert werden. Ein international viel diskutiertes Modell sieht vor, dass Kommunikationsunternehmen die Möglichkeiten schaffen müssen, bei Ende-zu-Ende-verschlüsselter Kommunikation – wie bei einer Mithöreinrichtung – Behörden als zusätzliche Empfänger in den Kommunikationsvorgang (verdeckt) einzubinden.[146] Am Behörden-„Ende" wird die Kommunikation dann ganz regulär entschlüsselt. Die Integrität der Verschlüsselung bleibt somit auf dem gesamten Transportweg gewahrt. Der Sender wird „nur" darüber getäuscht, an wen seine Daten noch übermittelt werden.

Ein solcher Eingriff in die hochkomplexen Verschlüsselungsarchitekturen und -protokolle, die große Over-the-Top-Dienste implementiert haben, ist allerdings nicht minimalinvasiv möglich. IT-Sicherheitsforscher haben gezeigt, dass Exceptional Access in der geschilderten Form einen grundlegenden Umbau des von den Kommunikationsanbietern verantworteten Identitätsmanagementsystems erforderlich machen würde; die dadurch geschaffenen Zugriffsmöglichkeiten auf die über das Netzwerk ausgetauschte Individualkommunikation lassen sich dabei aus technischen Gründen nicht so gestalten, dass nur (rechtsstaatlich einwandfrei handelnde) Behörden Zugriff auf die Kommunikation erhalten *können*.[147] Vielmehr werden die Diensteanbieter zu einer Absenkung des Gesamtsicherheitsniveaus gezwungen, die auch Dritten den (illegalen) Zugriff erleichtert. Die Pflicht zur Gewährung von Exceptional Access erhöht somit für alle Nutzer das Informationssicherheitsrisiko. Mit anderen Worten: Der Staat zwänge durch die Pflicht zur Gewährung von Exceptional Access die davon erfassten Diensteanbieter dazu, das IT-Sicherheitsniveau für alle Nutzer abzusenken, gegebenenfalls auch unterhalb das bisher durch den Stand der Technik geforderte Maß.

---

[146] Zum Folgenden vgl. die Darstellung der Mitarbeiter des U.K. Government Communications Headquarters (GCHQ): *I. Levy/C. Robinson*, Principles for a More Informed Exceptional Access Debate, Lawfare v. 29.11.2018: „In a world of encrypted services, a potential solution could be to go back a few decades. It's relatively easy for a service provider to silently add a law enforcement participant to a group chat or call. The service provider usually controls the identity system and so really decides who's who and which devices are involved – they're usually involved in introducing the parties to a chat or call. You end up with everything still being end-to-end encrypted, but there's an extra 'end' on this particular communication. This sort of solution seems to be no more intrusive than the virtual crocodile clips that our democratically elected representatives and judiciary authorise today in traditional voice intercept solutions and certainly doesn't give any government power they shouldn't have. We're not talking about weakening encryption or defeating the end-to-end nature of the service. In a solution like this, we're normally talking about suppressing a notification on a target's device, and only on the device of the target and possibly those they communicate with. That's a very different proposition to discuss and you don't even have to touch the encryption."

[147] Ausführlich *H. Abelson/R. Anderson et al.*, Keys Under Doormats, 7.7.2015; knapper *Global Encryption Coalition*, Breaking Encrpytion Myths, 2020.

Anders als früher der „Clipper Chip" lässt Exceptional Access also die Verschlüsselungsalgorithmen selbst intakt, nutzt jedoch die Tatsache aus, dass Verschlüsselung nie im luftleeren Raum erfolgt, sondern stets eine Infrastruktur als Vertrauensbasis voraussetzt. Nur diese wird manipuliert; im Ergebnis läuft auch dies jedoch für *alle* Nutzer des Dienstes auf einen Verlust an Informationssicherheit hinaus.

In eine ähnliche Richtung geht aus kryptographischer Sicht das speziell für den Kampf gegen Kindesmissbrauch entwickelte Konzept des „Client Side Scanning". Damit wird die aktuell von der Europäischen Kommission erwogene Verpflichtung von noch näher zu bestimmenden Anbietern von Online-Diensten bezeichnet, die über ihre Netzwerke übermittelten Daten ungeachtet von deren Verschlüsselungsstatus auf einschlägige Inhalte zu überprüfen.[148] Damit auch hier die Integrität der Ende-zu-Ende-Verschlüsselung gewahrt bleibt – diese verhindert ja auch, dass die Provider die Nachrichten ihrer Nutzer auswerten können – soll eine automatisierte Analyse („Scanning") der versendeten Informationen bereits auf dem Gerät des Nutzers („Client Side"), also vor deren Verschlüsselung, erfolgen.[149] Die Umsetzung einer solchen Verpflichtung ist technisch hochkomplex. Unabhängig davon, welcher Weg hier konkret gewählt wird, ist eindeutig, dass jede Form der Umsetzung dieser Maßnahme zwingend das Schutzniveau des Gesamtsystems reduziert, da nie sicher ausgeschlossen werden kann, dass die neue Funktionalität durch nicht autorisierte Akteure missbraucht wird.[150]

---

[148] Die Kommission hat am 11.5.2022 ihren Vorschlag für eine Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern vorgelegt, COM(2022) 209 final. Dieser ist von zahlreichen Seiten kritisiert worden, vgl. nur *M. Reuter*, Europas digitale Bürgerrechtsorganisationen gegen neue Form der Massenüberwachung, Netzpolitik.org v. 17.3.2022; *S. Meineck/A. Biselli*, EU-Datenschutzbehörden nehmen Chatkontrolle komplett auseinander, Netzpolitik.org v. 29.7.2022. Parallele Bestrebungen existieren in den USA, vgl. den Entwurf des U.S. Senats für den „Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2022" (EARN IT Act); dazu *R. Pfefferkorn*, The EARN IT Act is back, and it's more dangerous than ever, 4.2.2022. Positiver hingegen die Einschätzung bei *N. Weaver*, Encryption and Combating Child Exploitation Imagery, Lawfare v. 23.10.2019.

[149] Die angedachte Verpflichtung zum Client Side Scanning muss unterschieden werden von der Befugnis bestimmter OTT-Anbieter, die keine Ende-zu-Ende-Verschlüsselung nutzen (etwa: Facebook), die Kommunikation über ihr Netzwerk freiwillig auf illegale Inhalte zu scannen. Diese Befugnis stand durch die Erweiterung des Anwendungsbereichs des Telekommunikationsrechts durch die Kodex-RL 2018/1972 in Frage. Durch die VO (EU) 2021/1232 v. 14.7.2021 hat der europäische Gesetzgeber daher für Anbieter nummernunabhängiger interpersoneller Kommunikationsdienste eine Ausnahme von bestimmten Vorschriften der Richtlinie 2002/58/EG „hinsichtlich der Verwendung von Technologien durch zur Verarbeitung personenbezogener und anderer Daten zwecks Bekämpfung des sexuellen Missbrauchs von Kindern im Internet" geschaffen.

[150] Zu den Risiken der Technologie ausführlich *H. Abelson/R. Anderson et al.*, Bugs in our Pockets: The Risks of Client-Side Scanning, 14.10.2021.

3. Ziele und Grenzen der staatlichen Regulierung von Verschlüsselungstechnologien

Die erwähnten Regulierungsvorschläge haben noch keine hinreichend konkrete Gestalt angenommen, sodass eine umfassende rechtliche Würdigung möglich wäre. Hierfür kommt es entscheidend auch auf die Feinheiten der technischen Umsetzung an.[151] Zum aktuellen Zeitpunkt lassen sich daher nur allgemeine Leitlinien angeben, an denen sich die Kryptopolitik bei solchen Regulierungsvorhaben orientieren muss.

a) Gewährleistungsverantwortung und Förderpflicht

Der bisherige Grundkonsens deutscher Kryptopolitik, Verschlüsselungstechnik als Grundlage sicherer Informationstechnik zu fördern, ist verfassungsrechtlich in der staatlichen Gewährleistungsverantwortung für die IT-Sicherheit fundiert. Der Staat kommt dieser Verantwortung nicht nur durch entsprechende Forschungs- und Innovationsförderung nach.[152] Durch seine Behörden leistet er auch ganz konkrete Unterstützung für Unternehmen und Private bei der Implementation und Anwendung kryptographischer Verfahren (vgl. § 3 Nr. 14, 14a, 19 BSIG).[153] Darüber hinaus lässt sich den einzelnen Grundrechten[154] keine konkrete Vorgabe für das jeweils notwendige Verschlüsselungsniveau entnehmen, etwa dergestalt, dass die Anbieter von OTT-Kommunikation von Verfassungs wegen zur Einführung bestimmter Formen einer Ende-zu-Ende-Verschlüsselung verpflichtet werden müssen.[155] Hier hat der Gesetzgeber vielmehr Gestaltungsspielräume.

b) Beeinträchtigungen der Integrität von Verschlüsselungsmechanismen

Staatliches Handeln, das die Integrität von Verschlüsselungsmechanismen beeinträchtigt, muss selbstverständlich den rechtsstaatlichen Anforderungen genügen, das heißt vor allem auch grundrechtskonform sein. Ein Bedarf nach einem eigenständigen (Grund-)Recht auf Verschlüsselung[156] besteht dabei

---

[151] Zentrales Petitum bei *Landau*, Exceptional Access: The Devil is in the Details, Lawfare v. 26.12.2018.

[152] Hierzu auch im europäischen Kontext oben unter § 6 II. 3. b).

[153] Vgl. beispielhaft für diesbezügliche Aktivitäten staatlicher Stellen: *BMWi*, Einsatz von elektronischer Verschlüsselung – Hemmnisse für die Wirtschaft, 26.2.2018; *BSI*, TR-02102–1 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version: 2022–01.

[154] Siehe § 7 Fn. 70.

[155] Entsprechend auch *Dietrich*, Der Einsatz von Verschlüsselungstechniken zwischen Grundrechtsschutz und staatlicher Sicherheitsgewährleistung, GSZ 2021, S. 1 (3 f.).

[156] Zu dieser Forderung siehe § 7 Fn. 138.

nicht.[157] Vielmehr kann Verschlüsseln selbst Aspekt von grundrechtlich relevantem Handeln sein, sodass Verbote oder Beschränkungen des Einsatzes von Verschlüsselungstechnologie als Eingriffe in die jeweiligen Grundrechte zu werten sind.[158] Entsprechende Regeln müssen sich daher den grundrechtlichen Rechtfertigungsanforderungen stellen. Was das Erfordernis einer gesetzlichen Ermächtigungsgrundlage betrifft, gilt dabei das oben zur Schwachstellen-Governance Ausgeführte.[159]

c) Grenzen der Verschlüsselungsregulierung

Grenzen der Regulierung von Verschlüsselung ergeben sich somit in erster Linie erneut aus dem Bestimmtheits- und dem Verhältnismäßigkeitsgebot.[160] Insoweit ist vor allem die potenzielle Streubreite staatlicher Maßnahmen zu bedenken, ist Verschlüsselung doch Grundlage für den sicheren Austausch letztlich aller digitaler Daten. Eine absolute Grenze für staatliche Eingriffe ist daher dort erreicht, wo diese unkontrollierbare Folgewirkungen für die IT-Sicherheit haben. Dies ist beispielsweise der Fall, wenn grundlegende Verschlüsselungsprotokolle kompromittiert werden.[161] Das Inverkehrbringen einzelner Geräte mit fehlerhafter Verschlüsselung – seit langem ein beliebtes Vorgehen der Sicherheitsbehörden[162] – ist hingegen typischerweise beherrschbar und daher nicht per se unzulässig.

Anders als staatliche Manipulationen, die die Integrität der Verschlüsselungstechnik selbst, d. h. unabhängig von konkreten Anwendungskontexten kompromittieren, sind auch punktuelle Verbote des Einsatzes von Verschlüsselung bzw. von bestimmten Implementationsformen der Verschlüsselung für

---

[157] Ausführlich dazu *Gerhards*, (Grund-)Recht auf Verschlüsselung?, 2010, S. 123 ff.; entsprechend auch *Dietrich*, Der Einsatz von Verschlüsselungstechniken zwischen Grundrechtsschutz und staatlicher Sicherheitsgewährleistung, GSZ 2021, S. 1 (2).

[158] Vgl. speziell für Art. 10 Abs. 1 GG oben § 5 Fn. 54. Vgl. allgemein auch *Gerhards*, (Grund-)Recht auf Verschlüsselung?, 2010, S. 123 ff.; *Dietrich*, Der Einsatz von Verschlüsselungstechniken zwischen Grundrechtsschutz und staatlicher Sicherheitsgewährleistung, GSZ 2021, S. 1 (2 f.).

[159] Siehe § 7 II. 3. b) aa).

[160] Siehe § 5 Fn. 56 ff. Vgl. auch bereits § 7 Fn. 33.

[161] Zur (nicht endgültig belegten) staatlichen Einflussnahme auf die Entwicklung des für die Internetsicherheit zentralen Protokollstandards IPsec siehe § 6 Fn. 78.

[162] Zur langjährigen Praxis des BND siehe *G. Miller*, The Intelligence Coup of the Century, Washington Post, 11.2.2020. Aktuell beschäftigt der Fall „EncroChat" intensiv die europäische Justiz; ähnlich ist auch der Fall „Sky EEC" gelagert. Die juristische Debatte hierzu stellt allerdings bislang nicht das Inverkehrbringen kompromittierter Geräte, sondern die Rechtfertigung der konkreten Überwachungsmaßnahmen in den Vordergrund, vgl. aus der Literatur dazu nur *B. Derin/T. Singelnstein*, Verwendung und Verwertung von Daten aus massenhaften Eingriffen in informationstechnische Systeme aus dem Ausland (Encrochat), NStZ 2021, S. 449 ff.; *A. Roth*, EncroChat und kein Ende, GSZ 2021, S. 238 ff.; *A. Gebhard/R. Michalke*, Der Zweck heiligt die Mittel nicht, NJW 2022, S. 655 ff.

einzelne Dienste oder Kontexte nicht unter allen Umständen verfassungswidrig.[163] Dies gilt prima facie auch für Maßnahmen wie „Exceptional Access" oder „Client Side Scanning", die im öffentlichen Interesse ausgewählte Diensteanbieter zur Änderung ihrer Verschlüsselungsarchitektur verpflichten, was zur Absenkung des Sicherheitsniveaus nur dieser Dienste und Anwendungen führt. Auch eine allgemeine Pflicht, für die Kommunikation über OTT-Dienste nur Transport- und keine Ende-zu-Ende-Verschlüsselung anzubieten, sodass Anbieter dem staatlichen Verlangen nach Herausgabe der ihnen bekannten Schlüssel stets nachkommen könnten, wäre hier einzuordnen.[164] Im Ergebnis entsprechen derartige Maßnahmen dem Zwang zum Einbau einer „Hintertür", für die – wie dargestellt – eine illegale Nutzung seitens Dritter nie technisch sicher ausgeschlossen werden kann.

Allerdings wiegt die Beeinträchtigung der grundrechtlich geschützten Interessen *aller* Nutzer eines Dienstes, die mit Maßnahmen wie „Exceptional Access" einhergeht, im Lichte der üblichen Bewertungsmaßstäbe überaus schwer.[165] Kommt hinzu, dass staatlichen Stellen etwa durch die Nutzung von Schwachstellen effektive Alternativen zur Aufklärung zur Verfügung stehen, ist nicht ersichtlich, auf welche Weise eine derart großflächige Absenkung des IT-Sicherheitsniveaus gerechtfertigt werden kann.[166]

IV. Fazit

Informationssicherheit ist kein absolut geschütztes Rechtsgut. Staatliche Interventionen stehen hier jedoch vor hohen Hürden. Die verfassungsrechtliche Dimension derartiger Eingriffe wurde allerdings bisher nur teilweise richtig erkannt. Wohl auch aus diesem Grund ist das Feld bisher nur rudimentär rechtlich strukturiert worden. Sofern sich der Staat hier ein invasives Handeln vorbehalten möchte – wofür im Einzelfall gute Gründe sprechen mögen –, muss sich der Gesetzgeber der Thematik deutlich aktiver als bisher annehmen. Elementare Voraussetzung für entsprechende Maßnahmen ist die Ausarbeitung eines belastbaren Regulierungsrahmens für den Umgang mit Schwach-

[163] Ein globales Verbot von Verschlüsselung, wie es *Dietrich*, Der Einsatz von Verschlüsselungstechniken zwischen Grundrechtsschutz und staatlicher Sicherheitsgewährleistung, GSZ 2021, S. 1 (4), diskutiert, wäre hingegen offensichtlich unverhältnismäßig.

[164] Zu § 8 Abs. 3 TKÜV vgl. § 7 Fn. 124; vgl. allerdings den beschränkten Anwendungsbereich dieser Regelung gem. § 3 Abs. 1 S. 1 TKÜV.

[165] Im Falle von Exceptional Access sind maßgeblich die Grundrechte betroffen, die die (kommunikative) Privatsphäre schützen. Zum dort etablierten Faktor der Streubreite siehe § 5 Fn. 58 m. w. N.

[166] Skeptisch auch *Dietrich*, Der Einsatz von Verschlüsselungstechniken zwischen Grundrechtsschutz und staatlicher Sicherheitsgewährleistung, GSZ 2021, S. 1 (5). Vgl. auch allgemein in diese Richtung *S. Landau*, Listening In, 2017.

stellen. Ein Grundmodell hierfür wurde oben entwickelt. Dieses trägt der Tatsache Rechnung, dass Legislative und Exekutive angesichts der oft unvorhersehbaren Folgewirkungen hoheitlicher Interventionen hier besonders sensibel agieren müssen. Dies gilt nochmals gesteigert für Eingriffe in die Verschlüsselungstechnik.

Schluss

§ 8 Ausblick

Die stetig wachsende Zahl von Angriffen auf IT-Systeme ist nicht nur Krisenphänomen, sondern zeugt in erster Linie vom rasanten Fortschritt der Gesellschaft in Sachen Digitalisierung. Informationssicherheitsregulierung ist dementsprechend kein Krisenrecht, sondern die notwendige Reaktion des Rechtsstaats auf Veränderungen im Realbereich. In der Informationssicherheitsregulierung treten Recht und Technik in Austausch, um die Risiken der Digitalisierung beherrschbar zu machen, die Auswirkungen schädigender Ereignisse zu minimieren und die Belastungen angemessen zu verteilen.

Die Europäische Union und ihre Mitgliedstaaten haben in den letzten Jahren die Herausforderung angenommen, regulatorische Schutzmaßnahmen für die Informationsgesellschaft zu entwickeln. Die praktische Umsetzung ist allerdings mit erheblichen Herausforderungen konfrontiert, die ihren Ursprung in der spezifischen Struktur von Informationssicherheitsrisiken haben. Die Darstellung dieser Risikostrukturen, die Analyse und Bewertung der gesetzgeberischen Reaktionen und der Entwurf eines kohärenten Regulierungskonzepts bilden den Gegenstand dieser Arbeit.

Das Gerüst dieser Regulierung steht heute in weiten Teilen. Die Breite der Aufgabe und die dynamische Entwicklung der Technik werden dem Gesetzgeber aber in Zukunft erhebliche Anstrengungen abverlangen. Angesichts der fundamentalen Bedeutung der Sicherheitsgewährleistung für die Legitimität von Staat und Recht muss der Gesetzgeber diese Aufgabe ernst nehmen. Ebenso wie in der „analogen" Welt entscheidet sich an diesem Punkt, wie weit das Recht auch in der digitalen Gesellschaft mit seinem normativen Ordnungsanspruch durchdringen wird.

Die Fähigkeit, für die Sicherheit der Informationsordnung zu sorgen, muss der Staat aber auch aus einem weiteren elementaren Grund erwerben. Alle Überlegungen zur rechtlichen Regulierung der Informationstechnik müssen berücksichtigen, dass die (Informations-)Technik heute einen großen Teil dessen ausmacht, was der Staat *ist*. Diese Entwicklung begründet eine neue Abhängigkeit des Staates von der Technik. Werden technische Mittel punktuell zur Aufgabenerledigung herangezogen, lassen sich Ausfälle durch den Wechsel der Mittel kompensieren. Dies ist nicht mehr möglich, wenn informationstechnische Systeme zu einer für das Wirken des Staates unentbehrlichen Infrastruktur geworden sind. Hier öffnet sich ein Feld, das in der vorliegenden

Arbeit nur angedeutet, nicht ausgemessen wurde. Wenn die oft beschworene Wendung von der „digitalen Souveränität“ überhaupt einen Sinn hat, dann hier. Denn ein Staat, der weder die eigene Informationssicherheit noch die Informationssicherheit seiner Bürger garantieren kann, kann in einer digitalen Welt nicht mehr den Anspruch erheben, souverän zu sein.

§ 9 Zusammenfassung in Leitsätzen

I. Ausgangsproblem, Gegenstand und Ziel der Untersuchung

1. In einer umfassend digitalisierten und vernetzten Welt ist Informationssicherheit *systemrelevant*. Angesichts einer sich stetig verschärfenden Gefahrenlage ist konsentiert, dass die bisherigen, primär informellen Strategien zur Bewältigung der Informationssicherheitskrise nicht ausreichen. Vielmehr bedarf es verstärkter regulatorischer Anstrengungen. Ungeklärt ist allerdings, in welcher Form das Recht effektiv zur Abwehr von Informationssicherheitsrisiken beitragen kann. Hierfür ist auch verantwortlich, dass die rechtswissenschaftliche Durchdringung der Materie noch am Anfang steht (§ 1).

2. In den letzten Jahren hat sich der Regulierungsdruck kontinuierlich verschärft. In Deutschland wurden mit der Neufassung des BSIG im Jahr 2009, dem IT-SiG von 2015 und dem IT-SiG 2.0 von 2021 Regelungen erlassen, die weit in den gesellschaftlichen Bereich hinein auf eine Stärkung des Schutzniveaus für IT-Systeme und Netzwerke zielen. Auch die EU ist vielfach tätig geworden und gestaltet die Informationssicherheitsregulierung heute maßgeblich mit. Trotz dieses *Verrechtlichungsschubs* ist die Regulierungslandschaft nach wie vor fragmentiert und lückenhaft (§ 1 II.).

3. Der regulatorische Zugriff auf die Materie ist mit erheblichen Herausforderungen konfrontiert. Hierfür ist zum einen die besondere Struktur von Informationssicherheitsrisiken verantwortlich. Technische Schwachstellen gefährden nicht nur Hersteller, Betreiber und Nutzer und erleichtern aggressive Cyberaktivitäten jeder Art. Sie sind vielmehr auch für die Sicherheitsbehörden attraktiv, die diese Lücken für ihre Zwecke nutzen können, etwa zur Überwachung digitaler Kommunikation. Die Regulierung von Informationssicherheitsrisiken befindet sich daher in einem *„double bind"*. Dies hat Rückwirkungen auf den rechtspolitischen Diskurs, in dem aktuell Extrempositionen dominieren (§ 1 III.).

4. Zum anderen ist es aus regulatorischer Sicht alles andere als trivial, in dem bislang überwiegend privat organisierten, stark von den Eigengesetzlichkeiten der Technik geprägten und, jedenfalls in Teilbereichen, inhärent global strukturierten Feld der Informationssicherheitsgewährleistung rechtliche Ordnungsstrukturen zu etablieren. Die Analyse des Informationssicherheitsrechts berührt hier Grundfragen *rechtsstaatlich verantworteter Regulierung unter*

den Bedingungen der Digitalisierung und Globalisierung: Welche Wirkung kann das territorial radizierte Recht in der globalen Konstellation noch entfalten? Wie kann der Staat in einem hochkomplexen und hochdynamischen technischen Umfeld das erforderliche Regulierungswissen generieren? In welchem Verhältnis stehen staatliche und private Regulierung? Diese Fragen erfahren im vorliegenden Kontext eine besondere Zuspitzung, ist die Sicherheitsgewährleistung doch traditionell Kernfunktion von Staatlichkeit, zentraler Rechtfertigungsgrund für staatliche Herrschaft und Hauptindikator für staatliche Souveränität (§ 1 IV.).

5. Vor diesem Hintergrund ist es das *Ziel der Arbeit*, die verschiedenen Dimensionen der Aufgabe Informationssicherheit zu konkretisieren, die auf die Bewältigung dieser Aufgabe bezogene Rechtsmaterie zu strukturieren und davon ausgehend Grundbausteine eines Informationssicherheitsrechts zu entwickeln. Darüber hinaus verfolgt sie das Anliegen, die Herausforderungen zu konturieren, die die Digitalisierung und Globalisierung für das Recht bedeuten, und fragt, inwieweit der Staat unter diesen Bedingungen noch seinem Anspruch, Garant für die Sicherheit seiner Bürger zu sein, gerecht werden kann. Gleichzeitig gilt es auszuloten, inwieweit die Bemühungen des Staates um die Informationssicherheit mit seinen Bestrebungen kollidieren, Schwächen der Informationstechnik für eigene Zwecke auszunutzen (§ 2 I.–III.).

6. In methodischer Hinsicht ist die Arbeit einem *aufgabenbezogenen Verständnis* verpflichtet. Die Analyse und Bewertung der regulatorischen Vorgaben umfasst daher auch den Gesichtspunkt der Aufgabenadäquanz. Konkret verlangt dies, neben den rechtlichen Vorgaben auch die die Materie prägenden technischen und gesellschaftlichen Kontexte in den Blick zu nehmen. Zwischen den Maßstäben besteht kein Konkurrenz-, sondern ein Ergänzungsverhältnis. Gemeinsam können sie die Ausgestaltung des regulatorischen Programms anleiten und als Maßstab für die Bewertung bestehender Regelungen dienen. Eine besondere Herausforderung besteht vorliegend darin, dass bisher weitgehend ungeklärt ist, was alles zur „Aufgabe Informationssicherheit" gehört. Ziel der Arbeit ist es daher auch, Umfang und Grenzen des Informationssicherheitsproblems zu definieren (§ 2 IV.).

II. Grundlagen und Kontexte der Informationssicherheitsregulierung

7. Will das Recht Impulse für die Sicherheit der Informationstechnik setzen, ist das Teil jener Bemühungen des Staates um die Technik, die bis in die Zeiten der ersten Industriellen Revolution zurückreichen. Die *technikrechtliche* Dimension des Informationssicherheitsrechts ist von der Forschung allerdings bisher weitgehend ignoriert worden. Hierfür dürfte die enge Anbindung des Themas an das Datenschutzrecht, das eine eigenständige Regulierungstradi-

tion begründet hat, ausschlaggebend sein. Dies gilt es zu korrigieren. Die historisch-theoretische Rekonstruktion der zwischen Recht und Technik etablierten Kommunikationsbeziehungen macht dabei die Voraussetzungen, auf denen hoheitliche Technikregulierung basiert, deutlich. Sie zeigt zudem, welche Einsichten die Strukturen und Instrumente des Technikrechts für die Ausgestaltung des Informationssicherheitsrechts speichern (§ 3).

8. Schon aufgrund der begrifflichen Nähe ist ferner das Verhältnis der Informationssicherheitsregulierung zum Sicherheitsrecht zu klären. Sicherheitsbegriff und Sicherheitsrecht sind allerdings selbst seit geraumer Zeit Gegenstand intensiver Debatten. Diese werden auch durch das Informationssicherheitsproblem angetrieben, dient die dortige Infragestellung der etablierten Abgrenzung von „technischer" und „allgemeiner" Sicherheit doch Kritikern wie Befürwortern des *„neuen" Sicherheitsrechts* als Beleg für ihre Thesen, dass hier eine Relativierung liberal-rechtsstaatlicher Standards betrieben werde („Versicherheitlichung") bzw. dass ein grundlegender Umbau der rechtsstaatlichen „Sicherheitsarchitektur" unumgänglich sei (§ 4 I.).

9. Jedenfalls für die Informationssicherheit lässt sich jedoch zeigen, dass Versuche zur Konsolidierung und Effektuierung der Sicherheitsgewährleistung, die etablierte dogmatische Schemata überwinden, nicht notwendig Grundrechte, Gewaltenteilungsprinzip und föderale Kompetenzverteilung kompromittieren müssen, sondern auch eine sachgerechte Form vorsorgender Politik darstellen können. Soweit es daher im Recht der Informationssicherheit zu regulatorischen Neukonfigurationen kommt, die in einem *„All-Gefahren-Ansatz"* münden, lässt sich dies rechtfertigen, wenn nur auf diese Weise die Sicherheit einer komplexen, weitgehend anonymen, inhärent globalen und intensiv miteinander vernetzten Technologie gewährleistet werden kann. Besonders deutlich wird die Herausforderung, wenn das für die hergebrachte Sicherheitsregulierung fundamentale Kriterium der Verantwortung auf den Cyberraum angewendet werden soll. Die Analyse des sogenannten *„Attributionsproblems"* zeigt, dass die personale Verantwortungslogik des Rechts hier an ihre praktischen Grenzen kommt. Aus ähnlichen Gründen erweist sich die tradierte Unterscheidung von *safety*- und *security*-bezogener Regulierung als untauglich, um der Informationssicherheitsregulierung Strukturen zu verleihen. Vor diesem Hintergrund besteht die Herausforderung sowohl für die Gestaltung wie für die Analyse des Informationssicherheitsrechts darin, die neuen, aufgabenangemessenen, typischerweise breit und integrativ angelegten Regulierungsstrukturen in ein Verhältnis zu den Kategorien und Differenzierungen der tradierten verfassungs- und verwaltungsrechtlichen Dogmatik zu setzen. Hierfür erweist sich das Konzept der *Aufmerksamkeitsfelder*, an denen sich Gestaltung und Analyse der Materie orientieren müssen, als hilfreich (§ 4 II.).

10. Der von der Untersuchung verwendete Sicherheitsbegriff stellt somit insgesamt ein *offenes, heuristisches Konzept* dar, das seinen konkreten norma-

tiven Gehalt erst durch die Aufarbeitung des spezifischen Kontextes sowie mit Blick auf die maßgeblichen rechtlichen Regelungen – d. h. insbesondere auch auf die rechtlichen Grenzen – erhält. Der Begriff ist neutral, sowohl was die Entstehung der Gefährdungslage (Naturereignisse, Private, hoheitliche Akteure, Drittstaaten etc.) als auch was die Art und Intensität der Gefahr bzw. des Risikos sowie die Natur der Schutzgüter betrifft (§ 4 III.).

III. Unions- und verfassungsrechtliche Rahmenbedingungen der Informationssicherheitsregulierung

11. Zur Konturierung der in § 4 identifizierten Aufmerksamkeitsfelder sind die *grund- und organisationsrechtlichen Vorgaben des Grundgesetzes und des Unionsprimärrechts* zu analysieren. Hierbei sind sowohl jene Normen in den Blick zu nehmen, aus denen sich eine staatliche Verpflichtung ableiten lässt, Maßnahmen zur Abwehr von Informationssicherheitsrisiken zu ergreifen, als auch jene, die entsprechenden Interventionen Grenzen ziehen. Gestaltungsvorschläge müssen sich zudem im Rahmen der geltenden staatsorganisationsrechtlichen Prinzipien halten (§ 5).

12. Bei der Bestimmung der *grundrechtlichen Grenzen*, die hoheitlichen Interventionen durch das Grundgesetz und die Grundrechtecharta in Sachen Informationssicherheit gezogen sind, ist erneut zu berücksichtigen, dass derartige Interventionen unterschiedliche Stoßrichtungen verfolgen können („double bind"). Folgende allgemeine Maximen lassen sich hierzu formulieren (§ 5 I.):

a. Staatlichen Interventionen, die in Gestalt regulatorischer Vorgaben für private Betreiber digitaler Dienste und Infrastrukturen auf eine *Erhöhung des Informationssicherheitsniveaus* zielen, lassen sich regelmäßig durch das hohe Gewicht des Sicherheitsinteresses und der dadurch mittelbar geschützten Grundrechtsinteressen der Kunden und Nutzer rechtfertigen, wenn man die systemische Natur und mögliche Kaskadeneffekte von IT-Sicherheitsrisiken berücksichtigt. An dieser rechtlichen Bewertung ändert sich auch dann nichts, sofern man mit jüngeren Ansätzen in der Literatur den grundrechtlichen Interessen der betroffenen Digitalunternehmen durch eine kontextsensiblere Auslegung der einschlägigen Grundrechtsgarantien (insbesondere Art. 12 GG) Rechnung trägt. Deutlich stärker strukturierende Effekte für die Ausgestaltung des Informationssicherheitsrechts haben hingegen die Privatheitsinteressen der von den Sicherheitsmaßnahmen betroffenen Nutzer. Denn die technische Gewährleistung von Informationssicherheit verlangt vielfach die Verarbeitung von personenbezogenen Daten. Dient die Maßnahme zugleich dem Schutz der Nutzer, handelt es sich hierbei aus verfassungsrechtlicher Sicht um eine interne Spannungslage innerhalb des Grundrechts auf Datenschutz, die

nicht durch klare Vorrangregeln, sondern allein nach den Regeln des schonenden Ausgleichs bewältigt werden kann.

b. Weit engere Grenzen ziehen die Grundrechte staatlichem Handeln demgegenüber, wenn dieses *IT-Schwachstellen ausnutzt* oder gar aktiv das Informationssicherheitsniveau senkt. Solche staatlichen Maßnahmen haben potenziell Auswirkungen auf alle möglichen Grundrechte, da grundrechtlich relevantes Handeln heute in zahlreichen Bereichen von der Vertraulichkeit, Verfügbarkeit und Integrität der dafür genutzten informationstechnischen Systeme abhängig.

c. In seiner ersten Entscheidung zur Online-Durchsuchung aus dem Jahr 2007 hat das Bundesverfassungsgericht zwar eine zukunftsweisende Beschreibung des Informationssicherheitsproblems vorgelegt. Das als Antwort darauf entwickelte Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme hat freilich den Vertraulichkeits- und Integritätsschutz kaum erhöht. Eigentliches Defizit des „neuen" Grundrechts ist allerdings die Verengung, die die Diskussion um die grundrechtliche Relevanz von IT-Sicherheit durch ihre Verortung im allgemeinen Persönlichkeitsrecht erfahren hat. Dies verstellt bis heute den Blick darauf, dass Informationssicherheit *kein eigenständiges grundrechtliches Schutzgut*, sondern Querschnittsbedingung für die Ausübung zahlreicher, keineswegs nur dem Privatheitsschutz zuzuordnenden Grundrechte ist. Die grundrechtliche Bewertung staatlicher Manipulationen der Informationssicherheit muss sich daher aus dem Korsett des „IT-Grundrechts" lösen und differenzierte, auf den konkreten Eingriff angepasste Rechtfertigungsprogramme entwickeln.

13. Beeinträchtigungen der Integrität und Vertraulichkeit von IT-Systemen und digitalen Diensten drohen nicht nur durch (deutsche) Behörden, sondern auch und vor allem durch private Dritte sowie zunehmend durch fremde Staaten. Direktionskraft entfalten die Grundrechte für das staatliche Handeln daher nicht nur, indem sie den Staat darauf verpflichten, bestimmte Aktivitäten zu unterlassen. Vielmehr kann die *objektiv-rechtliche Funktion der Grundrechte* den Staat auch zur Hebung des Sicherheitsniveaus verpflichten (§ 5 II.):

a. Eine entsprechende normative Verdichtung muss stets aus einer konkret einschlägigen Grundrechtsgarantie heraus begründet werden. Eine allgemeine grundrechtliche Pflicht zur Gewährleistung von Informationssicherheit existiert ebenso wenig wie ein allgemeines „Recht" auf Sicherheit. Angesichts des Grads der digitalen Durchdringung der Lebenswelt lässt sich allerdings für zahlreiche Grundrechte plausibel machen, dass deren objektiv-rechtlicher Gehalt auch eine Absicherung durch Vorgaben zur Informationssicherheit verlangt (*Grundrechtsschutz durch Informationssicherheit*).

b. Die Übersetzung dieser Vorgaben in ein konkretes Regulierungsprogramm muss sich auch im Lichte der dem Gesetzgeber zustehenden Einschätzungs-, Wertungs- und Gestaltungsspielräume am Maßstab der *Risikoadäquanz* orientieren. Dabei ist zu berücksichtigen, ob staatliches Handeln zu ei-

ner Risikoerhöhung geführt hat. So trifft den Staat eine besonders intensive Garantenstellung hinsichtlich potenzieller integritätsverletzender Zugriffe Dritter, wenn er solche Zugriffe, etwa durch die Verpflichtung zur Vorratsdatenspeicherung oder das Verbot von Verschlüsselungstechniken, gewollt oder ungewollt erleichtert hat.

14. Die Integration des für die effektive Gewährleistung von Informationssicherheit geforderten All-Gefahren-Ansatz in die unions- und grundgesetzliche Kompetenzordnung ist nicht gänzlich spannungsfrei möglich. Beobachten lässt sich eine *latente Zentralisierung und Hochzonung* der Informationssicherheitsregulierung, die unter dem Gesichtspunkt der Aufgabenadäquanz begrüßenswert erscheinen mag, die jedoch den geltenden Kompetenzrahmen herausfordert. Soweit dem auf der Ebene der Verwaltung durch den Aufbau neuer Institutionen und deren Vernetzung begegnet wird, stellt dies aus kompetenzrechtlicher Sicht zwar ein milderes Mittel dar. Die Multiplizierung der Institutionen und ihre wechselseitige Vernetzung werfen jedoch in der Verwaltungspraxis erhebliche *Probleme der Koordinierung und Durchsetzung* auf. Der Grundsatz der Verantwortungsklarheit darf nicht kompromittiert werden (§ 5 III. 1.).

15. *Legitimationsfragen* stellen sich im Informationssicherheitsrecht aktuell nicht in exponiertem Maße. Bisher enthält das Unionsrecht keine Vorgaben, die zur Organisation des BSI als unabhängiger Behörde zwingen würden. Eine Lösung des BSI aus dem ministerialen Weisungszusammenhang ist auch aus Sachgründen nicht geboten. Allenfalls dann, wenn das BSI über seine Funktionen für die Exekutive hinaus umfassende Dienstleistungen für andere Staatsgewalten (Bundestag, Bundesgerichte) übernehmen würde, läge ein derartiger Schritt nahe. Keinen legitimatorischen Bedenken begegnet es ferner, wenn sich der Informationssicherheitsgesetzgeber auf eine Grobsteuerung der Materie beschränkt und die Konkretisierung seiner Vorgaben Behörden oder Privaten überlässt (§ 5 III. 2.).

IV. Grundzüge eines regulatorischen Schutzkonzepts

16. Die zahlreichen Regeln im Völker-, Unions- und nationalen Recht zur Informationssicherheit sind fragmentiert und lückenhaft. In der Literatur ist treffend von einem regulatorischen „patchwork of confusion“ die Rede. Die fehlende Klarheit über Umfang und Ziele des regulatorischen Programms gefährdet den Steuerungsanspruch des Rechts. Um dem abzuhelfen, gilt es, das geltende Recht mit den aufgabenbezogenen Anforderungen einerseits und den verfassungsrechtlichen Gewährleitungspflichten andererseits in Beziehung zu setzen, um auf dieser Grundlage die zentralen Regelungsstrukturen des Informationssicherheitsrechts freizulegen. Dabei wird hier nicht das Ziel verfolgt,

ein widerspruchsfreies „holistisches" Regelungssystem zu präsentieren. Angesichts der differenzierten und dynamischen Natur der Aufgabenstellung, der großen Zahl der im Mehrebenensystem zu beteiligenden Regulierungsakteure und der komplexen Abwägungen, die bei der Ausgestaltung der Querschnittsmaterie anzustellen sind, wäre wenig damit gewonnen, die Materie als klar geordnetes und festgefügtes „Rechtsgebiet" zu präsentieren. So erheben die im Folgenden erarbeiteten Regelungsstrukturen zwar den Anspruch auf eine aufgabenadäquate Beschreibung des Informationssicherheitsproblems und seiner Regulierung. Doch blenden sie den Suchprozess, auf den sich die regulatorische Aneignung neuer technischer Risiken stets einlassen muss, nicht aus. Zudem erkennen sie an, dass das „reale" Informationssicherheitsrecht jedenfalls auf mittlere Sicht durch Heterogenität, Lücken und normative Brüche geprägt sein wird. Eine auch am Gedanken der praktischen Wirksamkeit orientierte Rechtswissenschaft darf dies nicht ignorieren, sondern muss Strategien für den Umgang damit entwickeln (§ 6 I.).

17. Die zu diesem Zweck eingenommene integrative Perspektive kann vier allgemeine Bausteine bzw. Strukturelemente identifizieren, zu denen sich alle regulatorischen Bemühungen um die Informationssicherheit verhalten müssen (§ 6 II. 1–4):

a. Ausgangspunkt ist die bereits eingeforderte Bestimmung der *Aufgabe Informationssicherheit*. Hier hat der bisherige Regulierungsdiskurs eine signifikante Lücke. Dieser konzentriert sich auf die bekannten Schutzziele der Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit etc.), blendet jedoch aus, auf welchen Feldern und mit welchen Mitteln diese Ziele zu erreichen sind. Der Blick ins geltende Recht hilft an dieser Stelle nicht weiter, steht dessen Aufgabenadäquanz doch gerade auf dem Prüfstand. Es bedarf daher einer Bestandsaufnahme des Realbereichs, die freilich im Lichte der oben beschriebenen methodischen Grundsätze die rechtliche Regulierungsperspektive bei der Beschreibung der technischen Zusammenhänge nicht aus den Augen verlieren darf. Zu diesem Zweck wird hier ein *Schichtenmodell* entwickelt, wie es sich bereits in anderen Feldern der Digitalregulierung als analytisches Instrument bewährt hat. Der ersten Schicht ist dabei der *System- und Netzwerkschutz* zuzuordnen. Die zweite Schicht bildet die *Komponentensicherheit*. Schließlich müssen Kommunikationsarchitekturen sicher sein, die den Rahmen für die Kommunikation zwischen Netzwerken setzen, d. h. im Wesentlichen das Internet (*Internetsicherheit)*. Die drei Schichten dürfen nicht isoliert betrachtet werden. Eine aufgabenadäquate Regulierung muss vielmehr eine schichtenübergreifende Perspektive einnehmen (§ 6 II. 1.).

b. Die praktische Erfahrung und die Analyse des Schichtenmodells zeigen, dass die Möglichkeiten von Nationalstaaten und supranationalen Organisationen zur aufgabenadäquaten Regulierung in territorialer Hinsicht begrenzt sind. Das Problem verschärft sich durch den weitgehenden Ausfall der koor-

dinierenden Instanzen des Völkerrechts. Allerdings zeigen Referenzgebiete wie das Datenschutzrecht, dass sich auch zahlreiche Prozesse im digitalen Raum effektiv territorialisieren lassen. Dies lässt sich auf die Informationssicherheitsregulierung übertragen, die durch expansive Jurisdiktionsregeln, durch den Aufbau von Koordinations- und Kooperationsinstanzen sowie durch Lokalisierungspflichten grenzüberschreitenden Regulierungsdruck erzeugen kann. Dies ist allerdings mit teils erheblichen regulatorischen Kosten verbunden (§ 6 II. 2.).

c. Regulierung, die Impulse für Innovationen setzen bzw. auf sonstige Weise die Risiken der Informationstechnik einhegen will, muss mit den technischen Details und den sozialen Kontexten rechtlicher Interventionen vertraut sein. In diesem Sinne ist Informationssicherheit aus regulatorischer Sicht auch und in erster Linie ein Wissensproblem. Da hoheitliche Stellen selbst regelmäßig kein ausreichendes Regulierungswissen vorhalten, bedarf es Maßnahmen zur Wissensgenerierung und -distribution, die den privaten Sektor umfassen, die aber auch innerhalb der Verwaltung spezialisierte Organisationseinheiten und hinreichend leistungsfähige administrative Netzwerke etablieren. Das Informationssicherheitsrecht nutzt zu diesem Zweck schon heute zahlreiche Instrumente, von der Forschungsförderung bis hin zu Melde- und Informationspflichten. Zu wenig Aufmerksamkeit wird allerdings noch der Frage gewidmet, wie die Qualität der erhobenen Daten gesteigert und das Management des Wissens verbessert werden kann. Der Aufbau eines europäisch geführten und nach einheitlichen Kriterien administrierten Informationssystems ist nach wie vor ein Desiderat (§ 6 II. 3.).

d. Angesichts des für die Informationssicherheit prägenden Attributionsproblems kommt zuletzt auch der *Ausgestaltung der Verantwortungsarchitektur* zentrale Bedeutung zu. Der Gesetzgeber hat hier in jüngerer Zeit einen Paradigmenwechsel weg von der Störerhaftung hin zur Inpflichtnahme der Nichtstörer vollzogen. Dieser Wandel ist grundsätzlich sachangemessen. Im Detail weisen die entsprechenden Regelungen allerdings Defizite auf. Während das Verantwortlichkeitskriterium im Bereich der Netzwerk- und Systemsicherheit mittlerweile einigermaßen konsistent gehandhabt wird, sind die entsprechenden Ansätze im Bereich der Komponenten- und der Internetsicherheit nach wie vor lückenhaft und zudem nicht immer ideal implementiert (§ 6 II. 4.).

18. Aufbauend auf den vier allgemeinen Strukturelementen können dann *schichtenspezifische Pflichtenprogramme* zur Netzwerk- und Systemsicherheit, zur Komponentensicherheit und zur Internetsicherheit entwickelt werden, die durch öffentlich- und privatrechtliche Durchsetzungs- und Kontrollmechanismen abzusichern sind (§ 6 II. 5–8.).

a. Die Ausgestaltung der Verpflichtung, technische und organisatorische Maßnahmen zur *Netzwerk- und Systemsicherheit* zu ergreifen, muss im *Wech-*

selspiel zwischen hoheitlicher Regulierung und privater Normsetzung erfolgen. Dabei erweist es sich als nicht sachgerecht, technische Dynamik und rechtliche Statik – ein alter Topos der Kritik am Technikrecht – gegeneinander auszuspielen. Vielmehr muss das Verhältnis hoheitlicher und privater Normsetzung im konkreten Regulierungskontext und im Lichte des jeweiligen Risikos ausbalanciert werden.

b. Mit entsprechenden Herausforderungen ist auch die Gewährleistung der *Komponentensicherheit* konfrontiert. Diese ist in jüngerer Zeit Gegenstand umfangreicher gesetzgeberischer Bemühungen geworden, die unter anderem den Anschluss an das allgemeine Produktsicherheitsrecht gesucht haben. Dabei hat sich der Gesetzgeber allerdings bisher zu sehr auf den Aufbau privater Normungsinstanzen und zu wenig auf die Schaffung administrativer Kontrollkapazitäten konzentriert.

c. Nach wie vor weitgehend terra incognita ist schließlich die Regulierung der *Internetsicherheit*. Die bestehenden Möglichkeiten zur Territorialisierung dieser Sicherheitsdimension werden bisher wenig genutzt. Hier besteht erheblicher Entwicklungsbedarf.

d. Unter den zur *Durchsetzung und Kontrolle* des Regulierungsregimes bemühten Instrumenten bedarf vor allem die Rolle des Strafrechts einer kritischen Reflexion. Auch wenn strafrechtliche Sanktionen als ultima ratio unverzichtbar sein mögen, ist ihre Wirksamkeit durch das Territorialitäts- und das Attributionsproblem stark vermindert. Zudem hat die Pönalisierung der Materie teils erhebliche kontraproduktive Effekte. Weitere Verschärfungen des Strafrechts sind daher nicht geboten; das Gegenteil ist der Fall.

20. Insgesamt zeigt die Entwicklung des Informationssicherheitsrechts in den letzten Jahren, dass das „patchwork of confusion" allmählich einem strukturierteren Vorgehen weicht. Fünf übergreifende und tendenziell begrüßenswerte Entwicklungstrends lassen sich ausmachen: Eine deutliche *Europäisierung* der Rechtssetzung in Sachen Informationssicherheit; eine *Pluralisierung* der Regulierung, die den jeweiligen Regulierungskontexten größere Aufmerksamkeit widmet; eine starke *Institutionalisierung* sowohl in Gestalt des Auf- und Ausbaus spezialisierter Fachbehörden als auch in Form breiter Verbundstrukturen; der Wechsel von einem sektoral geprägten hin zu einem *horizontalen* Regulierungsmodell, das dem Querschnittscharakter der Problematik besser Rechnung trägt; sowie zuletzt, jedenfalls auf europäischer Ebene, eine konsequent als auf ein *rein defensives* IT-Sicherheitsverständnis ausgerichtete Informationssicherheitspolitik (§ 6 III.).

V. Grenzen für staatliche Manipulationen der Informationssicherheit

21. Staatliche Akteure gehören heute – global betrachtet – zu den wichtigsten Urhebern von Cyber-Unsicherheit. Auch deutsche Behörden sind nicht durchgängig einem rein defensiven IT-Sicherheitsverständnis verpflichtet. Vielmehr nutzen sie IT-Sicherheitslücken für eigene Zwecke, meist – etwa in Gestalt der Quellen-TKÜ – zur Abwehr von Gefahren oder zur Strafverfolgung. Entsprechende Maßnahmen stehen nicht nur deswegen unter besonderer Beobachtung, da sie tief in die Privatsphäre der Betroffen eingreifen. Sie werden vielmehr auch kritisiert, weil sie die Bemühungen des Staates, als Garant der Informationssicherheit zu wirken, effektiv unterminieren. Allein dieser zweite Aspekt wird hier näher betrachtet (§ 7 I.–III.):

a. In technisch-operativer Hinsicht setzen entsprechende Aktivitäten voraus, dass staatliche Stellen Kenntnis von IT-Schwachstellen erlangen, diese also entgegen den üblichen Regeln nicht offenlegen, sondern für eigene Zwecke nutzen. Ein derartiges Vorgehen erzeugt erhebliche Risiken für die IT-Sicherheit, deren rechtliche Relevanz bisher nicht hinreichend gewürdigt wurde: So führt die Nicht-Offenlegung regelmäßig dazu, dass auch Dritte die Lücke weiterhin ungestört ausnutzen können (*Kollisionsrisiko*). Zweitens zeigt die Erfahrung, dass entsprechendes behördliches Wissen durch Cyberangriffe erlangt oder sonst unbefugt in Verkehr gebracht werden kann (*Proliferationsrisiko*). Drittens können die von staatlichen Stellen genutzten Schwachstellen Manipulationen der Zielsysteme ermöglichen, die über das von der Maßnahme Bezweckte bzw. das von Rechts wegen Zulässige hinausgehen (*Einsatzrisiko*). Um diese Risiken auf ein (grund-)rechtlich noch akzeptables Maß zu reduzieren, bedarf es eines umfassenden *rechtlichen Rahmens für den staatlichen Umgang mit Schwachstellen*. Dessen Grundstrukturen werden hier erarbeitet.

b. Als Alternative zur staatlichen Schwachstellen-Nutzung wird in jüngerer Zeit – insbesondere im Kontext der Überwachung internetbasierter Kommunikation – über die regulatorische Schwächung der dort routinemäßig implementierten Ende-zu-Ende-Verschlüsselung diskutiert. Auf diese Weise soll verhindert werden, dass hoheitliche Überwachungsbefugnisse ins Leere laufen („going dark"). Doch auch wenn Verschlüsselung ohne Zweifel genutzt wird, um illegale Inhalte vor staatlichem Zugriff zu verbergen, zöge die Schwächung oder das Verbot potenter Verschlüsselungstechnologien erhebliche Kollateralschäden nach sich. Dies gilt auch für die derzeit auf Unionsebene diskutierten Vorhaben des „Exceptional Access" und des „Client Side Scanning".

22. Staatliche Manipulationen der Informationssicherheit stehen somit vor hohen rechtlichen Hürden. Entsprechende Eingriffe – für die im Einzelnen gute Gründe sprechen mögen –, verlangen vom Gesetzgeber in jedem Fall eine deutlich intensivere Befassung mit den dadurch erzeugten Risiken als bisher. Entsprechendes gilt für die Verfassungsgerichtsbarkeit.

Bibliographie*

Abbate, Janet: Inventing the Internet, Cambridge (Mass.) u. a. 1999.

Abelson, Hal/Anderson, Ross et al.: The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption, 1997, https://academiccommons.columbia.edu/doi/10.7916/D8GM8F2W.

–: Keys Under Doormats, 2015, https://www.schneier.com/wp-content/uploads/2016/09/paper-keys-under-doormats-CSAIL.pdf.

–: Bugs in our Pockets: The Risks of Client-Side Scanning, 2021, https://arxiv.org/abs/2110.07450.

Ablon, Lillian/Bogart, Andy: Zero Days, Thousands of Nights. The Life and Times of Zero-Day Vulnerabilities and Their Exploits, 2017, https://www.rand.org/pubs/research_reports/RR1751.html.

von Achenbach, Jelena: Anmerkung zu BVerfG, 21.10.2014 – 2 BvE 5/11, JZ 70 (2015), S. 96–99.

–: Parlamentarische Informationsrechte und Gewaltenteilung in der neueren Rechtsprechung des Bundesverfassungsgerichts, ZParl 48 (2017), S. 491–515.

Aden, Hartmut: Europäische Rechtsgrundlagen und Institutionen des Polizeihandelns, in: Lisken/Denninger, HdbPolR, 7. Aufl. München 2021, Kap. M.

Adriaans, Pieter: Information, in: Edward N. Zalta (Hrsg.), The Stanford Encyclopedia of Philosophy, Fall 2020 Edition, https://plato.stanford.edu/archives/fall2020/entries/information.

Agrafiotis, Ioannis/Nurse, Jason/Goldsmith, Michael/Creese, Sadie/Upton, David: A Taxonomy of Cyber-Harms. Defining the Impacts of Cyber-Attacks and Understanding How They Propagate, Journal of Cybersecurity 4:1 (2018), S. 1–15.

Aichholzer, Georg/Bora, Alfons/Bröchler, Stephan/Decker, Michael/Latzer, Michael (Hrsg.): Technology Governance. Der Beitrag der Technikfolgenabschätzung, Berlin 2010.

AK Grundsatz der DSK: ohne Titel, 9.11.2020, https://fragdenstaat.de/dokumente/9490-berichtakgrundsatzrahmenbedingungenproduktwarnungen002/.

Albers, Marion: Die Determination polizeilicher Tätigkeit in den Bereichen der Straftatenverhütung und der Verfolgungsvorsorge, Berlin 2001.

–: Information als neue Dimension im Recht, Rechtstheorie 33 (2002), S. 61–89.

–: Informationelle Selbstbestimmung, Baden-Baden 2005.

–: Grundrechtsschutz der Privatheit, DVBl. 2010, S. 1061–1069.

* Die in der Bibliographie angeführten Internetquellen wurden zuletzt am 1.9.2022 abgerufen. Soweit in den Fußnoten des Werks auf Übersichtsseiten im Internet verwiesen wurde, wurde darauf verzichtet, diese in die Bibliographie aufzunehmen. Ebenfalls nicht aufgenommen wurden Dokumente aus dem Gesetzgebungsverfahren und aus dem parlamentarischen Betrieb, die sich mit Hilfe des angegebenen Aktenzeichens über die üblichen Informationssysteme auffinden lassen.

–: Realizing the Complexity of Data Protection, in: Serge Gutwirth/Paul de Hert/Ronald Leenes (Hrsg.), Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenges, Dordrecht u. a. 2014, S. 213–235.
–: Sicherheitsbehördliche Vernetzung und Datenschutz, in: Margrit Seckelmann (Hrsg), Digitalisierte Verwaltung – Vernetztes E-Government, 2. Aufl. 2019, S. 509–533.
–: Umgang mit personenbezogenen Informationen und Daten, in: Andreas Voßkuhle/Martin Eifert/Christoph Möllers (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. 1, 3. Aufl. München 2022, § 22.
Albrecht, Peter-Alexis: Das Strafrecht auf dem Weg zur Sicherheitsgesellschaft, in: Gunnar Folke Schuppert/Wolfgang Merkel/Georg Nolte/Michael Zürn (Hrsg.), Der Rechtsstaat unter Bewährungsdruck, Baden-Baden 2010, S. 55–72.
von Alemann, Florian: Die Notwendigkeit eines formalen Rechtsbegriffes der Unionsrechtsordnung, Der Staat 45 (2006), S. 383–401.
Alexy, Robert: Theorie der juristischen Argumentation, Frankfurt am Main 1978.
Allianz: Allianz Risk Barometer, Januar 2022, https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html.
Altenhain, Karsten: IT-Strafrecht – Entstehung eines Rechtsgebiets, in: Norman Weiß (Hrsg.), Rechtsentwicklungen im vereinten Deutschland, Potsdam 2011, S 117–144.
Ambashta, Mimasa: Taking a Hard Look at the Vulnerabilities Equities Process and its National Security Implications, Berkeley Tech. L. J. Blog v. 22.4.2019, https://btlj.org/2019/04/taking-a-hard-look-at-the-vulnerable-equities-process-in-national-security/.
Amnesty International: Forensic Methodology Report, 18.7.2021, https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/.
Anderson, Ross: Why Information Security is Hard – An Economic Perspective, 2001, https://www.acsac.org/2001/papers/110.pdf.
anon.: U.S. Military Undergoes Restructuring to Emphasize Cyber and Space Capabilities, AJIL 113:3 (2019), S. 634–640.
Appel, Ivo: Das Verwaltungsrecht zwischen klassischem dogmatischen Verständnis und steuerungswissenschaftlichem Anspruch, in: VVDStRL 67 (2008), S. 226–285.
Aradau, Claudia: Security and the Democratic Scene: Desecuritization and Emancipation, Journal of International Relations and Development 7:4 (2004), S. 388–413.
von Arnauld, Andreas: Einbindung und Autonomie Privaten Rechts in die staatliche Rechtsordnung, in: Christian Bumke/Anne Röthel (Hrsg.), Privates Recht, Tübingen 2012, S. 246–268.
Arquilla, John/Ronfeldt, David (Hrsg.): In Athena's Camp. Preparing for Conflict in the Information Age, Santa Monica 1997.
Auby, Jean-Bernard: Die Transformation der Verwaltung und des Verwaltungsrechts, in: Armin von Bogdandy/Sabino Cassese/Peter M. Huber (Hrsg.), Handbuch Ius Publicum Europaeum, Bd. III, Heidelberg 2010, § 56.
Auerbach, Karl: Deconstructing Internet Governance, 26.2.2004, http://www.cavebear.com/archive/rw/deconstructing-internet-governance-ITU-Feb26–27–2004.htm.
Augsberg, Ino (Hrsg.): Extrajuridisches Wissen im Verwaltungsrecht. Analysen und Perspektiven, Tübingen 2013.
–: Informationsverwaltungsrecht. Zur kognitiven Dimension der rechtlichen Steuerung von Verwaltungsentscheidungen, Tübingen 2014.

Augsberg, Steffen: Rechtsetzung zwischen Staat und Gesellschaft. Möglichkeiten differenzierter Steuerung des Kapitalmarktes, Berlin 2003.
August, Vincent: Technologisches Regieren. Der Aufstieg des Netzwerk-Denkens in der Krise der Moderne. Foucault, Luhmann und die Kybernetik, Bielefeld 2021.
Aulehner, Josef: Polizeiliche Gefahren- und Informationsvorsorge. Grundlagen, Rechts- und Vollzugsstrukturen, dargestellt auch im Hinblick auf die deutsche Beteiligung an einem Europäischen Polizeiamt (EUROPOL), Berlin 1998.
Australian Signals Directorate: Responsible Release Principles for Cyber Security Vulnerabilities, 2022, https://www.asd.gov.au/sites/default/files/2022–03/Responsible-Release-Principles-for-Cyber-Security-Vulnerabilities.pdf.
Avant, Deborah/Haufler, Virginia: Public–Private Interactions and Practices of Security, in: Alexandra Gheciu/William C. Wohlforth (Hrsg.), The Oxford Handbook of International Security, Oxford 2018, S. 350–361.
Avbelj, Matej/Komárek, Jan (Hrsg.): Constitutional Pluralism in the European Union and Beyond, Oxford 2012.
Baade, Björnstjern: Fake News and International Law, EJIL 29:4 (2018), S. 1357–1376.
Bachmann, Gregor: Private Ordnung. Grundlagen ziviler Regelsetzung, Tübingen 2006.
–: Legitimation privaten Rechts, in: Christian Bumke/Anne Röthel (Hrsg.), Privates Recht, Tübingen 2012, S. 207–227.
Bachof, Otto: Die Dogmatik des Verwaltungsrechts vor den Gegenwartsaufgaben der Verwaltung, in: VVDStRL 30 (1972), S. 194–244.
Bäcker, Matthias: Das IT-Grundrecht: Funktion, Schutzgehalt, Auswirkungen auf staatliche Ermittlungen, in: Robert Uerpmann-Wittzack (Hrsg.), Das neue Computergrundrecht, Münster 2009, S. 1–30.
–: Die Vertraulichkeit der Internetkommunikation, in: Hartmut Rensen/Stefan Brink (Hrsg.), Linien der Rechtsprechung des Bundesverfassungsgerichts – erörtert von den wissenschaftlichen Mitarbeitern, Berlin 2009, S. 99–136.
–: Kriminalpräventionsrecht. Eine rechtsetzungsorientierte Studie zum Polizeirecht, zum Strafrecht und zum Strafverfahrensrecht, Tübingen 2015.
–: Von der Gefahr zum „Gefährder", in: Andreas Kulick/Michael Goldhammer (Hrsg.), Der Terrorist als Feind? Personalisierung im Polizei- und Völkerrecht, Tübingen 2020, S. 147–165.
–: Sicherheitsverfassungsrecht, in: Matthias Herdegen/Johannes Masing/Ralf Poscher/Klaus F. Gärditz (Hrsg.), Handbuch des Verfassungsrechts. Darstellung in transnationaler Perspektive, 2021, § 28.
–: Organisationsverfassungsrechtliche Grundlagen der Polizeiarbeit, in: Lisken/Denninger, HdbPolR, 7. Aufl. 2021, Kap. B III.
Bäcker, Matthias/Golla, Sebastian: Schutz der IT-Sicherheit durch Gefahrenabwehr, Strafverfolgung und nachrichtendienstliche Aufklärung, in: Gerrit Hornung/Martin Schallbruch (Hrsg.), IT-Sicherheitsrecht, Baden-Baden 2021, § 18.
Badura, Peter: Verwaltungsrecht im liberalen und im sozialen Rechtsstaat, Tübingen 1966.
Baecker, Dirk: Womit handeln Banken? Eine Untersuchung zur Risikoverarbeitung in der Wirtschaft, Frankfurt a. M. 1991.
Baecker, Ronald M.: Computers and Society. Modern Perspectives, Oxford 2019.
Baer, Susanne: Verwaltungsaufgaben, in: Andreas Voßkuhle/Martin Eifert/Christoph Möllers (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. 1, 3. Aufl. München 2022, § 13.

BaFin: Mindestanforderungen an das Risikomanagement (MaRisk), Rundschreiben 10/2021 in der Fassung vom 16.8.2021, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2021/rs_1021_MaRisk_BA.html.
–: Bankaufsichtliche Anforderungen an die IT (BAIT), Rundschreiben 10/2017 in der Fassung vom 16.8.2021, https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1710_ba_BAIT.pdf?__blob=publicationFile&v=6.
–: Zahlungsdiensteaufsichtliche Anforderungen an die IT von Zahlungs- und E-Geld-Instituten (ZAIT), Rundschreiben 11/2021 in der Fassung vom 16.8.2021, https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1121_BA_ZAIT.html.
Baker, Stewart: How Long Will Unbreakable Commercial Encryption Last?, Lawfare v. 20.9.2019, https://www.lawfareblog.com/how-long-will-unbreakable-commercial-encryption-last.
Baldus, Manfred: Entgrenzungen des Sicherheitsrechts – Neue Polizeirechtsdogmatik, DV 47 (2014), S. 1–23.
Baldwin, David A.: The Concept of Security, Review of International Studies 23:1 (1997), S. 5–26.
Baldwin, Robert/Cave, Martin/Lodge, Martin: Understanding Regulation. Theory, Strategy, and Practice, 2. Aufl. Oxford u. a. 2012.
Balzacq, Thierry: Securitization Theory. How security problems emerge and dissolve, Abingdon u. a. 2011.
Banks, William: State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0, Tex. L. Rev. 95 (2017), S. 1487–1513.
Bannelier, Karine/Christakis, Théodore: Cyber-Attacks – Prevention-Reactions. The Role of States and Private Actors, Paris 2017.
Bantlin, Franziska: Die G 10-Kommission – Zur Kontrolle der Nachrichtendienste, Berlin 2021.
Baran, Paul: On Distributed Communications Networks, IEEE Transactions on Communications Systems 12:1 (1964), S. 1–9.
–: Communications, computers and people, in: American Federation of Information Processing Societies (Hrsg.), Proceedings of the 1965 Fall Joint Computer Conference, Part II, New York 1965, S. 45–49.
Barczak, Tristan: Der nervöse Staat. Ausnahmezustand und Resilienz des Rechts in der Sicherheitsgesellschaft, 2. Aufl. Tübingen 2021.
Barlow, John Perry: A Declaration of the Independence of Cyberspace, in: Peter Ludlow (Hrsg.), Crypto Anarchy, Cyberstates, And Pirate Utopias. Part II, Cambridge (Mass.) 2001, S. 27–30.
Bast, Jürgen: Völker- und unionsrechtliche Anstöße zur Entterritorialisierung des Rechts, in: VVDStRL 76 (2017), S. 277–313.
Battis, Ulrich/Gusy, Christoph: Technische Normen im Baurecht, Düsseldorf 1988.
Bauer, Sebastian: Soziale Netzwerke und strafprozessuale Ermittlungen, Berlin 2018.
Bauer, Susanne/Heinemann, Torsten/Lemke, Thomas (Hrsg.): Science and Technology Studies. Klassische Positionen und aktuelle Perspektiven, Berlin 2017.
Baum, Gerhart: Freiheit: Ein Appell, 2021.
Baum, Gerhart/Kurz, Constanze/Schantz, Peter: Das vergessene Grundrecht, F.A.Z., 26.2.2013, http://www.faz.net/-gsf-778tf.
Bautze, Kristina: Die Fragmentierungsdebatte. Zwischen Einheit, Diversifikation und self-fulfilling prophecy, AVR 54 (2016), S. 91–100.

Bayerisches Landesamt für Datenschutzaufsicht: Good Practice bei technischen und organisatorischen Maßnahmen. Generischer Ansatz nach Art. 32 DS-GVO zur Sicherheit, 13.10.2020, https://www.lda.bayern.de/media/checkliste/baylda_checkliste_tom.pdf.

Bayertz, Kurt/Quante, Michael: Marxistische Technikphilosophie, in: Armin Grunwald (Hrsg.), Technikethik, Stuttgart u. a. 2013, S. 89–98.

BBK: 10 Jahre „KRITIS-Strategie". Einblicke in die Umsetzung der Nationalen Strategie zum Schutz Kritischer Infrastrukturen, 2020, https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/PiB/PiB-21-zehn-jahre-kritis-strategie.pdf?__blob=publicationFile&v=7.

–: Klärung und Erweiterung des KRITIS-Vokabulars. Kriterien und Vorgehensweise, 2021, https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/KRITIS/baukasten-kritis-vokabular-1.pdf?__blob=publicationFile&v=5.

BDI/DIN/DKE: Europaweite Cyberregulierung, 1.2.2021, https://www.din.de/resource/blob/788010/50c9e8bdb9890fa70935963033a2b34f/2021-bdi-din-dke-position-cybersicherheit-europa-de-final-data.pdf.

Beck, Stefan/Niewöhner, Jörg/Sörensen, Estrid: Science and Technology Studies: Eine sozialanthropologische Einführung, Bielefeld 2014.

Beck, Ulrich: Risikogesellschaft, Frankfurt a. M. 1986.

–: Weltrisikogesellschaft. Auf der Suche nach der verlorenen Sicherheit, Frankfurt a. M. 2008.

Becker, Florian: Kooperative und konsensuale Strukturen in der Normsetzung, Tübingen 2005.

–: Grundrechtliche Grenzen staatlicher Überwachung zur Gefahrenabwehr, NVwZ 2015, S. 1335–1340.

Bederna, Zsolt/Rajnai, Zoltan: Analysis of the cybersecurity ecosystem in the European Union, Int'l Cybersecurity L. Rev. 2022, S. 35–49.

Beissel, Stefan: Cybersecurity Investments. Decision Support under Economic Aspects, New York u. a. 2016.

Benda, Ernst: Privatsphäre und „Persönlichkeitsprofil", in: Gerhard Leibholz/Hans Joachim Faller et al. (Hrsg.), Menschenwürde und freiheitliche Rechtsordnung. Festschrift für Willi Geiger zum 65. Geburtstag, Tübingen 1974, S. 23–44.

–: Das Recht auf informationelle Selbstbestimmung und die Rechtsprechung des Bundesverfassungsgerichts zum Datenschutz, DuD 8 (1984), S. 86–90.

Bendiek, Annegret/Pander Maat, Eva: The EU's Regulatory Approach to Cybersecurity, SWP Working Paper, 2.10.2019, https://www.swp-berlin.org/publications/products/arbeitspapiere/WP_2019_Bendiek_Pander_Maat_EU_Approach_Cybersecurity.pdf.

–: The EU's Cybersecurity Policy: Building a Resilient Regulatory Framework, in: Gabi Siboni/Limor Ezioni (Hrsg.), Cybersecurity and Legal-Regulatory Aspects, Singapur 2021, S. 23–64.

Benedek, Wolfgang/Bauer, Veronika/Kettemann, Matthias (Hrsg.): Internet Governance and the Information Society: Global Perspectives and European Dimensions, Utrecht 2008.

Benkler, Yochai: From Consumers to Users. Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access, Fed. Comm. L. J. 52 (2000), S. 561–579.

Bennett Moses, Lyria: How to Think about Law, Regulation and Technology: Problems

with 'Technology' as a Regulatory Target, Law, Innovation and Technology 5:1 (2013), S. 1–20.
Benz, Arthur: Kooperative Verwaltung, Baden-Baden 1994.
Berberich, Matthias: Virtuelles Eigentum, Tübingen 2010.
Berg, Wilfried: Vom Wettlauf zwischen Recht und Technik. Am Beispiel neuer Regelungsversuche im Bereich der Informationstechnologie, JZ 40 (1985), S. 401–407.
Berkman Center for Internet & Society: Don't Panic. Making Progress on the "Going Dark" Debate, 1.2.2016, https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.
Berlit, Uwe/Dreier, Horst: Die legislative Auseinandersetzung mit dem Terrorismus, in: Fritz Sack/Heinz Steinert (Hrsg.), Protest und Reaktion, Opladen 1984, S. 227–318.
Bernau, Patrick: „Deutschland scheitert in kleinen Schritten", F.A.Z., 30.5.2021, https://zeitung.faz.net/fas/wirtschaft/2021–05–30/fe89e2d58aeac7fb63fbf74704468576/.
Betz, David J./Stevens, Tim: Cyberspace and the State. Toward a Strategy for Cyberpower, Abingdon u. a. 2011.
Bijker, Wiebe E.: Of Bicycles, Bakelites, and Bulbs. Toward a Theory of Sociotechnical Change, Cambridge (Mass.) 1995.
Bijker, Wiebe E./Hughes, Thomas P./Pinch, Trevor J. (Hrsg.): The Social Construction of Technological Systems. New Directions in the Sociology and History of Technology, Cambridge (Mass.) 1987.
Binder, Jens-Hinrich: Regulierungsinstrumente und Regulierungsstrategien im Kapitalgesellschaftsrecht, Tübingen 2012.
Binninger, Clemens: Das Nebeneinander von Bundes- und Landesbehörden in der Inneren Sicherheit – Probleme und Lösungsvorschläge aus Sicht der parlamentarischen Praxis, in: Jahrbuch des Föderalismus 2018, S. 88–99.
Birkland, Thomas A.: After Disaster. Agenda Setting, Public Policy, and Focusing Events, Washington D.C. 1997.
Biselli, Anna: „Ende des freien Internets in seiner bisherigen Form", Netzpolitik.org v. 12.3.2015, https://netzpolitik.org/2015/ende-des-freien-internets-in-seiner-bisherigen-form-leak-aus-rat-der-eu-warnt-vor-code-of-conduct-zur-cybersicherheit/.
–: Wir veröffentlichen Dokumente zum Bundestagshack: Wie man die Abgeordneten im Unklaren ließ, Netzpolitik.org v. 7.3.2016, https://netzpolitik.org/2016/wir-veroeffentlichen-dokumente-zum-bundestagshack-wie-man-die-abgeordneten-im-unklaren-liess/.
Bizer, Johann: Die Kryptokontroverse – Innere Sicherheit und Sicherungsinfrastrukturen, in: Volker Hammer (Hrsg.), Sicherungsinfrastrukturen – Gestaltungsvorschläge für Technik, Organisation und Recht, Berlin u. a. 1995, S. 179–216.
BKA: Standardisierende Leistungsbeschreibung für Software zur Durchführung von Maßnahmen der Quellen-Kommunikationsüberwachung und der Online-Durchsuchung, 5.10.2018, https://www.bka.de/SharedDocs/Downloads/DE/Sonstiges/standardisierendeLeistungsbeschreibungQuellenTKUE.pdf.
–: Bundeslagebild Cybercrime 2021, Mai 2022, https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html.
Black, Julia: The Role of Risk in Regulatory Processes, in: Robert Baldwin/Martin Cave/Martin Lodge (Hrsg.), The Oxford Handbook of Regulation, Oxford 2010, S. 302–348.
Blomley, Nicholas K./Delaney, David/Ford, Richard T.: The Legal Geographies Reader. Law, Power, and Space, Oxford u. a. 2001.

Blumenthal, Marjory/Clark, David D.: Rethinking the Design of the Internet: The End-to-end Arguments vs. the Brave New World, ACM Transactions on Internet Technology 1 (2001), S. 70–109.

BMBF: Digital. Sicher. Souverän. Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit 2021–2026, Juni 2021, https://www.bmbf.de/SharedDocs/Publikationen/de/bmbf/5/31672_Digital_Sicher_Souveraen.html.

BMI: Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI), 2005, https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/05–12–09/05–12–09-anlage-nr-16.pdf?__blob=publicationFile&v=2.

–: Schutz Kritischer Infrastrukturen – Basisschutzkonzept, September 2005, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritische-infrastrukturen-basisschutzkonzept.html.

–: Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen, 2007, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/IT-digitalpolitik/umsetzungsplan-kritis.html.

–: Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), Juni 2009, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.html.

–: Cyber-Sicherheitsstrategie für Deutschland 2016, 2016, https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf.

–: Cybersicherheitsstrategie 2021, 2021, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf?__blob=publicationFile&v=2.

–: Referentenentwurf. Zweite Verordnung zur Änderung der BSI-Kritisverordnung, 22.4.2021, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/zweite-verordnung-aenderung-bsi-kritis-vo-refe.html.

–: Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat. Ziele und Maßnahmen für die 20. Legislaturperiode, 2022, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislatur.pdf.

BMI/BBK: Stärkung des Bevölkerungsschutzes durch Neuausrichtung des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe, März 2021, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/03/konzept-neuausrichtung-bbk.html.

BMI/BSI: Charta zur Stärkung der vertrauenswürdigen Kommunikation, 18.11.2015, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/IT-digitalpolitik/charta-vertrauenswuerdige-kommunikation.html.

BMWi: Einsatz von elektronischer Verschlüsselung – Hemmnisse für die Wirtschaft, 26.2.2018, https://www.de.digital/DIGITAL/Redaktion/DE/Publikation/einsatz-von-elektronischer-verschluesselung-hemmnisse-fuer-die-wirtschaft.html.

BMWi: Schwerpunktstudie Digitale Souveränität, 2021, https://www.bmwk.de/Redaktion/DE/Publikationen/Digitale-Welt/schwerpunktstudie-digitale-souveranitaet.html.

BNetzA: IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz, August 2015, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_08–2015.pdf.

–: IT-Sicherheitskatalog gemäß § 11 Absatz 1b Energiewirtschaftsgesetz, Dezember

2018, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_2018.pdf.
–: Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Telekommunikationsgesetz (TKG) Version 2.0, Stand: 29.4.2020, https://www.bundesnetzagentur.de/sicherheitsanforderungen.
–: Liste der kritischen Funktionen nach § 109 Abs. 6 Satz 1 Nr. 2 TKG für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial, Stand: 18.8.2021, www.bundesnetzagentur.de/sicherheitsanforderungen.
Böck, Nicole/Theurer, Jakob: Herstellerpflichten und Haftungsrisiken bei IT-Sicherheitslücken vernetzter Produkte, BB 2021, S. 520–525.
Böckenförde, Ernst-Wolfgang: Grundrechte als Grundsatznormen. Zur gegenwärtigen Lage der Grundrechtsdogmatik, Der Staat 29 (1990), S. 1–31.
–: Die Organisationsgewalt im Bereich der Regierung, 2. Aufl. Berlin 1998.
–: Demokratie als Verfassungsprinzip, in: Josef Isensee/Paul Kirchhof (Hrsg.), Handbuch des Staatsrechts, Bd. II, 3. Aufl. 2004, § 24.
Böhlke, Dietmar/Yilmaz, Öznur: Auswirkungen von § 202c StGB auf die Praxis der IT-Sicherheit, CR 2008, S. 261–266.
Boehme-Neßler, Volker: Das Ende des Staates? Zu den Auswirkungen der Digitalisierung auf den Staat, ZÖR 64 (2009), S. 145–199.
–: BilderRecht, Berlin u. a. 2010.
Böhret, Carl: Gesetzesfolgenabschätzung, 2. Aufl. Speyer 1997.
Böken, Arnd: IT-Sicherheitsforschung, in: Dennis-Kenji Kipker (Hrsg.), Cybersecurity, München 2020, Kap. 15.
Böse, Martin: Kompetenzen der Union auf dem Gebiet des Straf- und Strafverfahrensrechts, in: Martin Böse (Hrsg.), Europäisches Strafrecht (Enzyklopädie Europarecht), Bd. 11, 2. Aufl. Baden-Baden 2021, § 4.
von Bogdandy, Armin: Gubernative Rechtsetzung. Eine Neubestimmung der Rechtsetzung und des Regierungssystems unter dem Grundgesetz in der Perspektive gemeineuropäischer Dogmatik, Tübingen 2000.
–: The Past and Promise of Doctrinal Constructivism: A Strategy for Responding to the Challenges Facing Constitutional Scholarship in Europe, I•CON 7 (2009), S. 364–400.
von Bogdandy, Armin/Hering, Laura: Die Informationsbeziehungen im europäischen Verwaltungsverbund, in: Andreas Voßkuhle/Martin Eifert/Christoph Möllers (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. 1, 3. Aufl. München 2022, § 25.
Bora, Alfons: Ökologie der Kontrolle. Technikregulierung unter der Bedingung von Nicht-Wissen, in: Christoph Engel/Jost Halfmann/Martin Schulte (Hrsg.), Wissen, Nichtwissen, unsicheres Wissen, Baden-Baden 2002, S. 253–275.
–: Im Schatten von Normen und Fakten – Die Kolonisierung der Politik durch technowissenschaftliche Normativität, Zeitschrift für Rechtssoziologie 27 (2006), S. 31–50.
– (Hrsg.): Rechtliches Risikomanagement. Form, Funktion und Leistungsfähigkeit des Rechts in der Risikogesellschaft, Berlin 1999.
Borowski, Martin: Grundrechte als Prinzipien, Baden-Baden 2007.
Borucki, Isabelle/Schünemann, Wolf J. (Hrsg.): Internet und Staat – Perspektiven auf eine komplizierte Beziehung, Baden-Baden 2019.
Bossong, Raphael: Der Ausbau von Frontex – zwischen politischer Symbolik und den

Dilemmas der Umsetzung, in: Robert Chr. van Ooyen/Martin H. W. Möllers (Hrsg), Jahrbuch Öffentliche Sicherheit 2020/2021, Baden-Baden 2021, S. 707–722.

Bourbeau, Philippe/Vuori, Juha A.: Security, Resilience and Desecuritization: Multidirectional Moves and Dynamics, Critical Studies on Security 3:3 (2015), S. 253–268.

Bourgon, Jocelyne: Responsive, Responsible and Respected Government. Towards a New Public Administration Theory, International Review of Administrative Sciences 73 (2007), S. 7–26.

Bradford, Anu: The Brussels Effect, Nw. U. L. Rev. 107 (2012), S. 1–68.

–: The Brussels Effect. How the European Union Rules the World, Oxford 2020.

Bradford Franklin, Sharon: The Need for Countries to Establish Robust and Transparent Vulnerabilities Equities Processes, Fletcher Security Review 6:1 (2019), S. 45–48.

Braithwaite, John/Coglianese, Cary/Levi-Faur, David: Can Regulation and Governance Make a Difference?, Regulation & Governance 1 (2007), S. 1–7.

Bredt, Stephan: Die demokratische Legitimation unabhängiger Institutionen. Vom funktionalen zum politikfeldbezogenen Demokratieprinzip, Tübingen 2006.

von Bremen, Anna: IT-Sicherheitsrecht in der Energiewirtschaft, EWeRK 2020, S. 29–34.

Bremser, Dietmar/Fritsch, Sebastian: Europäische Cybersicherheitszertifizierung – der große Sprung nach vorn?, BSI Forum in der <kes> 2020, S. 35–38.

Breuer, Rüdiger: Direkte und indirekte Rezeption technischer Regeln durch die Rechtsordnung, AöR 101 (1976), S. 46–88.

–: Freiheit des Berufs, in: Josef Isensee/Paul Kirchhof (Hrsg.), Handbuch des Staatsrechts, 3. Aufl. Heidelberg 2010, § 170.

Breyer, Stephen: Regulation and its Reform, Cambridge (Mass.) 1982.

Breyer, Stephen/Stewart, Richard B./Sunstein, Cass R./Vermeule, Adrian/Herz, Michael E.: Administrative Law and Regulatory Policy: Problems, Text, and Cases, 9. Aufl. New York 2022.

Britz, Gabriele: Vertraulichkeit und Integrität informationstechnischer Systeme, DÖV 2008, S. 411–415.

–: Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: Wolfgang Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, Tübingen 2010, S. 561–596.

–: Elektronische Verwaltung, in: Wolfgang Hoffmann-Riem/Eberhard Schmidt-Aßmann/Andreas Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. 2, 2. Aufl. München 2012, § 26.

Britz, Gabriele/Eifert, Martin: Digitale Verwaltung, in: Andreas Voßkuhle/Martin Eifert/Christoph Möllers (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. 1, 3. Aufl. München 2022, § 26.

Bröckling, Ulrich: Dispositive der Vorbeugung: Gefahrenabwehr, Resilienz, Precaution, in: Christopher Daase/Philipp Offermann/Valentin Rauer (Hrsg.), Sicherheitskultur – Soziale und politische Praktiken der Gefahrenabwehr, Frankfurt a. M. 2012, S. 93–108.

–: Gute Hirten führen sanft – Über Menschenregierungskünste, Berlin 2017.

Brodowski, Dominik: Cybersicherheit durch Cyber-Strafrecht? Über die strafrechtliche Regulierung des Internets, in: Hans-Jürgen Lange/Astrid Bötticher (Hrsg.), Cyber-Sicherheit, Wiesbaden 2015, S. 249–276.

–: Verdeckte technische Überwachungsmaßnahmen im Polizei- und Strafverfahrens-

recht. Zur rechtsstaatlichen und rechtspraktischen Notwendigkeit eines einheitlichen operativen Ermittlungsrechts, Tübingen 2016.
Brodowski, Dominik/Freiling, Felix C.: Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, 2011.
Broemel, Roland/Trute, Hans-Heinrich: Alles nur Datenschutz? Zur rechtlichen Regulierung algorithmenbasierter Wissensgenerierung, Berliner Debatte Initial 27:4 (2016), S. 50–65.
Brohm, Winfried: Strukturen der Wirtschaftsverwaltung. Organisationsformen und Gestaltungsmöglichkeiten im Wirtschaftsverwaltungsrecht, Stuttgart u. a. 1969.
–: Die Dogmatik des Verwaltungsrechts vor den Gegenwartsaufgaben in der Verwaltung, in: VVDStRL 30 (1972), S. 245–312.
Brooks, David J.: What Is Security: Definition Through Knowledge Categorization, Security Journal 23 (2009), S. 225–239.
Brousseau, Eric/Marzouki, Meryem/Méadel, Cécile (Hrsg.): Governance, Regulation and Powers on the Internet, Cambridge 2012.
Brown, Ian/Marsden, Christopher T.: Regulating Code. Good Governance and Better Regulation in the Information Age, Cambridge (Mass.) u. a. 2013.
Brownsword, Roger/Scotford, Eloise/Yeung, Karen: Law, Regulation, and Technology: The Field, Frame, and Focal Questions, in: dies. (Hrsg.), The Oxford Handbook of Law, Regulation, and Technology, Oxford 2017, S. 1–38.
– (Hrsg.): The Oxford Handbook of Law, Regulation, and Technology, Oxford 2017.
Brownsword, Roger/Yeung, Karen (Hrsg.): Regulating Technologies. Legal Futures, Regulatory Frames and Technological Fixes, Oxford 2008.
Brugger, Winfried: Gewährleistung von Freiheit und Sicherheit im Lichte unterschiedlicher Staats- und Verfassungsverständnisse, in: VVDStRL 63 (2004), S. 102–150.
Brummer, Chris: Territoriality as a Regulatory Technique: Notes from the Financial Crisis, University of Cincinnati L. Rev. 79 (2011), S. 499–526.
Brunst, Philipp W.: Cyberabwehr, in: Jan-Hendrik Dietrich/Sven-R. Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, Stuttgart u. a. 2017, S. 817–864.
BSI: Verschlüsselt kommunizieren im Internet, ohne Datum, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Verschluesselt-kommunizieren/verschluesselt-kommunizieren_node.html.
–: E-Mail Verschlüsselung, ohne Datum, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Verschluesselt-kommunizieren/E-Mail-Verschluesselung/e-mail-verschluesselung_node.html.
–: Die Lage der IT-Sicherheit in Deutschland 2014, 2014. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile&v=1.
–: Die Lage der IT-Sicherheit in Deutschland 2016, 2016, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.pdf?__blob=publicationFile&v=1.
–: IT-Grundschutz-Methodik, BSI-Standard 200–2, Version 1.0, Oktober 2017, https://www.bsi.bund.de/grundschutz.
–: Die Lage der IT-Sicherheit in Deutschland 2018, 2018, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?__blob=publicationFile&v=1.

–: Handhabung von Schwachstellen. Empfehlungen für Hersteller, BSI-CS 019, Version 2.0 v. 11.7.2018, https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_019.pdf.
–: Industrial Control System Security: Top 10 Bedrohungen und Gegenmaßnahmen v1.3, 27.2.2019, https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005.html.
–: Die Lage der IT-Sicherheit in Deutschland 2020, 2020, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2.
–: Lage der IT-Sicherheit in Deutschland 2021, 2021, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf?__blob=publicationFile&v=3.
–: TR-02102–1 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version: 2022–01, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.html.
–: CON.8: Software-Entwicklung, Februar 2021, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/03_CON_Konzepte_und_Vorgehensweisen/CON_8_Software_Entwicklung_Edition_2021.pdf?__blob=publicationFile&v=2.
–: SYS. 1.1: Allgemeiner Server, Februar 2021, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/07_SYS_IT_Systeme/SYS_1_1_Allgemeiner_Server_Edition_2021.pdf?__blob=publicationFile&v=2.
–: Glossar der Cyber-Sicherheit, 2022, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/glossar-der-cyber-sicherheit_node.html.
–: IT-Grundschutz-Bausteine: Edition 2022, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html.
Bubrowski, Helene: Katastrophenschutz stärken, Streit vermeiden, F.A.Z., 5.7.2022, https://www.faz.net/-gpg-at056.
–: Faeser will Grundgesetz für Cybersicherheit ändern, F.A.Z., 12.7.2022, https://www.faz.net/-gpg-atdxh.
Buchan, Russell: Cyber Espionage and International Law, Oxford u. a. 2019.
Buchanan, Ben: Nobody But Us: The Rise and Fall of the Golden Age of Signals Intelligence, Aegis Series Paper No. 1708, 30.8.2017, https://www.hoover.org/sites/default/files/research/docs/buchanan_webreadypdf.pdf.
–: The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations, Oxford 2017.
Buchheim, Johannes: Die Grenzen des „entgrenzten Gerichts“: Von der Notwendigkeit verfassungsprozessualer Rahmenbedingungen – ein Kommentar zum IT-Sicherheitslückenbeschluss des BVerfG vom 8. Juni 2021, VerfBlog, 27.7.2021, https://verfassungsblog.de/die-grenzen-des-entgrenzten-gerichts/.
Buchheim, Johannes/Möllers, Christoph: Gerichtliche Verwaltungskontrolle als Steuerungsinstrument, in: Andreas Voßkuhle/Martin Eifert/Christoph Möllers (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. 2, 3. Aufl. München 2022, § 46.
Buermeyer, Ulf/Golla, Sebastian: „Digitaler Hausfriedensbruch“ – Der Entwurf eines

Gesetzes zur Strafbarkeit der unbefugten Benutzung informationstechnischer Systeme, K&R 2017, S. 14–18.
Büthe, Tim/Mattli, Walter: The New Global Rulers. The Privatization of Regulation in the World Economy, Princeton u. a. 2011.
Bull, Hans Peter: Verwaltung durch Maschinen. Rechtsprobleme der Technisierung der Verwaltung, 1963.
–: Die „völlig unabhängige" Aufsichtsbehörde. Zum Urteil des EuGH vom 9.3.2010 in Sachen Datenschutzaufsicht, EuZW 2010, S. 488–494.
–: Informationelle Selbstbestimmung – Vision oder Illusion?, 2. Aufl. Tübingen 2011.
Bullinger, Martin: Regulierung als modernes Instrument zur Ordnung liberalisierter Wirtschaftszweige, DVBl. 2003, S. 1355–1361.
Bumke, Christian: Die Entwicklung der verwaltungsrechtswissenschaftlichen Methodik in der Bundesrepublik Deutschland, in: Eberhard Schmidt-Aßmann/Wolfgang Hoffmann-Riem (Hrsg.), Methoden der Verwaltungsrechtswissenschaft, Baden-Baden 2004, S. 73–130.
–: Rechtsetzung in der Europäischen Gemeinschaft. Bausteine einer gemeinschaftsrechtlichen Handlungsformenlehre, in: Gunnar Folke Schuppert/Ingolf Pernice/Ulrich Haltern (Hrsg.), Europawissenschaft, 2. Aufl. Baden-Baden 2006, S. 643–702.
–: Rechtsdogmatik, JZ 69 (2014), S. 641–650.
–: Rechtsdogmatik. Eine Disziplin und ihre Arbeitsweise, zugleich eine Studie über das rechtsdogmatische Arbeiten Friedrich Carl von Savignys, Tübingen 2017.
Bumke, Christian/Röthel, Anne: Auf der Suche nach einem Recht des privaten Rechts, in: dies. (Hrsg.), Privates Recht, Tübingen 2012, S. 1–20.
– (Hrsg.): Privates Recht, Tübingen 2012.
Bundesregierung: Bericht über die Anwendung der elektronischen Datenverarbeitung in der Bundesverwaltung, BT-Drs. V/3355, 1968.
–: Bericht zu den Auswirkungen der Nutzung kryptografischer Verfahren auf die Arbeit der Strafverfolgungs- und Sicherheitsbehörden (Verschlüsselungsbericht), 2002, https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/2002–06–06/anlage-15.pdf.
–: On the Application of International Law in Cyberspace, March 2021, https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf.
–: Deutsche Strategie zur Stärkung der Resilienz gegenüber Katastrophen, Juli 2022, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/BMI22017-resilienz-katastrophen.pdf.
Burgi, Martin: Die Energiewende und das Recht, JZ 68 (2013), S. 745–753.
–: Wohlstandsvorsorge als Staatsziel und als Determinante im Wirtschaftsverwaltungsrecht, AöR Beiheft 2014, S. 30–48.
–: Rechtsregime, in: Andreas Voßkuhle/Martin Eifert/Christoph Möllers (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. 1, 3. Aufl. München 2022, § 18.
Burk, Dan L.: Legal Consequences of the Cyberspatial Metaphor, in: Mia Consalvo/Nancy Baym et al. (Hrsg.), Internet Research Annual. Selected Papers from the Association of Internet Researchers Conferences 2000–2002, Bd. 1, New York 2003, S. 17–24.
Burton, Joe/Lain, Clare: Desecuritising Cybersecurity: Towards a Societal Approach, Journal of Cyber Policy 5:3 (2020), S. 449–470.

von dem Bussche, Axel/Schelinski, Tobias: Rechtsgrundlagen und Haftungsfolgen in der IT-Sicherheit, in: Andreas Leupold/Andreas Wiebe/Silke Glossner (Hrsg.), IT-Recht, 4. Aufl. München 2021, Teil 7.1.

Busse, Volker: Kabinettsausschüsse der Bundesregierung, DVBl. 1993, S. 413–417.

Buxbaum, Hannah L.: Territory, Territoriality, and the Resolution of Jurisdictional Conflict, Am. J. Comp. L. 57 (2009), S. 631–675.

Buzan, Barry/Hansen, Lene: The Evolution of International Security Studies, Cambridge 2009.

Buzan, Barry/Wæver, Ole/Wilde, Jaap de: Security. A New Framework for Analysis, Boulder (Colo.) 1998.

Cafaggi, Fabrizio (Hrsg.): Enforcement of Transnational Regulation. Ensuring Compliance in a Global World, Cheltenham 2012.

Calliess, Christian/Baumgarten, Ansgar: Cybersecurity in the EU. The Example of the Financial Sector: A Legal Perspective, German L. J. 21 (2020), S. 1149–1179.

Calliess, Gralf-Peter: Transnationales Verbrauchervertragsrecht, RabelsZ 68 (2004), S. 244–287.

– (Hrsg.): Transnationales Recht. Stand und Perspektiven, Tübingen 2014.

Calliess, Gralf-Peter/Zumbansen, Peer: Rough Consensus and Running Code. A Theory of Transnational Private Law, Oxford u. a. 2012.

Cancik, Pascale: Der „Kernbereich exekutiver Eigenverantwortung" – zur Relativität eines suggestiven Topos, ZParl 45 (2014), S. 885–907.

Carrapico, Helena/Barrinha, André: The EU as a Coherent (Cyber)Security Actor?, JCMS 55:6 (2017), S. 1254–1272.

Cassese, Sabino: New Paths for Administrative Law: A Manifesto, I•CON 10 (2012), S. 603–613.

Castells, Manuel: The Rise of the Network Society (1996), 2. Aufl. Oxford 2009.

–: The Power of Identity (1997), 2. Aufl. Oxford 2009.

–: End of Millennium (1998), 2. Aufl. Oxford 2010.

Caulfield, Tristan/Ioannidis, Christos/Pym, David: The U.S. Vulnerabilities Equities Process: An Economic Perspective, in: Stefan Rass/Bo An et al. (Hrsg.), Decision and Game Theory for Security. GameSec 2017, 2017, S. 131–150.

Center for the Protection of National Infrastructure: Security Assessment of the Transmission Control Protocol (TCP), 2009.

CEPS: Software Vulnerability Disclosure in Europe. Technology, Policies and Legal Challenge, June 2018, https://www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges/.

Cerf, Vint/Ryan, Patrick/Senges, Max: Internet Governance is our Shared Responsibility, I/S: A Journal of Law and Policy for the Information Society 10 (2014), S. 1–40.

Chander, Anupam: Is Data Localization a Solution for Schrems II?, Journal of International Economic Law 23:3 (2020), S. 771–784.

Chaos Computer Club: Stellungnahme v. 3.11.2020, https://www.cccs.de/2020–11–03-stellungnahme-cyberberagentur/Stellungnahme_Cybersicherheitsagentur.pdf.

Chaudhary, Tarun/Jordan, Jenna/Salomone, Michael/Baxter, Phil: Patchwork of Confusion. The Cybersecurity Coordination Problem, Journal of Cybersecurity 4:1 (2018), S. 1–13.

Choucri, Nazli: Cyberpolitics in International Relations, Cambridge u. a. 2012.

Chrétien, Patrice: Wissenschaft vom Verwaltungsrecht: Frankreich, in: Armin von

Bogdandy/Sabino Cassese/Peter M. Huber (Hrsg.), Handbuch Ius Publicum Europaeum, Bd. IV, Heidelberg 2011, § 58.
Christakis, Théodore: European Digital Sovereignty: Successfully Navigating Between the Brussels Effect and Europe's Quest for Strategic Autonomy, 7.12.2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3748098.
Christou, George: Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy, London 2016.
Clark, D. D.: The Design Philosophy of the DARPA Internet Protocols, Computer Communication Review 18:4 (1988), S. 106–114.
Clopton, Zachary D.: Territoriality, Technology, and National Security, U. Chi L. Rev. 83 (2016), S. 45–63.
Cohen, Julie E.: Cyberspace As/And Space, Colum. L. Rev. 107 (2007), S. 210–256.
Cohen, Reuven/Erez, Keren/ben-Avraham, Daniel/Havlin, Shlomo: Breakdown of the Internet under Intentional Attack, Physical Review Letters 86:16 (2001), S. 3682–3685.
Collier, Jamie: Cybersecurity Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision, Politics and Governance 6:2 (2018), S. 13–21.
Collier, Stephen J./Lakoff, Andrew: The Vulnerability of Vital Systems: How 'Critical Infrastructure' Became a Security Problem in: Myriam Dunn Cavelty/Kristian Søby Kristensen (Hrsg.), Securing 'the Homeland'. Critical infrastructure, risk and (in)security, Abingdon 2008, S. 17–39.
Collin, Peter: Staatliche Kapitalhilfe für Unternehmen. Polizeiwissenschaftliche Lehren und Nationalökonomie in der ersten Hälfte des 19. Jahrhunderts, Rechtsgeschichte 15 (2009), S. 126–144.
–: Privat-staatliche Regelungsstrukturen im frühen Industrie- und Sozialstaat, Berlin u. a. 2016.
–: The Legitimation of Self-Regulation and Co-Regulation in Corporatist Concepts of Legal Scholars in the Weimar Republic, Politics and Governance 5:1 (2017), S. 15–25.
–: Regulierte Selbstregulierung in rechtshistorischer Perspektive. Studien und Materialien, 2018, https://ssrn.com/abstract=3170912.
Collin, Peter/Bender, Gerd/Ruppert, Stefan/Seckelmann, Margrit/Stolleis, Michael (Hrsg.): Selbstregulierung im 19. Jahrhundert – zwischen Autonomie und staatlichen Steuerungsansprüchen, Frankfurt a. M. 2011.
–: Regulierte Selbstregulierung im frühen Interventions- und Sozialstaat, Frankfurt a.M. 2012.
–: Regulierte Selbstregulierung in der westlichen Welt des späten 19. und frühen 20. Jahrhunderts, Frankfurt a. M. 2014.
Committee on the Judiciary of the House of Representatives: Going Dark: Lawful Electronic Surveillance in the Face of New Technologies. Hearing before the Subcommittee on Crime, Terrorism and Homeland Security, 17.2.2011, https://www.govinfo.gov/content/pkg/CHRG-112hhrg64581/pdf/CHRG-112hhrg64581.pdf.
Conrad, Isabell/Streitz, Siegfried: Compliance, IT-Sicherheit, Ordnungsmäßigkeit der Datenverarbeitung, in: Astrid Auer-Reinsdorff/Isabell Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019, § 33.
Conze, Eckart: Securitization. Gegenwartsdiagnose oder historischer Analyseansatz?, Geschichte und Gesellschaft 38 (2012), S. 453–467.
Conze, Werner: „Sicherheit, Schutz", in: Otto Brunner/Werner Conze/Reinhart Ko-

selleck (Hrsg.), Geschichtliche Grundbegriffe. Historisches Lexikon zur politisch-sozialen Sprache in Deutschland, Bd. 5, Stuttgart 1984, S. 831–862.

Cordey, Sean/Dewar, Robert S. (Hrsg.): National Cybersecurity and Cyberdefense Policy Snapshots: Updated Collection 2, Center for Security Studies (CSS), ETH Zürich 2019.

Cormac, Rory/Aldrich, Richard J.: Grey is the New Black: Covert Action and Implausible Deniability, International Affairs 94:3 (2018), S. 477–494.

Cornils, Matthias: Entterritorialisierung im Wirtschaftsrecht und im Kommunikationsrecht, in: VVDStRL 76 (2017), S. 390–442.

Crawford, James: Brownlie's Principles of Public International Law, 9. Aufl. Oxford 2019.

Cremer, Wolfram: Freiheitsgrundrechte. Funktionen und Strukturen, 2003.

Cremona, Marise/Scott, Joanne (Hrsg.): EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law, Oxford 2018.

Cybersecurity and Infrastructure Security Agency: Cost of a Cyber Incident: Systematic Review and Cross-Validation, 26.10.2020, https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf.

Cyberspace Solarium Commission: Report, März 2020, https://www.fdd.org/analysis/2020/03/11/cyberspace-solarium-commission-report/.

Daase, Christopher: Sicherheitskultur als interdisziplinäres Forschungsprogramm, in: Christopher Daase/Philipp Offermann/Valentin Rauer (Hrsg.), Sicherheitskultur. Soziale und politische Praktiken der Gefahrenabwehr, Frankfurt a. M. 2012, S. 23–44.

Dammann, Ulrich/Karhausen, Mark/Müller, Paul/Steinmüller, Wilhelm (Hrsg.): Datenbanken und Datenschutz, Frankfurt a. M. 1974.

Daniel, Michael: Heartbleed: understanding when we disclose cyber vulnerabilities, 28.4.2014, https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

von Danwitz, Thomas: Was ist eigentlich Regulierung?, DÖV 2004, S. 977–985.

Daskal, Jennifer: The Un-Territoriality of Data, Yale L. J. 125 (2015), S. 326–398.

–: The Overlapping Web of Data, Territoriality, and Sovereignty, in: Paul Schiff Berman (Hrsg.), The Oxford Handbook of Global Legal Pluralism, Oxford 2020, S. 955–974.

Datenschutzkonferenz: Das Standard-Datenschutzmodell (Version 2.0b), 17.4.2020, https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V2.0b.pdf.

Davis, John S./Boudreaux, Benjamin et al.: Stateless Attribution. Toward International Accountability in Cyberspace, 2017, https://www.rand.org/pubs/research_reports/RR2081.html.

Davis, Joshua: Hackers Take Down the Most Wired Country in Europe, Wired, 21.8.2007, www.wired.com/2007/08/ff-estonia/.

de Búrca, Gráinne/Keohane, Robert O./Sabel, Charles F.: New Modes of Pluralist Global Governance, N.Y.U. J. Int'l L. & Pol. 45 (2012–2013), S. 723–786.

–: Global Experimentalist Governance, British Journal of Political Science 44 (2014), S. 477–486.

de Búrca, Gráinne/Scott, Joanne (Hrsg.): Law and New Governance in the EU and the US, Oxford, Portland 2006.

de Wyl, Christian/Weise, Michael/Bartsch, Alexander: Neue Sicherheitsanforderungen für Netzbetreiber. IT-Sicherheitsgesetz und IT-Sicherheitskatalog, N&R 2015, S. 23–28.

Debiel, Tobias: Human Security und die Vereinten Nationen. Eine Bestandsaufnahme nach 25 Jahren, in: Bernd Oberdorfer/Ines-Jacqueline Werkner (Hrsg.), Menschliche Sicherheit und gerechter Frieden, Wiesbaden 2019, S. 13–28.

DeCanio, Samuel: Democracy and the Origins of the American Regulatory State, New Haven u. a. 2015.

Decker, Michael/Grunwald, Armin/Knapp, Martin (Hrsg.): Der Systemblick auf Innovation. Technikfolgenabschätzung in der Technikgestaltung, Berlin 2012.

Deibert, Ronald: Parchment, Printing, and Hypermedia. Communication and World Order Transformation, New York 1997.

–: Trajectories for Future Cybersecurity Research, in: Alexandra Gheciu/William C. Wohlforth (Hrsg.), The Oxford Handbook of International Security, Oxford 2018, S. 531–546.

Deißler, Lena-Sophie: Gewährleistung von Informationsqualität in europäischen Informationssystemen. Eine Analyse behördlicher Pflichten und Instrumente zur Sicherstellung der Informationsqualität im Europäischen Verwaltungsverbund, Baden-Baden 2018.

Delacourt, John T.: The International Impact of Internet Regulation, Harv. Int'l L. J. 38 (1997), S. 207–235.

Delaney, David G.: Cybersecurity and the Administrative National Security State: Framing the Issues for Federal Legislation, Journal of Legislation 40 (2013–2014), S. 251–279.

Delerue, François: Cyber Operations and International Law, Cambridge 2020.

DeNardis, Laura: Protocol Politics. The globalization of Internet governance, Cambridge (Mass.) u. a. 2009.

– (Hrsg.): Opening Standards. The Global Politics of Interoperability, Cambridge (Mass.) 2011.

–: The Global War for Internet Governance, New Haven u. a. 2014.

–: The Internet Design Tension between Surveillance and Security, IEEEA 37:2 (2015), S. 72–83.

–: One Internet: An Evidentiary Basis for Policy Making on Internet Universality and Fragmentation, CIGI/Chatham House, Global Commission on Internet Governance Paper Series No. 38, 2016.

Denninger, Erhard: Der Präventions-Staat, Kritische Justiz 21 (1988), S. 1–15.

–: Verfassungsrechtliche Anforderungen an die Normsetzung im Umwelt- und Technikrecht, Baden-Baden 1990.

–: Rechtsstaatliche und demokratische Grundlagen der Polizeiarbeit, in: Lisken/Denninger, HdbPolR, 7. Aufl. 2021, Kap. B I.

Denninger, Erhard/Hoffmann-Riem, Wolfgang/Schneider, Hans-Peter/Stein, Ekkehart (Hrsg.): Kommentar zum Grundgesetz für die Bundesrepublik Deutschland (AK-GG), 3. Aufl. Neuwied u. a. 2001, Stand: 2. EL August 2002.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit: Vermerk: Abdingbarkeit von TOMs (Art. 32 DSGVO), 24.11.2021, https://datenschutz-hamburg.de/assets/pdf/Vermerk-Abdingbarkeit_TOMs.pdf.

Derin, Benjamin/Golla, Sebastian: Der Staat als Manipulant und Saboteur der IT-Sicherheit? Die Zulässigkeit von Begleitmaßnahmen zu „Online-Durchsuchung" und Quellen-TKÜ, NJW 2019, S. 1111–1116.

Derin, Benjamin/Singelnstein, Tobias: Verwendung und Verwertung von Daten aus

massenhaften Eingriffen in informationstechnische Systeme aus dem Ausland (Encrochat), NStZ 2021, S. 449–454.
Dessauer, Friedrich: Philosophie der Technik. Das Problem der Realisierung, Bonn 1926.
Deusch, Florian/Eggenhofer, Tobias: IT-Sicherheit, in: Jürgen Taeger/Jan Pohle (Hrsg.), Computerrechts-Handbuch, Stand: Februar 2021, Kapitel 50.1.
Deutscher Bundestag: Neunter Zwischenbericht der Enquete-Kommission „Internet und digitale Gesellschaft". Zugang, Struktur und Sicherheit im Netz, BT-Drs. 17/12541, 19.3.2013.
–: Wenig Beifall für das geplante IT-Sicherheitsgesetz 2.0, 2021, https://www.bundestag.de/dokumente/textarchiv/2021/kw09-pa-innen-informationstechnik-821484.
Deutscher Bundestag/Bundesarchiv (Hrsg.): Der Parlamentarische Rat 1948–1949. Akten und Protokolle, Boppard am Rhein 1975 ff.
Dewar, Robert S.: Cyber Security in the European Union: An Historical Institutionalist Analysis of a 21st Century Security Concern, Diss. Glasgow 2017, http://theses.gla.ac.uk/8188/.
–: The European Union and Cybersecurity: A Historiography of an Emerging Actor's Response to a Global Security Concern, in: Maria O'Neill/Ken Swinton (Hrsg.), Challenges and Critiques of the EU Internal Security Strategy, Newcastle upon Tyne 2017, S. 113–148.
Dewar, Robert S./Dunn Cavelty, Myriam: Die Cybersicherheitspolitik der Europäischen Union – Bollwerk gegen die Versicherheitlichung eines Politikbereichs, in: Wolf J. Schüneman/Marianne Kneuer (Hrsg.), E-Government und Netzpolitik im europäischen Vergleich, 2. Aufl. Baden-Baden 2019, S. 281–300.
Di Fabio, Udo: Risikoentscheidungen im Rechtsstaat. Zum Wandel der Dogmatik im öffentlichen Recht, insbesondere am Beispiel der Arzneimittelüberwachung, Tübingen 1994.
–: Verwaltung und Verwaltungsrecht zwischen gesellschaftlicher Selbstregulierung und staatlicher Steuerung, in: VVDStRL 56 (1997), S. 235–282.
–: Technikrecht – Entwicklung und kritische Analyse, in: Klaus Vieweg (Hrsg.), Techniksteuerung und Recht, Köln u. a. 2000, S. 9–21.
–: Der Verfassungsstaat in der Weltgesellschaft, Tübingen 2001.
–: Grundrechtsgeltung in digitalen Systemen. Selbstbestimmung und Wettbewerb im Netz, München 2016.
Dienel, Hans-Liudger (Hrsg.): Der Optimismus der Ingenieure. Triumph der Technik in der Krise der Moderne, Stuttgart 1998.
Dieterich, Peter: Systemgerechtigkeit und Kohärenz. Legislative Einheit und Vielheit durch Verfassungs- und Unionsrecht, Berlin 2014.
Dietlein, Johannes: Die Lehre von den grundrechtlichen Schutzpflichten, 2. Aufl. Berlin 2005.
Dietrich, Jan-Hendrik: Der Einsatz von Verschlüsselungstechniken zwischen Grundrechtsschutz und staatlicher Sicherheitsgewährleistung, GSZ 2021, S. 1–6.
Dietrich, Jan-Hendrik/Fahrner, Matthias/Gazeas, Nikolaos/von Heintschel-Heinegg, Bernd (Hrsg.): Handbuch Sicherheits- und Staatsschutzrecht, München 2022.
Diffie, Whitfield/Landau, Susan: Privacy on the Line. The Politics of Wiretapping and Encryption, Cambridge (Mass.) 1998.
–: The Export of Cryptography in the 20th Century and the 21st, in: Karl De Leeuw/Jan Bergstra (Hrsg.), The History of Information Security: A Comprehensive Handbook, Amsterdam 2007, S. 725–736.

Dimitropoulos, Georgios: Zertifizierung und Akkreditierung im Internationalen Verwaltungsverbund. Internationale Verbundverwaltung und gesellschaftliche Administration, Tübingen 2012.

Dix, Alexander: Unabhängige Datenschutzkontrolle als vorgezogener Grundrechtsschutz, in: Malte Kröger/Arne Pilniok (Hrsg.), Unabhängiges Verwalten in der Europäischen Union, Tübingen 2016, S. 121–130.

Djeffal, Christian: Neue Sicherungspflicht für Telemediendiensteanbieter. Webseitensicherheit jetzt Pflicht nach dem IT- Sicherheitsgesetz, MMR 2015, S. 716–721.

Dolata, Ulrich/Werle, Raymund (Hrsg.): Gesellschaft und die Macht der Technik. Sozioökonomischer und institutioneller Wandel durch Technisierung, Frankfurt a. M. 2007.

Dommann, Monika: Rechtsinstrumente. Die Übersetzung von Technik in Recht, Schweizerische Zeitschrift für Geschichte 55 (2005), S. 17–33.

Dommering, Egbert: Regulating Technology: Code is not Law, in: Egbert Dommering/Lodewijk Asscher (Hrsg.), Coding Regulation. Essays on the Normative Role of Information Technology, Den Haag 2006, S. 1–16.

Dornbusch, Julia: Das Kampfführungsrecht im internationalen Cyberkrieg, Baden-Baden 2019.

Dörr, Oliver: Die Anforderungen an ein zukunftsfähiges Infrastrukturrecht, in: VVDStRL 73 (2014), S. 323–368.

Drackert, Stefan: Die Risiken der Verarbeitung personenbezogener Daten. Eine Untersuchung zu den Grundlagen des Datenschutzrechts, Berlin 2014.

Drake, William/Wilson, Ernest (Hrsg.): Governing Global Electronic Networks: International Perspectives on Policy and Power, Cambridge 2008.

Drake, William/Cerf, Vinton G./Kleinwächter, Wolfgang: Internet Fragmentation: An Overview, World Economic Forum, Future of the Internet Initiative White Paper, 2016.

Dreier, Horst (Hrsg.): Grundgesetz-Kommentar, 3 Bde., 3. Aufl. Tübingen 2013–2018.

Dreier, Horst (Begr.)/*Brosius-Gersdorf, Frauke* (Hrsg.): Grundgesetz-Kommentar, Bd. 1, 4. Aufl. i. E.

Dreier, Horst/Forkel, Hans/Laubenthal, Klaus (Hrsg.): Raum und Recht. Festschrift 600 Jahre Würzburger Juristenfakultät, Berlin 2002.

Drüen, Klaus-Dieter: Die Indienstnahme Privater für den Vollzug von Steuergesetzen, Tübingen 2012.

DSK, Zur Möglichkeit der Nichtanwendung technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO auf ausdrücklichen Wunsch betroffener Personen, Beschluss vom 24.11.2021, https://www.datenschutzkonferenz-online.de/media/dskb/20211124_TOP_7_Beschluss_Verzicht_auf_TOMs.pdf.

Dürig, Günter (Begr.)/*Herzog, Roman/Scholz, Rupert/Herdegen, Matthias/Klein, Hans H.* (Hrsg.): Grundgesetz. Kommentar, Stand: 98. Ergänzungslieferung 2022 (Loseblatt-Ausgabe: 7 Bde., München 1958 ff.).

Dunn Cavelty, Myriam: Cyber-Security and Threat Politics. US Efforts to Secure the Information Age, London u. a. 2008.

–: Gesellschaft im Daueralarm. Gefahrendarstellungen im Cybersecurity-Diskurs, in: Christopher Daase/Stefan Engert/Julian Junk (Hrsg.), Verunsicherte Gesellschaft – überforderter Staat: Zum Wandel der Sicherheitskultur, Frankfurt a. M. u. a. 2013, S. 133–150.

–: Die materiellen Ursachen des Cyberkriegs. Cybersicherheitspolitik jenseits diskursiver Erklärungen, Journal of Self-Regulation and Regulation 1 (2015), S. 167–184.

–: Cybersecurity Research Meets Science and Technology Studies, Politics and Governance 6:2 (2018), S. 22–30.
–: Europe's cyber-power, European Politics and Society 19:3 (2018), S. 304–320.
Dunn Cavelty, Myriam/Egloff, Florian J.: The Politics of Cybersecurity: Balancing Different Roles of the State, St Antony's International Review 15 (2019), S. 37–57.
Dunn Cavelty, Myriam/Kavanagh, Camino: Cybersecurity and Human Rights, in: Ben Wagner/Matthias Kettemann/Kilian Vieth (Hrsg.), Research Handbook on Human Rights and Digital Technology, Cheltenham 2019, S. 73–97.
Dunn Cavelty, Myriam/Kristensen, Kristian Søby: Introduction: Securing the Homeland – Critical Infrastructure, Risk, and (In)Security, in: Myriam Dunn Cavelty/Kristian Søby Kristensen (Hrsg.), The Politics of Securing the Homeland: Critical Infrastructure, Risk and Securitisation, London 2008, S. 1–14.
Dunn Cavelty, Myriam/Mauer, Victor/Krishna-Hensel, Sai Felicia (Hrsg.): Power and Security in the Information Age. Investigating the Role of the State in Cyberspace, Aldershot u. a. 2007.
Dunn Cavelty, Myriam/Wenger, Andreas: Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science, Contemporary Security Policy 41:1 (2020), S. 5–32.
Dunn, Edgar S.: The Idea of a National Data Center and the Issue of Personal Privacy, The American Statistician 21 (1967), S. 21–27.
Durner, Wolfgang: Schutz der Verbraucher durch Regulierungsrecht, in: VVDStRL 70 (2011), S. 398–447.
Dyson, George: Turing's Cathedral. The Origins of the Digital Universe, New York 2012.
Eckert, Claudia: IT-Sicherheit, 10. Aufl. Berlin u. a. 2018.
Economides, Kim/Blacksell, Mark/Watkins, Charles: The Spatial Analysis of Legal Systems: Towards a Geography of Law?, Journal of Law and Society 13 (1986), S. 161–181.
Edwards, Paul: The Closed World. Computers and the Politics of Discourse in Cold War America, Cambridge (Mass.) 1996.
Efrony, Dan/Shany, Yuval: A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice, AJIL 112:4 (2018), S. 583–657.
Egloff, Florian: Contested Public Attributions of Cyber Incidents and the Role of Academia, Contemporary Security Policy 41:1 (2020), S. 55–81.
–: Intentions and Cyberterrorism, in: Paul Cornish (Hrsg.), The Oxford Handbook of Cyber Security, Oxford 2021, S. 187–200.
Egloff, Florian J./Dunn Cavelty, Myriam: Attribution and Knowledge Creation Assemblages in Cybersecurity Politics, Journal of Cybersecurity 7:1 (2021), S. 1–12.
Eichenhofer, Johannes: e-Privacy. Theorie und Dogmatik eines europäischen Privatheitsschutzes im Internet-Zeitalter, Tübingen 2021.
Eichensehr, Kristen E.: Giving Up On Cybersecurity, UCLA L. Rev. Discourse 64 (2016), S. 320–339.
–: Public-Private Cybersecurity, Tex. L. Rev. 95:3 (2016–2017), S. 467–538.
–: Decentralized Cyberattack Attribution, AJIL Unbound 113 (2019), S. 213–217.
–: The Law and Politics of Cyberattack Attribution, UCLA L. Rev. 67 (2020), S. 520–598.
Eifert, Martin: Grundversorgung mit Telekommunikationsleistungen im Gewährleistungsstaat, Baden-Baden 1998.

–: Electronic Government als gesamtstaatliche Organisationsaufgabe, ZG 2001, S. 115–129.
–: Regulierte Selbstregulierung und die lernende Verwaltung, DV Beiheft 4 (2001), S. 137–158.
–: Innovationen in und durch Netzwerkorganisationen: Relevanz, Regulierung und staatliche Einbindung, in: Martin Eifert/Wolfgang Hoffmann-Riem (Hrsg.), Innovation und rechtliche Regulierung. Schlüsselbegriffe und Anwendungsbeispiele rechtswissenschaftlicher Innovationsforschung, Baden-Baden 2002, S. 88–133.
–: Electronic Government. Das Recht der elektronischen Verwaltung, Baden-Baden 2006.
–: Informationelle Selbstbestimmung im Internet – das BVerfG und die Online-Durchsuchungen, NVwZ 2008, S. 521–523.
–: Das Verwaltungsrecht zwischen klassischem dogmatischen Verständnis und steuerungswissenschaftlichem Anspruch, in: VVDStRL 67 (2008), S. 286–329.
–: Innovationsfördernde Regulierung, in: Martin Eifert/Wolfgang Hoffmann-Riem (Hrsg.), Innovationsfördernde Regulierung, 2008, S. 9–17.
–: Zum Verhältnis von Dogmatik und pluralisierter Rechtswissenschaft, in: Gregor Kirchhof/Stefan Magen/Karsten Schneider (Hrsg.), Was weiß Dogmatik?, Tübingen 2012, S. 79–96.
–: „Sachverständiges Recht" am Beispiel des Technikrechts, in: Christian Bumke/Anne Röthel (Hrsg.), Privates Recht, Tübingen 2012, S. 79–91.
–: Elektronische Verwaltung – von der Verwaltungsreform zum Verwaltungsreformrecht, in: Peter Friedrich Bultmann/Klaus Joachim Grigoleit et al. (Hrsg.), Allgemeines Verwaltungsrecht. Festschrift für Ulrich Battis, München 2014, S. 421–435.
–: Behördliches Informationsmanagement als Gegenstand des Europäischen Verwaltungsrechts – Ansatz und Kritik des Buches VI des ReNEUAL-Musterentwurfs, in: Jens-Peter Schneider/Klaus Rennert/Nikolaus Marsch (Hrsg.), ReNEUAL Musterentwurf für ein EU-Verwaltungsverfahrensrecht – Tagungsband, München 2016, S. 214–230.
–: Autonomie und Sozialität: Schwierigkeiten rechtlicher Konzeptionalisierung ihres Wechselspiels am Beispiel der informationellen Selbstbestimmung, in: Christian Bumke/Anne Röthel (Hrsg.), Autonomie im Recht, 2017, S. 365–384.
–: Telekommunikationsrecht, in: Dirk Ehlers/Michael Fehling/Hermann Pünder (Hrsg.), Besonderes Verwaltungsrecht, Bd. 1, 4. Aufl. Heidelberg 2019, S. 993–1043.
–: Regulierungsstrategien, in: Andreas Voßkuhle/Martin Eifert/Christoph Möllers (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. 1, 3. Aufl. München 2022, § 19.
Einzinger, Kurt: Keine Cyber-Sicherheit ohne Datenschutz. Datenschutzrechtlichte Herausforderungen bei der Etablierung von nationalen CERTs, DuD 39 (2015), S. 723–729.
Einzinger, Kurt/Skopik, Florian: Über die datenschutzrechtliche Problematik in CERTs/CSIRTs-Netzwerken, DuD 41 (2017), S. 572–576.
Ellis, Ryan: Regulating Cybersecurity: Institutional Learning or a Lesson in Futility?, IEEE Security & Privacy 12:6 (2014), S. 48–54.
Engel, Christoph: Rationale Rechtspolitik und ihre Grenzen, JZ 60 (2005), S. 581–590.
Engel, Christoph/Halfmann, Jost/Schulte, Martin (Hrsg.): Wissen – Nichtwissen – Unsicheres Wissen, Baden-Baden 2002.
Engels, Jens Ivo: Relevante Beziehungen. Vom Nutzen des Kritikalitätskonzepts für Geisteswissenschaftler, in: Jens Ivo Engels/Alfred Nordmann (Hrsg.), Was heißt

Kritikalität? Zu einem Schlüsselbegriff der Debatte um Kritische Infrastrukturen, Bielefeld 2018, S. 17–46.

ENISA: Coordinated Vulnerability Disclosure Policies in the EU, 13.4.2022, https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu.

Ennuschat, Jörg: Behördliche Nachschau in Geschäftsräumen und die Unverletzlichkeit der Wohnung gem. Art. 13 GG, AöR 127 (2002), S. 252–290.

Epping, Volker/Hillgruber, Christian (Hrsg.): BeckOK Grundgesetz, 52. Ed., München 2022.

Ernestus, Walter: Bedarf die Anlage zu § 9 BDSG einer Modernisierung?, RDV 2000, S. 146–149.

Eskridge, William N.: The New Public Law Movement: Moderation as a Postmodern Cultural Form, Mich. L. Rev. 89 (1991), S. 707–791.

Esposito, Elena: The future of futures. The time of money in financing and society, Cheltenham 2011.

Europäische Kommission: Bericht über die Auswirkungen künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung, COM(2020) 64 final, 19.2.2020.

–: Mitteilung „Gestaltung der digitalen Zukunft Europas", COM(2020) 67 final, 19.2.2020.

–: EU-Strategie für eine Sicherheitsunion, COM(2020) 605 final, 24.7.2020.

–: Initiative zur Bekämpfung des sexuellen Missbrauchs von Kindern: Erkennung, Entfernung und Meldung illegaler Online-Inhalte, 2020, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12726-Bekampfung-des-sexuellen-Missbrauchs-von-Kindern-Erkennung-Entfernung-und-Meldung-illegaler-Online-Inhalte_de.

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, 13.9.2017.

–: Gemeinsame Mitteilung „Die Cybersicherheitsstrategie der EU für die digitale Dekade", JOIN(2020) 18 final, 16.12.2020.

Europäischer Rat: Eine neue strategische Agenda 2019–2024, Juni 2019, https://www.consilium.europa.eu/media/39963/a-new-strategic-agenda-2019–2024-de.pdf.

Europäischer Rechnungshof: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU, März 2019, https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_DE.pdf.

European Court of Human Rights: Guide on Article 8 of the European Convention on Human Rights, Stand 30.4.2022, www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf.

European Data Protection Board: Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, 12.3.2019, https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en.pdf.

–: Guidelines 01/2021 on Examples regarding Personal Data Breach Notification, Version 2.0, 14.12.2021, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_de.

European Parliament, Directorate-General for Internal Policies: Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, Study for the LIBE Committee, 2017, https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf.

Expertenkommission Forschung und Innovation: Gutachten zu Forschung, Innovation und technologischer Leistungsfähigkeit Deutschlands 2020, BT-Drs. 19/23070, 20.2. 2020.

Ewald, François: Der Vorsorgestaat, Frankfurt a. M. 1993.

Fagin, Matthew: Regulating Speech Across Borders: Technology vs. Values, Mich. Telecomm. & Tech. L. Rev. 9 (2003), S. 395–455.

Fahey, Elaine: The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security, European Journal of Risk Regulation 5:1 (2014), S. 46–60.

Febvre, Lucien/Martin, Henri-Jean: L'Apparition du livre, Paris 1958.

Federal Communications Commission (FCC): Notice of Inquiry, In the matter of Secure Internet Routing, FCC 22–18 v. 28.2.2022, https://www.fcc.gov/document/fcc-launches-inquiry-internet-routing-vulnerabilities.

Federrath, Hannes/Pfitzmann, Andreas: Datensicherheit, in: Martin Schulte/Rainer Schröder (Hrsg.), Handbuch des Technikrechts, 2011, S. 857–886.

Feeley, Matthew J.: EU Internet Regulation Policy. The Rise of Self-Regulation, Boston College Int'l & Comp. L. Rev. 22 (1999), S. 112–174.

Feiler, Lukas: Information Security Law in the EU and the U.S. A Risk-based Assessment of Regulatory Policies, Wien u. a. 2012.

Feintuck, Mike: Regulatory Rationales Beyond the Economic: In Search of the Public Interest, in: Robert Baldwin/Martin Cave/Martin Lodge (Hrsg.), The Oxford Handbook of Regulation, Oxford 2010, S. 39–63.

Feldstein, Steven: The Rise of Digital Repression. How Technology is Reshaping Power, Politics, and Resistance, Oxford 2021.

Felt, Ulrike/Fouché, Rayvon et al. (Hrsg.): The Handbook of Science and Technology Studies, 4. Aufl. Cambridge (Mass.) 2017.

Fickers, Andreas/Griset, Pascal: Communicating Europe. Technologies, Information, Events, London 2019.

Fidler, Bradley: Cybersecurity Governance. A Prehistory and its Implications, Digital Policy, Regulation and Governance 19:6 (2017), S. 449–465.

Fiedler, Herbert: Datenschutz und Gesellschaft, in: D. Siefkes (Hrsg.), Gesellschaft für Informatik – 4. Jahrestagung, Berlin u. a. 1975, S. 68–84.

Finnemore, Martha/Hollis, Duncan B.: Constructing Norms for Global Cybersecurity, AJIL 110 (2016), S. 425–479.

–: Beyond Naming and Shaming. Accusations and International Law in Cybersecurity, EJIL 31:3 (2020), S. 969–1003.

Fischer, Lars/Messerschmidt, Michel: Ohne Security keine Safety in Kritischen Infrastrukturen – Begriffliche Trennung und Zusammenführung, 4.5.2020, https://ag.kritis.info/wp-content/uploads/2020/05/AG_KRITIS-Ohne_Safety_keine_Security_in_KRITIS.pdf.

Fischer, Matthias: IT-Sicherheitsanforderungen an Kritische Infrastrukturen und digitale Dienste, in: Gerrit Hornung/Martin Schallbruch (Hrsg.), IT-Sicherheitsrecht, Baden-Baden 2021, § 13.

Fischer, Matthias/Kipker, Dennis-Kenji/Voskamp, Friederike: Internationaler Rahmen, in: Dennis-Kenji Kipker (Hrsg.), Cybersecurity, München 2020, Kap. 16.

Fischer, Robert/Halibozek, Edward/Walters, David: Introduction to Security, 10. Aufl. Kidlington 2018.

Fischer-Lescano, Andreas/Teubner, Gunther: Regime-Kollisionen, Frankfurt a. M. 2006.

–: Fragmentierung des Weltrechts. Vernetzung globaler Regimes statt etatistischer Rechtseinheit, in: Mathias Albert/Rudolf Stichweh (Hrsg.), Weltstaat und Weltstaatlichkeit: Beobachtungen globaler politischer Strukturbildung, Wiesbaden 2007, S. 37–61.
Flichy, Patrice: L'imaginaire d'internet, Paris 2001.
Floridi, Luciano (Hrsg.): The Onlife Manifesto. Being Human in a Hyperconnected Era, Cham u. a. 2015.
Folkers, Andreas: Das Sicherheitsdispositiv der Resilienz. Katastrophische Risiken und die Biopolitik vitaler Systeme, Frankfurt a. M. u. a. 2018.
–: Was ist kritisch an Kritischer Infrastruktur? Kriegswichtigkeit, Lebenswichtigkeit, Systemwichtigkeit und die Infrastrukturen der Kritik, in: Jens Ivo Engels/Alfred Nordmann (Hrsg.), Was heißt Kritikalität? Zu einem Schlüsselbegriff der Debatte um Kritische Infrastrukturen, Bielefeld 2018, S. 123–154.
–: Kritische Infrastruktur, Arch+ 2020, S. 102–109.
Ford, Richard T.: Against Cyberspace, in: Austin Sarat/Lawrence Douglas/Martha Merrill Umphry (Hrsg.), The Place of Law, Ann Arbor 2009, S. 147–180.
Forsthoff, Ernst: Der totale Staat, 1. Aufl. Hamburg 1933.
–: Lehrbuch des Verwaltungsrechts, Bd. 1, 1. Aufl. München 1950.
–: Der lästige Jurist, DÖV 1955, S. 648–650.
–: Der Jurist in der industriellen Gesellschaft, NJW 1960, S. 1273–1277.
–: Rechtsstaat im Wandel. Verfassungsrechtliche Abhandlungen 1950–1964, Stuttgart 1964.
–: Technisch bedingte Strukturwandlungen des modernen Staates, in: Hans Freyer/Johannes Chr. Papalekas/Georg Weippert (Hrsg.), Technik im technischen Zeitalter, Düsseldorf 1965, S. 211–231.
–: Technischer Prozess und politische Ordnung, Studium Generale 22 (1969), S. 849–856.
–: Von der sozialen zur technischen Realisation, Der Staat 9 (1970), S. 145–160.
–: Der Staat der Industriegesellschaft. Dargestellt am Beispiel der Bundesrepublik Deutschland, München 1971.
–: Lehrbuch des Verwaltungsrechts: Allgemeiner Teil, 10. Aufl. München 1973.
–: Technische Realisation und politische Ordnung, in: Oskar Schatz (Hrsg.), Auf dem Weg zur hörigen Gesellschaft?, Graz 1973, S. 183–198.
Foucault, Michel: Überwachen und Strafen. Die Geburt des Gefängnisses, Frankfurt a. M. 1976.
–: Dispositive der Macht. Michel Foucault über Sexualität, Wissen und Wahrheit, Berlin 1978.
–: Sicherheit, Territorium, Bevölkerung (Geschichte der Gouvernementalität I). Vorlesungen am Collège de France, 1977–1978, Frankfurt a. M. 2004.
Fox, Dirk: Computer Emergency Response Team (CERT), DuD 2002, S. 493.
Frank, Hans: Technik des Staates, Berlin u. a. 1942.
Frankenreiter, Jens: The Missing "California Effect" in Data Privacy Law, 15.9.2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3883728.
Franzius, Claudio: Technikermöglichungsrecht, DV 34 (2001), S. 487–516.
–: Gewährleistung im Recht, Tübingen 2009.
Frau, Robert: Der nachrichtendienstliche Zugriff auf Smarthome-Geräte – Grundrechtseingriffe in Alexa, Google Home & Co, GSZ 2020, S. 149–155.
Frauenrath, Ralf: Die Verfassungsschutzbehörden im Gefüge der deutschen Sicher-

heitsarchitektur, in: Hans-Jürgen Lange/Michaela Wendekamm (Hrsg.), Die Verwaltung der Sicherheit, Wiesbaden 2019, S. 155–163.
Freiling, Felix/Safferling, Christoph/Rückert, Christian: Quellen-TKÜ und Online-Durchsuchung als neue Maßnahmen für die Strafverfolgung: Rechtliche und technische Herausforderungen, JR 2018, S. 9–22.
Freimuth, Christoph: Die Gewährleistung der IT-Sicherheit Kritischer Infrastrukturen. Am Beispiel der Pflichten des IT-Sicherheitsgesetzes und der RL (EU) 2016/1148, Berlin 2018.
Fremuth, Michael Lysander: Wächst zusammen, was zusammengehört? Das Trennungsgebot zwischen Polizeibehörden und Nachrichtendiensten im Licht der Reform der deutschen Sicherheitsarchitektur, AöR 139 (2014), S. 32–79.
Frenz, Walter: Stärkerer staatlicher Schutz vor Cyberangriffen, DVBl. 2019, S. 1021–1025.
Frenzel, Eike M.: „Völlige Unabhängigkeit" im demokratischen Rechtsstaat. Der EuGH und die mitgliedstaatliche Verwaltungsorganisation, DÖV 2010, S. 925–931.
Frevel, Bernhard: Dilemmata des Sicherheitsdiskurses, in: Patrick E. Sensburg (Hrsg.), Sicherheit in einer digitalen Welt, Baden-Baden 2017, S. 167–180.
Freyer, Hans: Theorie des gegenwärtigen Zeitalters, Stuttgart 1955.
–: Über das Dominantwerden technischer Kategorien in der Lebenswelt der industriellen Gesellschaft (1960), in: ders.: Herrschaft, Planung und Technik, Weinheim 1987, S. 117–129.
Friauf, Karl-Heinrich (Begr.)/*Höfling, Wolfram/Augsberg, Steffen/Rixen, Stephan* (Hrsg.): Berliner Kommentar zum Grundgesetz, 6 Bde., Berlin 2000 ff.; Stand: Januar 2022
Friedel, Andreas: Blackbox Parlamentarisches Kontrollgremium des Bundestages. Defizite und Optimierungsstrategien bei der Kontrolle der Nachrichtendienste, Wiesbaden 2019.
Fritsch, Sebastian/Bremser, Dietmar: Europäische Zertifizierungsschemata – ein Interpretationsansatz, BSI Forum in der <kes> 2020, S. 44–49.
Gabel, Detlev/Heinrich, Tobias/Kiefner, Alexander (Hrsg.): Rechtshandbuch Cyber-Security, Frankfurt a. M. 2019
Gagliani, Gabriele: Cybersecurity, Technological Neutrality, and International Trade Law, Journal of International Economic Law 23:3 (2020), S. 723–745.
Gallaher, Michael P./Link, Albert N./Rowe, Brent R.: Cyber Security. Economic Strategies and Public Policy Alternatives, Cheltenham u. a. 2008.
Gallwas, Hans-Ullrich: Verfassungsrechtliche Grundlagen des Datenschutzes, Der Staat 18 (1979), S. 507–520.
Gander, Hans-Helmuth/Perron, Walter/Poscher, Ralf/Riescher, Gisela/Würtenberger, Thomas (Hrsg.): Resilienz in der offenen Gesellschaft, Baden-Baden 2012.
Ganz, Wilfried: My Home(office) is my castle – Zum Recht des Betriebsrats und der Berufsgenossenschaft, Arbeitsplätze zu besichtigen, ArbRAktuell 2018, S. 35–37.
Gärditz, Klaus F.: Europäisches Regulierungsverwaltungsrecht auf Abwegen, AöR 135 (2010), S. 251–288.
–: Infrastruktursicherung, in: Gregor Kirchhof/Stefan Korte/Stefan Magen (Hrsg.), Öffentliches Wettbewerbsrecht. Neuvermessung eines Rechtsgebiets, Heidelberg u. a. 2014, § 11.
–: Der digitalisierte Raum des Netzes als emergente Ordnung und die repräsentativ-demokratische Herrschaftsform, Der Staat 54 (2015), S. 113–139.

–: Sicherheitsrecht als Perspektive, GSZ 2017, S. 1–6.
–: Die „Neue Verwaltungsrechtswissenschaft" – Alter Wein in neuen Schläuchen?, DV Beiheft 4 (2017), S. 105–146.
–: Sicherheitsverfassungsrecht und technische Aufklärung durch Nachrichtendienste, EuGRZ 2018, S. 6–22.
–: Zentralisierung von Verfassungsschutzaufgaben und bundesstaatliche Kompetenzarchitektur, AöR 144 (2019), S. 81–132.
–: Bundesnachrichtendienst semper reformanda, DVBl. 2021, S. 905–914.
Gaudion, Amy: It's Time to Reform the U.S. Vulnerabilities Equities Process War Room, 2.9.2021, https://warroom.armywarcollege.edu/articles/vep/.
Gauger, Dörte: Produktsicherheit und staatliche Verantwortung. Das normative Leitbild des Produktsicherheitsgesetzes, Berlin 2015.
Gaycken, Sandro: Cybersecurity in der Wissensgesellschaft, in: Christopher Daase/Stefan Engbert/Julian Junk (Hrsg.), Verunsicherte Gesellschaft – Überforderter Staat, Frankfurt a. M. 2013, S. 109–132.
Gazeas, Nikolaos: Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, Berlin 2014.
GCHQ: The Equities Process, 29.11.2018, https://www.gchq.gov.uk/information/equities-process.
Gebhard, Angelina/Michalke, Reinhart: Der Zweck heiligt die Mittel nicht – Der EncroChat-Komplex und die Grenzen strafprozessualer Beweisverwertung, NJW 2022, S. 655–659.
Geer, Dan/Jardine, Eric/Leverett, Eireann: On market concentration and cybersecurity risk, Journal of Cyber Policy 5:1 (2020), S. 9–29.
Gehlen, Arnold: Die Seele im technischen Zeitalter. Sozialpsychologische Probleme in der industriellen Gesellschaft, Reinbek 1957.
Gehring, Thomas/Faude, Benjamin: The Dynamics of Regime Complexes: Microfoundations and Systemic Effects, Global Governance 19 (2013), S. 119–130.
Gehrmann, Mareike/Voigt, Paul: IT-Sicherheit – Kein Thema nur für Betreiber Kritischer Infrastrukturen, CR 2017, S. 93–99.
Gellert, Raphaël: The Risk-Based Approach to Data Protection, Oxford 2020.
Gentz, Manfred: Die Unverletzlichkeit der Wohnung. Artikel 13 des Grundgesetzes, Berlin 1968.
Georgieva, Ilina: The Unexpected Norm-Setters: Intelligence Agencies in Cyberspace, Contemporary Security Policy 41:1 (2020), S. 33–54.
Gercke, Marco: Der Entwurf für eine EU-Richtlinie über Netz- und Informationssicherheit (NIS), CR 2016, S. 28–30.
Gerhards, Julia: (Grund-)Recht auf Verschlüsselung?, Baden-Baden 2010.
Gerling, Rainer W./Gerling, Sebastian et al.: Stand der Technik bei Videokonferenzen – und die Interpretation der Aufsichtsbehörden, Datenschutz und Datensicherheit, DuD 44:11 (2020), S. 740–747.
Germano, Judith: Whitepaper Third-Party Cyber Risk & Corporate Responsibility, 2017, http://www.lawandsecurity.org/wp-content/uploads/2017/02/Germano.NYU_.ThirdPartyRiskWhitepaper.Feb2017.pdf.
Gersdorf, Hubertus/Paal, Boris (Hrsg.): BeckOK Informations- und Medienrecht, 37. Ed., München 2022.
Gilardi, Fabrizio: Independent Regulatory Agencies in Western Europe, Cheltenham 2008.

Gitter, Rotraud: Recht der IT-Sicherheitsbehörden, in: Gerrit Hornung/Martin Schallbruch (Hrsg.), IT-Sicherheitsrecht, Baden-Baden 2021, § 15.
Glaser, Markus A.: Internationale Verwaltungsbeziehungen, Tübingen 2010.
Glawe, Robert: Der Bundessicherheitsrat als sicherheits- und rüstungspolitisches Koordinationselement, DVBl. 2012, S. 329–336.
–: Der Geheimrat, NVwZ 2014, S. 1632–1636.
Glen, Carol: Internet Governance: Territorializing Cyberspace?, Politics & Policy 42 (2014), S. 635–657.
Global Encryption Coalition: Breaking Encrpytion Myths: What the European Commission's leaked report got wrong about online security, 2020, https://www.globalencryption.org/wp-content/uploads/2020/11/2020-Breaking-Encryption-Myths.pdf.
Godefroy, Bruno: Von der Krise zur Versicherheitlichung. Reinhart Kosellecks Krisentheorie in „unsicheren Zeiten", in: Karl-Rudolf Korte (Hrsg.), Politik in unsicheren Zeiten – Kriege, Krisen und neue Antagonismen, Baden-Baden 2016, S. 62–81.
Goel, Sanjay: How Improved Attribution in Cyber Warfare Can Help De-Escalate Cyber Arms Race, Connections 19:1 (2020), S. 87–95.
Goel, Sanjay/Nussbaum, Brian: Attribution Across Cyber Attack Types. Network Intrusions and Information Operations, IEEE Open Journal of the Communications Society 2 (2021), S. 1082–1093.
Goldmann, Matthias: Internationale öffentliche Gewalt. Handlungsformen internationaler Institutionen im Zeitalter der Globalisierung, Heidelberg u. a. 2015.
Goldsmith, Jack: The Internet and the Abiding Significance of Territorial Sovereignty, Indiana Journal of Global Legal Studies 5 (1998), S. 475–491.
Goldsmith, Jack/Wu, Tim: Who Controls the Internet? Illusions of a Borderless World, New York u. a. 2008.
Golla, Sebastian: IT-Sicherheit und Strafrecht – Neukalibrierung eines belasteten Verhältnisses JZ 76 (2021), S. 985–990.
Golla, Sebastian/Thess, Sebastian: Das Strafrecht als schlechtes Vorbild – Betrachtung zum „Dateneigentum" und § 202d StGB, in: Moritz Hennemann/Andreas Sattler (Hrsg.), Immaterialgüter und Digitalisierung: Junge Wissenschaft zum Gewerblichen Rechtsschutz, Urheber- und Medienrecht, Baden-Baden 2018, S. 9–26.
Golumbia, David: The cultural logic of computation, Cambridge (Mass.) 2009.
Gont, Fernando: IPv6 Security for IPv4 Engineers, 2019, https://www.internetsociety.org/wp-content/uploads/2019/03/deploy360-ipv6-security-v1.0.pdf.
Goodwin, Morag/Koops, Bert-Jaap/Leenes, Ronald (Hrsg.): Dimensions of Technology Regulation, Nijmegen 2010.
Gordon, Lawrence/Loeb, Martin: The Economics of Information Security Investment, ACM Transactions on Information and System Security 5 (2002), S. 438–457.
Götz, Volkmar: Innere Sicherheit, in: Josef Isensee/Paul Kirchhof (Hrsg.), Handbuch des Staatsrechts, Bd. IV, 3. Aufl. 2006, § 85.
Grabenwarter, Christoph/Pabel, Katharina: Europäische Menschenrechtskonvention, 7. Aufl. München 2021.
Grady, Mark F./Parisi, Francesco (Hrsg.): The Law and Economics of Cybersecurity, Cambridge 2005.
Gräfin von Wintzingerode, Christina/Müllmann, Dirk/Spiecker gen. Döhmann, Indra: Ein Netzwerk für Europas Cybersicherheit, NVwZ 2021, S. 690–695.
Graulich, Kurt: Das Handeln von Polizei- und Ordnungsbehörden zur Gefahrenabwehr, in: Lisken/Denninger, HdbPolR, 7. Aufl. 2021, Kap. E.

Grawert, Rolf: Technischer Fortschritt in staatlicher Verantwortung, in: Joseph Listl/Johannes Schambeck (Hrsg.), Demokratie in Anfechtung und Bewährung. Festschrift für Johannes Broermann, 1982, S. 457–490.

Greßmann, Michael: Nachrichtendienste und Strafverfolgung, in: Jan-Hendrik Dietrich/Sven-R. Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, Stuttgart 2017, Kap. IV § 3.

Grewal, David Singh: Network Power. The Social Dynamics of Globalization, New Haven 2008

Grieger, Ferdinand: Portscans im Lichte des Rechts: Eine straf- und zivilrechtliche Analyse, Int'l Cybersecurity L. Rev. 2021, S. 297–316.

Grigsby, Alex: The End of Cyber Norms, Survival 59:6 (2017), S. 109–122.

Grimm, Dieter: Die Zukunft der Verfassung, Frankfurt a. M. 1991.

– (Hrsg.): Rechtswissenschaften und Nachbarwissenschaften, Bd. 1 und 2, Frankfurt a. M. 1973.

Groom, Frank M./Groom, Kevin/Jones, Stephan S.: Network and Data Security for Non-Engineers, Portland 2016.

Gross, Michael L./Canetti, Daphna/Vashdi, Dana R.: Cyberterrorism: Its effects on psychological well-being, public confidence and political attitudes, Journal of Cybersecurity 3:1 (2017), S. 49–58.

Groß, Thomas: Verantwortung und Effizienz in der Mehrebenenverwaltung, in: VVDStRL 66 (2007), S. 152–215.

–: Ist die Wirtschaftskrise ein Katalysator für das Entstehen unabhängiger Behörden? Reformen der Bankenaufsicht im Vergleich, DV 47 (2014), S. 197–219.

–: Die Legitimation der polyzentralen EU-Verwaltung, Tübingen 2015.

Grüner, Anna-Maria: Biologische Katastrophen. Eine Herausforderung an den Rechtsstaat, Baden-Baden 2017.

Grunwald, Armin: Technik, in: Armin Grunwald (Hrsg.), Technikethik, Stuttgart u. a. 2013, S. 13–17.

Grunwald, Armin/Julliard, Yannick: Technik als Reflexionsbegriff. Überlegungen zur semantischen Struktur des Redens über Technik, Philosophie naturalis 2005, S. 127–157.

Guckelberger, Annette: Energie als kritische Infrastruktur, DVBl. 2015, S. 1213–1222.

–: Öffentliche Verwaltung im Zeitalter der Digitalisierung. Analysen und Strategien zur Verbesserung des E-Governments aus rechtlicher Sicht, Baden-Baden 2019.

Guitton, Clement: Inside the Enemy's Computer. Identifying Cyber Attackers, Oxford 2017.

Günther, Andreas: Produkthaftung für Informationsgüter. Verlagserzeugnisse, Software und Multimedia im deutschen und US-amerikanischen Produkthaftungsrecht, Köln 2001.

Günther, Klaus: Der Wandel der Staatsaufgaben und die Krise des regulativen Rechts, in: Dieter Grimm (Hrsg.), Wachsende Staatsaufgaben – sinkende Steuerungsfähigkeit des Rechts, Baden-Baden 1990, S. 50–69.

Gurlit, Elke: Das Informationsverwaltungsrecht im Spiegel der Rechtsprechung, DV 44 (2011), S. 75–103.

Gusy, Christoph: Techniksteuerung durch Recht: Aufgaben und Grenzen, in: Hartwig Donner (Hrsg.), Umweltschutz zwischen Staat und Markt: Moderne Konzeptionen im Umweltschutz, Baden-Baden 1989, S. 241–268.

–: Vom Polizeirecht zum Sicherheitsrecht, Staatswissenschaft und Staatspraxis 5 (1994), S. 187–210.

–: Probleme der Verrechtlichung technischer Standards, NVwZ 1995, S. 105–112.
–: Gewährleistung von Freiheit und Sicherheit im Lichte unterschiedlicher Staats- und Verfassungsverständnisse, in: VVDStRL 63 (2004), S. 151–190.
–: Vom neuen Sicherheitsbegriff zur neuen Sicherheitsarchitektur, VerwArch 2010, S. 309–333.
–: Resilient Societies. Staatliche Katastrophenschutzverantwortung und Selbsthilfefähigkeit der Gesellschaft, in: Dirk Heckmann/Ralf P. Schenke/Gernot Sydow (Hrsg.), Verfassungsstaatlichkeit im Wandel. Festschrift für Thomas Würtenberger, 2013, S. 995–1010.
–: Katastrophenschutzrecht. Zur Situation eines Rechtsgebietes im Wandel, in: Hans-Jürgen Lange/Christoph Gusy (Hrsg.), Kooperation im Katastrophen- und Bevölkerungsschutz, Wiesbaden 2015, S. 65–77.
–: Kontrolle der Nachrichtendienste, VerwArch 106 (2015), S. 437–458.
–: Ziele, Aufträge und Maßstäbe der Sicherheitsgewährleistung, in: Christoph Gusy/Dieter Kugelmann/Thomas Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, Berlin u. a. 2017, S. 55–86.
–: Nachrichtendienste in der sicherheitsbehördlichen Kooperation, in: Jan-Hendrik Dietrich/Sven-R. Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, Stuttgart 2017, Kap. IV § 2.
–: Organisation und Aufbau der deutschen Nachrichtendienste, in: Jan-Hendrik Dietrich/Sven-R. Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, Stuttgart 2017, Kap. IV § 1.
–: Sicherheitsrecht als Rechtsgebiet? – Ein Streit um Worte oder um die Sache und wenn ja, welche Sache?, in: Jan-Hendrik Dietrich/Klaus Ferdinand Gärditz (Hrsg.), Sicherheitsverfassung – Sicherheitsrecht. Festgabe für Kurt Graulich, Tübingen 2019, S. 9–24.
–: Katastrophenrecht, GSZ 2020, S. 101–108.
Gusy, Christoph/Eichenhofer, Johannes/Schulte, Laura: e-privacy. Von der Digitalisierung der Kommunikation zur Digitalisierung der Privatsphäre, JöR 64 (2016), S. 385–409.
Gusy, Christoph/Kapitza, Annika: Entparlamentarisierung der Sicherheitsgesetzgebung, in: Martin H. W. Möllers/Robert Chr. van Ooyen (Hrsg.), Jahrbuch Öffentliche Sicherheit 2014/2015, Frankfurt a. M. 2015, S. 367–374.
Haake, Camilla: Technik – Recht – Raum. Der Cyberspace als Rechtsraum besonderer Art. Zugleich eine Analyse des Verhältnisses von Völkerrecht und Technik, Tübingen 2022.
Haase, Adrian: Computerkriminalität im Europäischen Strafrecht. Kompetenzen, Harmonisierungen und Kooperationsperspektiven, Tübingen 2017.
Habermas, Jürgen: Technischer Fortschritt und soziale Lebenswelt (1965), in: ders., Technik und Wissenschaft als „Ideologie", Frankfurt a. M. 1968, S. 104–119.
–: Technik und Wissenschaft als „Ideologie" (1968), Frankfurt a. M. 1989.
–: Strukturwandel der Öffentlichkeit. Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft (1962), Frankfurt a. M. 1990.
Hacker, Philipp: Datenprivatrecht. Neue Technologien im Spannungsfeld von Datenschutzrecht und BGB, Tübingen 2020.
Hagemeier, Heike: Kryptografie – heute und zukünftig, DuD 43 (2019), S. 631–635.
Hakimi, Monica: Introduction to the Symposium on Cyber Attribution, AJIL Unbound 113 (2019), S. 189–190.

Haldenwang, Thomas/Postberg, Rupert: „Going Dark" – Sicherheit braucht eine wirksame Telekommunikationsüberwachung, in: Thomas Sauerland/Sabine Leppek (Hrsg.), Hochschule und Verwaltung zukunftsgerecht gestalten: Festschrift für Thomas Bönders zum Abschied aus dem Amt, 2019, S. 51–73.

Halfmann, Jost: Technikrecht aus der Sicht der Soziologie in: Martin Schulte/Rainer Schröder (Hrsg.), Handbuch des Technikrechts, 2. Aufl. Berlin u. a. 2011, S. 93–107.

Halliday, Terence C./Shaffer, Gregory (Hrsg.): Transnational Legal Orders, Cambridge 2015.

Hamdorf, Kai: Auskunftsrechte des Deutschen Bundestages gegenüber der Bundesregierung, in: Fabian Scheffczyk/Kathleen Wolter (Hrsg.), Linien der Rechtsprechung des Bundesverfassungsgerichts, Bd. 4, Berlin u. a. 2016, S. 467–490.

Hameiri, Shahar/Jones, Lee: Governing Borderless Threats. Non-Traditional Security and the Politics of State Transformation, 2015.

Handl, Günther/Zekoll, Joachim/Zumbansen, Peer (Hrsg.): Beyond Territoriality. Transnational Legal Authority in an Age of Globalization, Leiden u. a. 2012.

Hanks, Craig (Hrsg.): Technology and Values: Essential Readings, Malden (Mass.) 2010.

Hanschel, Dirk: Konfliktlösung im Bundesstaat. Die Lösung föderaler Kompetenz-, Finanz- und Territorialkonflikte in Deutschland, den USA und der Schweiz, Tübingen 2012.

Hansen, Lene: Reconstructing Desecuritisation: The Normative-Political in the Copenhagen School and Directions for How to Apply it, Review of International Studies 38:3 (2012), S. 525–546.

Hansen, Lene/Nissenbaum, Helen: Digital Disaster, Cyber Security, and the Copenhagen School, International Studies Quarterly 53 (2009), S. 1155–1175.

Hansen, Marit: Private Haushalte, in: Gerrit Hornung/Martin Schallbruch (Hrsg.), IT-Sicherheitsrecht, Baden-Baden 2021, § 26.

Hansson, Sven Ove: The Ethics of Technology. Methods and Approaches, London u. a. 2017.

Harrison Dinniss, Heather: Cyber Warfare and the Laws of War, Cambridge u. a. 2012.

Härtel, Ines: Das europäische Datenschutzgrundrecht in der digitalen „Infosphäre", in: Carsten Nowak/Carmen Thiele (Hrsg.), Effektivität des Grundrechtsschutzes in der Europäischen Union, Baden-Baden 2021, S. 103–138.

Hartmann, Christoph/Klindt, Thomas: Kritisches zum Kommissions-Entwurf für eine Produktsicherheits-VO, ZfPC 2022, S. 73–77.

Hathaway, Melissa: Connected Choices: How the Internet Is Challenging Sovereign Decisions, American Foreign Policy Interests 36 (2014), S. 300–313.

Hathaway, Oona A./Crootof, Rebecca et al.: The Law of Cyber-Attack, Calif. L. Rev. 100:4 (2012), S. 817–885.

Hauck, Pierre: Heimliche Strafverfolgung und Schutz der Privatheit. Eine vergleichende und interdisziplinäre Analyse des deutschen und englischen Rechts unter Berücksichtigung der Strafverfolgung in der Europäischen Union und im Völkerstrafrecht, Tübingen 2014.

Haunss, Sebastian/Hofmann, Jeanette: Entstehung von Politikfeldern – Bedingungen einer Anomalie, dms 8:1 (2015), S. 29–49.

Hauser, Markus: Das IT-Grundrecht. Schnittfelder und Auswirkungen, Berlin 2015.

Haverkamp, Rita/Kaufmann, Stefan/Zoche, Peter: Einführung, in: Peter Zoche/Stefan Kaufmann/Rita Haverkamp (Hrsg.), Zivile Sicherheit. Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken, Bielefeld 2011, S. 9–20.

Headrick, Daniel R.: Tools of Empire. Technology and European Imperialism in the Nineteenth Century, New York 1981.
–: Power over Peoples: Technology, Environments, and Western Imperialism, 1400 to the Present, Princeton 2010.
Healey, Jason: The U.S. Government and Zero-Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers, Journal of International Affairs 67:11 (2016), S. 1–20.
Heckmann, Dirk: Staatliche Schutz- und Förderpflichten zur Gewährleistung von IT-Sicherheit. Erste Folgerungen aus dem Urteil des Bundesverfassungsgerichts zur „Online-Durchsuchung", in: Helmut Rüßmann (Hrsg.), Festschrift für Gerhard Käfer, Saarbrücken 2009, S. 129–164.
–: Perspektiven des IT-Einsatzes in der öffentlichen Verwaltung, DV 46 (2013), S. 1–20.
– (Hrsg.), jurisPK-Internetrecht, 4. Aufl. 2014.
Heidegger, Martin: Die Frage nach der Technik (1953), in: ders., Vorträge und Aufsätze, Pfullingen 1954, S. 13–44.
–: Die Technik und die Kehre, Pfullingen 1962.
–: Nur noch ein Gott kann uns retten, in: Der Spiegel 30 H. 23 (1976), S. 193–219.
Heilmann, Wolfgang/Reusch, Günter: Datensicherheit und Datenschutz. Hilfen zur Bestimmung eines eigenen Standpunktes, Wiesbaden 1984.
Heinemann, Marcus: Grundrechtlicher Schutz informationstechnischer Systeme. Unter besonderer Berücksichtigung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Berlin 2015.
Hellgardt, Alexander: Regulierung und Privatrecht. Staatliche Verhaltenssteuerung mittels Privatrecht und ihre Bedeutung für Rechtswissenschaft, Gesetzgebung und Rechtsanwendung, Tübingen 2016.
–: Wer hat Angst vor der unmittelbaren Drittwirkung? – Die Konsequenz der Stadionverbot-Entscheidung des BVerfG für die deutsche Grundrechtsdogmatik, JZ 73 (2018), S. 901–910.
Henriksen, Anders: The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace, Journal of Cybersecurity 5:1 (2019), S. 1–9.
Herdegen, Matthias/Masing, Johannes/Poscher, Ralf/Gärditz, Klaus Ferdinand (Hrsg.): Handbuch des Verfassungsrechts, München 2021.
Herf, Jeffrey: Der nationalsozialistische Technikdiskurs, in: Wolfgang Emmerich/Carl Wege (Hrsg.), Der Technikdiskurs in der Hitler-Stalin-Ära, Stuttgart u. a. 1995, S. 72–93.
Hermes, Georg: Das Grundrecht auf Schutz von Leben und Gesundheit. Schutzpflicht und Schutzanspruch aus Art. 2 Abs. 2 Satz 1 GG, Heidelberg 1987.
–: Staatliche Infrastrukturverantwortung. Rechtliche Grundstrukturen netzgebundener Transport- und Übertragungssysteme zwischen Daseinsvorsorge und Wettbewerbsregulierung am Beispiel der leitungsgebundenen Energieversorgung in Europa, Tübingen 1998.
–: Abhängige und unabhängige Verwaltungsbehörden – ein Überblick über die Bundesverwaltung, in: Johannes Masing/Gérard Marcou (Hrsg.), Unabhängige Regulierungsbehörden. Organisationsrechtliche Herausforderungen in Frankreich und Deutschland, Tübingen 2010, S. 53–86.
Hermstrüwer, Yoan: Informationelle Selbstgefährdung. Zur rechtsfunktionalen, spieltheoretischen und empirischen Rationalität der datenschutzrechtlichen Einwilligung und des Rechts auf informationelle Selbstbestimmung, Tübingen 2016.
Herpig, Sven: Government Hacking: Computer Security vs. Investigative Powers, Juni

2017, https://www.stiftung-nv.de/sites/default/files/snv_tcf_government_hacking-problem_analysis_0.pdf.
–: Schwachstellen-Management für mehr Sicherheit. Wie der Staat den Umgang mit Zero-Day-Schwachstellen regeln sollte, 27.8.2018, https://www.stiftung-nv.de/sites/default/files/vorschlag.schwachstellenmanagement.pdf.
Herpig, Sven/Bredenbrock, Clara: Cybersicherheitspolitik in Deutschland – Akteure, Aufgaben und Zuständigkeiten. Im Fokus: Das Cyber-Abwehrzentrum, April 2019, https://www.stiftung-nv.de/sites/default/files/cybersicherheitspolitik_in_deutschland.pdf.
Herpig, Sven/Heumann, Stefan: The Encryption Debate in Germany, 2019, https://carnegieendowment.org/files/WP_The_Encryption_Debate_in_Germany_WEB.pdf.
Herpig, Sven/Kipker, Dennis-Kenji: Emotet-Takedown Der Zweck heiligt nicht die Mittel, Netzpolitik.org v. 18.2.2021, https://netzpolitik.org/2021/emotet-takedown-der-zweck-heiligt-nicht-die-mittel/.
Herpig, Sven/Rupp, Christina: Deutschlands staatliche Cybersicherheitsarchitektur, 8. Aufl. April 2022, https://www.stiftung-nv.de/sites/default/files/cybersicherheitsarchitektur_achteauflage0422.pdf.
Herpig, Sven/Schuetze, Julia: The Encryption Debate in Germany: Update, 2021, https://carnegieendowment.org/files/202104-Germany_Country_Brief.pdf.
Herr, Trey/Schneier, Bruce/Morris, Christopher: Taking Stock: Estimating Vulnerability Rediscovery, Revised Version: October 2017, https://ssrn.com/abstract=2928758.
Herrera, Geoffrey Lucas: Technology and International Transformation. The Railroad, the Atom Bomb, and the Politics of Technological Change, New York 2006.
Herzog, Roman: Evangelisches Staatslexikon, in: Hermann Kunst (Hrsg.), Der Mensch des technischen Zeitalters in Recht und Theologie, 1966, S. XXI-XLVI.
Hesse, Hans A.: Der Schutzstaat – Rechtssoziologische Skizzen in dunkler Zeit, Baden-Baden 1994.
Hesse, Konrad: Die normative Kraft der Verfassung, Tübingen 1959.
–: Der unitarische Bundesstaat, Karlsruhe 1962.
–: Aspekte des kooperativen Föderalismus in der Bundesrepublik, in: Theo Ritterspach/Willi Geiger (Hrsg.), FS für Gebhard Müller, Tübingen 1970, S. 141–160.
Hessel, Stefan/Potel, Karin: Update qua Gesetz – Aktualisierungspflicht nach § 327f BGB in der Praxis, RDi 2022, S. 25–31.
Hessel, Stefan/Schneider, Moritz: Inspector Gadget ermittelt? Zur Unzulässigkeit von Produktwarnungen durch die Datenschutzaufsichtsbehörden, K&R 2022, S. 82–86.
Heußner, Kristina: Informationssysteme im europäischen Verwaltungsverbund, Tübingen 2007.
Heyen, Erk Volkmar (Hrsg.): Technikentwicklung zwischen Wirtschaft und Verwaltung in Großbritannien und Deutschland, Baden-Baden 2008.
Hilbert, Patrick: Systemdenken in Verwaltungsrecht und Verwaltungsrechtswissenschaft, Tübingen 2015.
Hildebrandt, Mireille: Smart Technologies and the End(s) of Law, Cheltenham 2016.
Hill, Hermann: Wandel von Verwaltungskultur und Kompetenzen im digitalen Zeitalter, in: Hermann Hill (Hrsg.), Transparenz, Partizipation, Kollaboration. Die digitale Verwaltung neu denken, Baden-Baden 2014, S. 125–148.

Hill, Hermann/Hof, Hagen (Hrsg.): Wirkungsforschung zum Recht II: Verwaltung als Adressat und Akteur, Baden-Baden 2000.
Hobe, Stephan: Cyberspace – der virtuelle Raum, in: Josef Isensee/Paul Kirchhof (Hrsg.), Handbuch des Staatsrechts, Bd. XI, 3. Aufl. 2013, § 231.
Hof, Hagen/Lübbe-Wolff, Gertrude (Hrsg.): Wirkungsforschung zum Recht I: Wirkungen und Erfolgsbedingungen von Gesetzen, Baden-Baden 1999.
Hof, Hagen/Schulte, Martin (Hrsg.): Wirkungsforschung zum Recht III: Folgen von Gerichtsentscheidungen, Baden-Baden 2001.
Hoffmann-Riem, Wolfgang: Reform des Allgemeinen Verwaltungsrechts als Aufgabe, AöR 115 (1990), S. 400–447.
–: Öffentliches Recht und Privatrecht als wechselseitige Auffangordnungen – Systematisierung und Entwicklungsperspektiven, in: Wolfgang Hoffmann-Riem/Eberhard Schmidt-Aßmann (Hrsg.), Öffentliches Recht und Privatrecht als wechselseitige Auffangordnungen Baden-Baden 1996, S. 261–336.
–: Innovationen durch Recht und im Recht, in: Martin Schulte (Hrsg.), Technische Innovation und Recht. Antrieb oder Hemmnis?, Heidelberg 1997, S. 3–32.
–: Informationelle Selbstbestimmung in der Informationsgesellschaft. Auf dem Wege zu einem neuen Konzept des Datenschutzes, AöR 123 (1998), S. 513–540.
–: Sozialwissenschaften im Verwaltungsrecht: Kommunikation in einer multidisziplinären Scientific Community, DV Beiheft 2 (1999), S. 83–102.
–: Verwaltungsrecht in der Informationsgesellschaft – Einleitende Problemskizze, in: Wolfgang Hoffmann-Riem/Eberhard Schmidt-Aßmann (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, 2000, S. 9–66.
–: Methoden einer anwendungsorientierten Verwaltungsrechtswissenschaft, in: Eberhard Schmidt-Aßmann/Wolfgang Hoffmann-Riem (Hrsg.), Methoden der Verwaltungsrechtswissenschaft, Baden-Baden 2004, S. 9–72.
–: Innovationsoffenheit und Innovationsverantwortung durch Recht, AöR 131 (2006), S. 255–277.
–: Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 63 (2008), S. 1009–1022.
–: Grundrechts- und Funktionsschutz für elektronisch vernetzte Kommunikation, AöR 134:4 (2009), S. 513–541.
–: Rechtsformen, Handlungsformen, Bewirkungsformen, in: Wolfgang Hoffmann-Riem/Eberhard Schmidt-Aßmann/Andreas Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. 2, 2. Aufl. München 2012, § 33.
–: Freiheitsschutz in den globalen Kommunikationsinfrastrukturen, JZ 69 (2014), S. 53–63.
–: Regulierungswissen in der Regulierung, in: Alfons Bora/Anna Henkel/Carsten Reinhard (Hrsg.), Wissensregulierung und Regulierungswissen, Weilerswist 2014, S. 135–156.
–: Innovation und Recht – Recht und Innovation, Tübingen 2016.
–: Der Staat als Garant von Freiheit und Sicherheit, in: Hans-J. Papier/Ursula Münch/Gero Kellermann (Hrsg.), Freiheit und Sicherheit – Verfassungspolitik, Grundrechtsschutz, Sicherheitsgesetze, Baden-Baden 2016, S. 19–38.
–: Schutz der natürlichen und der gesellschaftlichen Umwelt – zum Vergleich von Umweltrecht und Digitalisierungsrecht, EurUP 16 (2018), S. 2–11.
– (Hrsg.): Sozialwissenschaften im öffentlichen Recht, Neuwied 1981.
Hoffmann-Riem, Wolfgang/Pilniok, Arne: Die Eigenständigkeit der Verwaltung, in:

Andreas Voßkuhle/Martin Eifert/Christoph Möllers (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. 1, 3. Aufl. München 2022, § 12.
Hoffmann-Riem, Wolfgang/Schneider, Jens-Peter (Hrsg.): Rechtswissenschaftliche Innovationsforschung, Baden-Baden 1998.
Hofmann, Hans: Die bundesstaatliche Architektur der inneren Sicherheit: Status und Reformoptionen im deutschen Mehrebenensystem der Sicherheitsarchitektur, in: Jahrbuch des Föderalismus 2018, S. 51–67.
Hofmann, Henning: Predictive Policing. Methodologie, Systematisierung und rechtliche Würdigung der algorithmusbasierten Kriminalitätsprognose durch die Polizeibehörden, Berlin 2020.
Höhn, Reinhard: Die Wandlung im staatsrechtlichen Denken, Hamburg 1934.
Hollis, Duncan B.: An e-SOS for Cyberspace, Harv. Int'l L. J. 52 (2011), S. 373–432.
Hollis, Duncan B./Waxman, Matthew C.: Promoting International Cybersecurity Cooperation. Lessons from the Proliferation Security Initiative, Temple Int'l & Comp. L. J. 32 (2018), S. 147–160.
Horn, Hans-Detlef: Schutz der Privatsphäre, in: Josef Isensee/Paul Kirchhof (Hrsg.), Handbuch des Staatsrechts, Bd. VII, 3. Aufl. 2009, § 149.
Hörnle, Julia: Juggling More Than Three Balls at Once: Multilevel Jurisdictional Challenges in EU Data Protection Regulation, Int'l J. L. & Info. Tech. 27:2 (2019), S. 142–170.
Hornung, Gerrit: Ein neues Grundrecht. Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme", CR 2008, S. 299–306.
–: Neue Pflichten für Betreiber kritischer Infrastrukturen. Das IT-Sicherheitsgesetz des Bundes, NJW 2015, S. 3334–3340.
–: Grundrechtsinnovationen, Tübingen 2015.
–: Das IT-Sicherheitsgesetz 2.0: Kompetenzaufwuchs des BSI und neue Pflichten für Unternehmen, NJW 2021, S. 1985–1991.
Hornung, Gerrit/Schallbruch, Martin (Hrsg.): IT-Sicherheitsrecht. Praxishandbuch, Baden-Baden 2021.
Hornung, Gerrit/Schomberg, Sabrina: Datensouveränität im Spannungsfeld zwischen Datenschutz und Datennutzung: das Beispiel des Data Governance Acts, CR 2022, S. 508–516.
Horst, Johan: Transnationale Rechtserzeugung. Elemente einer normativen Theorie der Lex Financiaria, Tübingen 2019.
Horwitz, Morton J.: The Transformation of American Law 1870–1960. The Crisis of Legal Orthodoxy, New York u. a. 1992.
Hösl, Maximilian/Irgmaier, Florian/Kniep, Ronja: Diskurse der Digitalisierung und organisationaler Wandel in Ministerien, in: Tanja Klenk/Frank Nullmeier/Göttrik Wewer (Hrsg.), Handbuch Digitalisierung in Staat und Verwaltung, Wiesbaden 2020, S. 383–394.
Hubbard, Douglas W./Seiersen, Richard: How to Measure Anything in Cybersecurity Risk, Hoboken 2016.
Huber, Hans: Das Recht im technischen Zeitalter, Bern 1960.
Huber, Peter M.: Der ungeliebte Bundesstaat, NVwZ 2019, S. 665–672.
Huber, Peter M./Voßkuhle, Andreas (Hrsg.): Kommentar zum Grundgesetz, 3 Bde., 8. Aufl. München 2023.
Hubig, Christoph: Mittel, Bielefeld 2002.
–: Die Kunst des Möglichen II, Bielefeld 2007.

–: Technik als Medium, in: Armin Grunwald (Hrsg.), Handbuch Technikethik, Stuttgart u. a. 2013, S. 118–123.
Hubig, Christoph/Huning, Alois/Ropohl, Günter (Hrsg.): Nachdenken über Technik. Die Klassiker der Technikphilosophie und neuere Entwicklungen, 3. Aufl. 2013.
Hufen, Friedhelm: Berufsfreiheit – Erinnerung an ein Grundrecht, NJW 1994, S. 2913–2922.
Hughes, Thomas P.: Networks of Power: Electrification in Western Society, 1880–1930, Baltimore, 1983.
Hunter, Dan: Cyberspace as Place and the Tragedy of the Digital Anticommons, Calif. L. Rev. 91 (2003), S. 439–520.
Hurel, Louise Marie/Lobato, Luisa Cruz: Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs, Journal of Cyber Policy 3:1 (2018), S. 61–76.
Hurni, Pascal: Cybernetics, German Public Administration and the Reframing of the Public Servant in the Neo-Verwaltungswissenschaft, in: Fritz Sager/Patrick Overeem (Hrsg.), The European Public Servant, 2015, S. 175–198.
ICANN: Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends, 1.10.2016, https://www.icann.org/news/announcement-2016–10–01-en.
IETF: Internet Security Glossary RFC 2828 (May 2000), https://datatracker.ietf.org/doc/html/rfc2828.
–: Security Assessment of the Internet Protocol Version 4, RFC 6274, July 2011, https://tools.ietf.org/html/rfc6274.
Ihde, Don: Technics and Praxis, Dordrecht 1979.
International Law Commission: Fragmentation of International Law: Difficulties arising from the Diversification and Expansion of International Law, A/CN.4/L.682, 13.4.2006.
Iorio, Marco: Regel und Grund. Eine philosophische Abhandlung, Berlin u. a. 2012.
Iorio, Marco/Reisenzein, Rainer (Hrsg.): Regel, Norm, Gesetz. Eine interdisziplinäre Bestandsaufnahme, Frankfurt a. M. 2010.
Ipsen, Jörn: Die Bewältigung der wissenschaftlichen und technischen Entwicklungen durch das Verwaltungsrecht, in: VVDStRL 48 (1990), S. 187–206.
Isensee, Josef: Das Grundrecht auf Sicherheit. Zu den Schutzpflichten des freiheitlichen Verfassungsstaates, Berlin u. a. 1983.
–: Staatsaufgaben, in: Josef Isensee/Paul Kirchhof (Hrsg.), Handbuch des Staatsrechts, Bd. IV, 3. Aufl. 2006, § 73.
–: Idee und Gestalt des Föderalismus im Grundgesetz, in: Josef Isensee/Paul Kirchhof (Hrsg.), Handbuch des Staatrechts, Bd. VI, 3. Aufl. 2008, § 126.
–: Grundrechtsvoraussetzungen und Verfassungserwartungen, in: Josef Isensee/Paul Kirchhof (Hrsg.), Handbuch des Staatsrechts, Bd. IX, 3. Aufl. 2011, § 190.
–: Das Grundrecht als Abwehrrecht und als staatliche Schutzpflicht, in: Josef Isensee/Paul Kirchhof (Hrsg.), Handbuch des Staatsrechts, Bd. IX, 3. Aufl. 2011, § 191.
–: Sicherheit als Voraussetzung und als Thema einer freiheitlichen Verfassung, in: Michael Anderheiden/Rainer Keil et al. (Hrsg.), Verfassungsvoraussetzungen. Gedächtnisschrift für Winfried Brugger, Tübingen 2013, S. 499–521.
ISO: Information technology – Security techniques – Vulnerability handling processes, ISO/IEC 30111:2013, November 2013.
IT-Planungsrat: Leitlinie für die Informationssicherheit in der öffentlichen Verwal-

tung, 6.12.2018, https://www.IT-planungsrat.de/fileadmin/beschluesse/2019/Beschluss 2019–04_TOP12_Anlage_Leitlinie.pdf.
–: Verbindliches Meldeverfahren zum Informationsaustausch über IT-Sicherheitsvorfälle im VerwaltungsCERT-Verbund (Meldestandard), Beschluss 2017/35 v. 5.10. 2017, https://www.IT-planungsrat.de/fileadmin/beschluesse/2017/Beschluss2017–35_Meldestandards_Anlage1.pdf.
ITU: Security Architecture for Open Systems Interconnection for CCITT Applications. Recommendation X.800, 1991.
Jaeckel, Liv: Gefahrenabwehrrecht und Risikodogmatik. Moderne Technologien im Spiegel des Verwaltungsrechts, Tübingen 2010.
Jandt, Silke: IT-Sicherheit als Mittel und als Bedrohung des Datenschutzes, in: Gerrit Hornung/Martin Schallbruch (Hrsg.), IT-Sicherheitsrecht, Baden-Baden 2021, § 17.
–: Technikadäquate Grundrechtsentwicklung. Verfassungsrechtliche Steuerung technischer Innovationen am Beispiel des Internet, Kassel 2022.
Janich, Peter: Logisch-pragmatische Propädeutik, Weilerswist 2001.
Jarass, Hans D.: Politik und Bürokratie als Element der Gewaltenteilung, München 1975.
–: Charta der Grundrechte der Europäischen Union, 4. Aufl. München 2021.
Jellinghaus, Lorenz: Zwischen Daseinsvorsorge und Infrastruktur. Zum Funktionswandel von Verwaltungswissenschaften und Verwaltungsrecht in der zweiten Hälfte des 19. Jahrhunderts, Frankfurt a. M. 2006.
Jervis, Robert: The Meaning of the Nuclear Revolution, 1989.
Jessup, Philip C.: Transnational Law, New Haven 1956.
Jestaedt, Matthias: Demokratieprinzip und Kondominialverwaltung. Entscheidungsteilhabe Privater an der öffentlichen Verwaltung auf dem Prüfstand des Verfassungsprinzips Demokratie, Berlin 1993.
–: Bundesstaat als Verfassungsprinzip, in: Josef Isensee/Paul Kirchhof (Hrsg.), Handbuch des Staatsrechts, Bd. II, 3. Aufl. 2004, § 29.
–: Perspektiven der Rechtswissenschaftstheorie, in: Matthias Jestaedt/Oliver Lepsius (Hrsg.), Rechtswissenschaftstheorie, Tübingen 2008, S. 185–205.
Joe: Mind the (Air) Gap, 31.5.2021, https://pylos.co/2021/05/13/mind-the-air-gap/.
Joerges, Bernward: Soziologie und Maschinerie – Vorschläge zu einer »realistischen« Techniksoziologie, in: Peter Weingart (Hrsg.), Technik als sozialer Prozeß, Frankfurt a. M. 1989, S. 44–89.
–: Do Politics Have Artefacts?, Social Studies of Science 29 (1999), S. 411–431.
Joerges, Bernward/Nowotny, Helga (Hrsg.): Social Studies of Science and Technology: Looking Back, Ahead, Dordrecht 2003.
Joggerst, Laura/Wendt, Janine: Die Weiterentwicklung der Produkthaftungsrichtlinie, InTeR 2021, S. 13–17.
Johnson, David R./Post, David: Law and Borders – The Rise of Law in Cyberspace, Stan. L. Rev. 48 (1996), S. 1367–1402.
Jonas, Hans: Technology and Responsibility. Reflections on the New Tasks of Ethics, Social Research 40 (1973), S. 31–54.
–: Das Prinzip Verantwortung. Versuch einer Ethik für die technologische Zivilisation, Frankfurt a. M. 1979.
Jones, Steven: Against Technology. From the Luddites to Neo-Luddism, London 2006.
Joyce, Rob: Improving and Making the Vulnerability Equities Process Transparent is

the Right Thing to Do, 15.11.2017, https://trumpwhitehouse.archives.gov/articles/improving-making-vulnerability-equities-process-transparent-right-thing/.
Jünger, Friedrich Georg: Die Perfektion der Technik, Frankfurt a. M. 1939.
Jurčys, Paulius/Kjaer, Poul F./Yatsunami, Ren (Hrsg.): Regulatory Hybridization in the Transnational Sphere, Leiden u. a. 2013.
Kahl, Arno: Entterritorialisierung im Wirtschaftsrecht und im Kommunikationsrecht, in: VVDStRL 76 (2017), S. 343–390.
Kahl, Wolfgang: Über einige Pfade und Tendenzen in Verwaltungsrecht und Verwaltungsrechtswissenschaft – ein Zwischenbericht, DV 42 (2009), S. 463–500.
–: Europäische Behördenkooperationen – Typen und Formen von Verbundsystemen und Netzwerkstrukturen, in: Michael Holoubek (Hrsg.), Verfahren der Zusammenarbeit von Verwaltungsbehörden in Europa, Wien 2012, S. 15–46.
–: Kodifizierung des Verwaltungsverfahrensrechts in Deutschland und in der EU, JuS 2018, S. 1025–1033.
–: Kontrolle der Verwaltung und des Verwaltungshandelns, in: Andreas Voßkuhle/Martin Eifert/Christoph Möllers (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. 2, 3. Aufl. München 2022, § 45.
Kahl, Wolfgang/Ludwig, Markus (Hrsg.): Handbuch des Verwaltungsrechts, Heidelberg 2021 ff.
Kahl, Wolfgang/Waldhoff, Christian/Walter, Christian (Hrsg.): Bonner Kommentar zum Grundgesetz, Heidelberg 1989–; Stand: 215. EL Juni 2022.
Kaiser, Anna-Bettina: Die Kommunikation der Verwaltung. Diskurse zu den Kommunikationsbeziehungen zwischen staatlicher Verwaltung und Privaten in der Verwaltungsrechtswissenschaft der Bundesrepublik Deutschland, Baden-Baden 2009.
–: Multidisziplinäre Begriffsverwendungen, in: Ino Augsberg (Hrsg.), Extrajuridisches Wissen im Verwaltungsrecht. Analysen und Perspektiven, Tübingen 2013, S. 99–119.
–: Ausnahmeverfassungsrecht, Tübingen 2020.
Kamlah, Ruprecht: Right of Privacy. Das allgemeine Persönlichkeitsrecht in amerikanischer Sicht unter Berücksichtigung neuer technologischer Entwicklungen, Köln 1969.
–: Datenüberwachung und Bundesverfassungsgericht, DÖV 1970, S. 361–364.
Kapitza, Annika: Entparlamentarisierung der Sicherheitsgesetzgebung. Eine Untersuchung am Beispiel der Telekommunikationsüberwachung, Berlin 2015.
Karpen, Ulrich/Hof, Hagen (Hrsg.): Wirkungsforschung zum Recht IV: Möglichkeiten einer Institutionalisierung der Wirkungskontrolle von Gesetzen, Baden-Baden 2003.
Kaspersky Lab: Equation Group: The Crown Creator of Cyber-Espionage, 16.2.2015, www.kaspersky.co.in/about/news/virus/2015/equation-group-the-crown-creator-of-cyber-espionage.
Katagiri, Nori: Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks, Journal of Cybersecurity 7:1 (2021), S. 1–9.
Katsarov, Ivaylo Nikolaev: Sicherheitsgesetzgebung zwischen Legislative und Exekutive. Zur Funktionsweise der Gewaltengliederung am Beispiel der Einführung der polizeilichen Videoüberwachung an Kriminalitätsschwerpunkten in Nordrhein-Westfalen, Hessen und Brandenburg, Frankfurt a. M. 2014.
Katzenstein, Peter J.: Introduction: Alternative Perspectives on National Security, in: Peter J. Katzenstein (Hrsg.), The Culture Of National Security: Norms And Identity In World Politics, 1996, S. 1–31.

Kaufhold, Ann-Katrin: Systemaufsicht: Anforderungen an die Ausgestaltung einer Aufsicht zur Abwehr systemischer Risiken entwickelt am Beispiel der Finanzaufsicht, Tübingen 2016.

Kaufhold, Ann-Katrin/Langenbucher, Katja et al.: BaFin (in)dependence – A reform proposal, March 2021, https://safe-frankfurt.de/de/publikationen/details/publicationname/bafin-independence-a-reform-proposal.html.

Kaufmann, Stefan: Zivile Sicherheit: Vom Aufstieg eines Topos, in: Leon Hempel/Susanne Krasmann/Ulrich Bröckling (Hrsg.), Sichtbarkeitsregime. Überwachung, Sicherheit und Privatheit im 21. Jahrhundert, Wiesbaden 2011, S. 101–122.

–: Das Themenfeld „Zivile Sicherheit", in: Christoph Gusy/Dieter Kugelmann/Thomas Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, Berlin u. a. 2017, S. 3–22.

Kelemen, R. Daniel: The Dangers of Constitutional Pluralism, in: Gareth Davies/Matej Avbelj (Hrsg.), Research Handbook on Legal Pluralism and EU Law, Cheltenham, UK 2018, S. 392–404.

Kello, Lucas: The Virtual Weapon and International Order, New Haven 2017.

–: Cyber Defence, in: Hugo Meijer/Marco Wyss (Hrsg.), The Handbook of European Defence Policies and Armed Forces, Oxford 2018, S. 658–674.

–: Cyber Threats, in: Thomas G. Weiss/Sam Daws (Hrsg.), The Oxford Handbook on the United Nations, 2. Aufl. Oxford 2018, S. 528–537.

Kempen, Bernhard: Staat und Raum, Paderborn 2014.

Kempny, Simon: Verwaltungskontrolle. Zur Systematisierung der Mittel zur Sicherung administrativer Rationalität unter besonderer Berücksichtigung der Gerichte und der Rechnungshöfe, Tübingen 2017.

Keohane, Robert O./Victor, David G.: The Regime Complex for Climate Change, Perspectives on Politics 9 (2011), S. 7–23.

Kern, Eduard: Schutz des Lebens, der Freiheit und des Heims, in: Franz L. Neumann/Hans Carl Nipperdey/Ulrich Scheuner (Hrsg.), Die Grundrechte. Handbuch der Theorie und Praxis der Grundrechte, Bd. II, Berlin 1954, S. 51–109.

Kesan, Jay P./Hayes, Carol M.: Bugs in the Market: Creating a Legitimate, Transparent, and Vendor-Focused Market for Software Vulnerabilities, Arizona L. Rev. 58:3 (2016), S. 753–830.

Kesan, Jay P./Shah, Rajiv C.: Shaping Code, Harv. J. L. & Tech. 18 (2005), S. 319–399.

Kettemann, Matthias: Das Internet als internationales Schutzgut: Entwicklungsperspektiven des Internetvölkerrechts anlässlich des Arabischen Frühlings, ZaöRV 72 (2012), S. 469–482.

–: "This is not a drill": International law and protection of cybersecurity, in: Ben Wagner/Matthias Kettemann/Kilian Vieth (Hrsg.), Research Handbook on Human Rights and Digital Technology, Cheltenham 2019, S. 113–128.

–: The Normative Order of the Internet: A Theory of Rule and Regulation Online, Oxford 2020.

Kettemann, Matthias/Kunz, Raffaela/Golia, Angelo: Introduction, ZaöRV 81 (2021), S. 597–599.

Kibler, Cornelia: Datenschutzaufsicht im europäischen Verbund. Unabhängigkeit, Effektivität, Rechtsschutz und Legitimation, Tübingen 2021.

Kidwell, Peggy Aldrich: The Role of Governments in the Spread of Novel Computing Devices in the Nineteenth and Early Twentieth Century United States, IEEEA 41:1 (2019), S. 7–19.

Kießling, Andrea: Die aktionelle Maßnahme im Vorfeld – Voraussetzungen und Grenzen im Lichte aktueller Gesetzesänderungen, in: Andreas Kulick/Michael Goldhammer (Hrsg.), Der Terrorist als Feind? Personalisierung im Polizei- und Völkerrecht, Tübingen 2020, S. 261–283.
Kilovaty, Ido: An Extraterritorial Human Right to Cybersecurity, Notre Dame J. Int'l & Comp. Law 10 (2020), S. 35–55.
Kingdon, John W.: Agendas, Alternatives, and Public Policies, 2. Aufl. New York u. a. 1995.
Kingreen, Thorsten/Kühling, Jürgen: Der überspannte Parlamentsvorbehalt im Datenschutzrecht, JZ 70 (2015), S. 213–221.
Kingsbury, Benedict: The Concept of 'Law' in Global Administrative Law, EJIL 20 (2009), S. 23–57.
Kipker, Dennis-Kenji: Grundlagen und Strukturen, in: Dennis-Kenji Kipker (Hrsg.), Cybersecurity, München 2020, Kap. 1
– (Hrsg.): Cybersecurity, München 2020.
Kipker, Dennis-Kenji/Birreck, Piet et al.: NIS-Richtlinie und der Entwurf der NIS-2-Richtlinie. Überblick, Gemeinsamkeiten und Unterschiede, MMR 2021, S. 214–220.
Kipker, Dennis-Kenji/Scholz, Dario: Das IT-Sicherheitsgesetz 2.0. Neue Rahmenbedingungen für die Cybersicherheit in Deutschland, MMR 2019, S. 431–435.
Kipker, Dennis-Kenji/Walkusz, Michael: Mehr verbraucherbezogene IT-Sicherheit durch die Umsetzung der Digitale-Inhalte-Richtlinie?, RDi 2021, S. 30.
Kirchhof, Ferdinand: Private Rechtsetzung, Berlin 1987.
Kirchhof, Paul: Kontrolle der Technik als staatliche und private Aufgabe, NVwZ 1988, S. 97–104.
Kittler, Friedrich: Auto Bahnen, in: Wolfgang Emmerich/Carl Wege (Hrsg.), Der Technikdiskurs in der Hitler-Stalin-Ära, Stuttgart u. a. 1995, S. 114–122.
Klafki, Anika: Risiko und Recht. Risiken und Katastrophen im Spannungsfeld von Effektivität, demokratischer Legitimation und rechtsstaatlichen Grundsätzen am Beispiel von Pandemien, Tübingen 2017.
Klems, Wolfgang: Die unbewältigte Moderne. Geschichte und Kontinuität der Technikkritik, Frankfurt a. M. 1988.
Klindt, Thomas (Hrsg.): ProdSG, München 2021.
Klindt, Thomas/Schucht, Carsten: Internationales, europäisches und nationales Technikrecht, in: Dirk Ehlers/Michael Fehling/Hermann Pünder (Hrsg.), Besonderes Verwaltungsrecht, Bd. 1, 4. Aufl. Heidelberg 2019, § 36.
Kloepfer, Michael: Recht ermöglicht Technik. Zu einer wenig beachteten Funktion des Umwelt- und Technikrechts, NuR 1997, S. 417–418.
–: Informationsgesetzbuch – Zukunftsvision?, K&R 1999, S. 241–251.
–: Informationsrecht, München 2002.
–: Einleitung, in: Michael Kloepfer (Hrsg.), Schutz kritischer Infrastrukturen, Baden-Baden 2010, S. 9–20.
–: Instrumente des Technikrechts, in: Martin Schulte/Rainer Schröder (Hrsg.), Handbuch des Technikrechts, 2. Aufl. Berlin u. a. 2011, S. 151–199.
– (Hrsg.): Katastrophenrecht: Grundlagen und Perspektiven, Baden-Baden 2008.
– (Hrsg.): Schutz kritischer Infrastrukturen, Baden-Baden 2010.
Kloepfer, Michael/Franzius, Claudio/Weber, Tim: Technik und Recht im wechselseitigen Werden. Kommunikationsrecht in der Technikgeschichte, Berlin 2002.
Kloepfer, Michael/Walus, Andreas/Deye, Sandra/Schärdel, Florian: Handbuch des

Katastrophenrechts. Bevölkerungsschutzrecht, Brandschutzrecht, Katastrophenschutzrecht, Katastrophenvermeidungsrecht, Rettungsdienstrecht, Zivilschutzrecht, Baden-Baden 2015.

Kment, Martin: Grenzüberschreitendes Verwaltungshandeln. Transnationale Elemente deutschen Verwaltungsrechts, Tübingen 2010.

–: Der Europäische Verbund für territoriale Zusammenarbeit. Vergegenwärtigung und kritische Analyse eines weithin unbekannt gebliebenen europäischen Organisationsmodells, DV 45 (2012), S. 155–169.

Knake, Robert K.: Internet Governance in an Age of Cyber Insecurity, New York 2010.

Knauff, Matthias: Der Regelungsverbund. Recht und Soft Law im Mehrebenensystem, 2010.

Kniesel, Michael: Sicherheitsrecht. Anmerkungen zu einem Rechtsgebiet in der Findungsphase, Die Polizei 2018, S. 265–274.

Knoll, Maximilian L.: Streitkräfteeinsatz zur Verteidigung gegen Cyberangriffe, Berlin 2020.

Knopp, Michael: Stand der Technik. Ein alter Hut oder eine neue Größe?, DuD 2017, S. 663–666.

Kochheim, Dieter: Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl. München 2018.

Köck, Wolfgang: Katastrophenschutzrecht, in: Dirk Ehlers/Michael Fehling/Hermann Pünder (Hrsg.), Besonderes Verwaltungsrecht, Bd. 3, 4. Aufl. Heidelberg 2021, § 71.

Kötter, Matthias: Subjektive Sicherheit, Autonomie und Kontrolle: Eine Analyse der jüngeren Diskurse des Sicherheitsrechts, Der Staat 43 (2004), S. 371–398.

–: Pfade des Sicherheitsrechts. Begriffe von Sicherheit und Autonomie im Spiegel der sicherheitsrechtlichen Debatte der Bundesrepublik Deutschland, Baden-Baden 2008.

Kolasky, Bob: A Risk-based Approach to National Cybersecurity, 14.1.2021, https://www.cisa.gov/blog/2021/01/14/risk-based-approach-national-cybersecurity.

Koloßa, Stephan: The GDPR's Extra-Territorial Scope. Data Protection in the Context of International Law and Human Rights Law, ZaöRV 80 (2020), S. 791–818.

Kompetenzzentrum Öffentliche IT: Deutschland-Index der Digitalisierung 2021, Berlin 2021, https://www.oeffentliche-it.de/deutschland-index.

Koreng, Ansgar/Lachenmann, Matthias (Hrsg.): Formularhandbuch Datenschutzrecht, 3. Aufl. München 2021.

Korzak, Elaine: UN GGE on Cybersecurity: The End of an Era?, DIPLOMAT v. 31.7.2017, https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe.

Koselleck, Reinhart: Geschichte, Geschichten und formale Zeitstrukturen, in: ders. (Hrsg.), Geschichte, Ereignis und Erzählung, München 1973, S. 211–222.

Kosseff, Jeff: Defining Cybersecurity Law, Iowa L. Rev. 103 (2018), S. 985–1013.

–: Hacking Cybersecurity Law, U. Ill. L. Rev. 2020, S. 811–850.

Kowalski, Bernd/Intemann, Matthias/Mühlenbruch, Tobias: Bedeutung des Cybersecurity Acts für die IT-Sicherheitszertifizierung in Deutschland und Europa, DuD 2021, S. 244–248.

Krämer, Felix: Europäische Sicherheitsarchitektur. Ambivalenzen im Raum der Freiheit, der Sicherheit und des Rechts, in: Tobias Brings-Wiesen/Frederik Ferreau (Hrsg.), 40 Jahre „Deutscher Herbst". Neue Überlegungen zu Sicherheit und Recht, 2019, S. 39–58.

Krämer, Hannes: Extraterritoriale Wirkungen des Unionsrechts – eine normanalytische Skizze, EuR 2021, S. 137–149.
Krasemann, Henry: Der aktuelle Stand der Datenschutz-Zertifizierung und Akkreditierung in Deutschland und Europa, DuD 2020, S. 645–648.
Krasmann, Susanne/Paul, Bettina et al.: Die gesellschaftliche Konstruktion von Sicherheit. Zur medialen Vermittlung und Wahrnehmung der Terrorismusbekämpfung, Berlin 2014.
Krasner, Stephen (Hrsg.): International Regimes, Ithaca, NY 1983.
Krause, Keith/Williams, Michael C.: Security and "Security Studies": Conceptual Evolution and Historical Transformation, in: Alexandra Gheciu/William C. Wohlforth (Hrsg.), The Oxford Handbook of International Security, Oxford 2018, S. 14–28.
Kretschmann, Andrea: Soziale Tatsachen. Eine wissenssoziologische Perspektive auf den „Gefährder", APuZ 67:32/33 (2017), S. 11–16.
Kretschmann, Andrea/Legnaro, Aldo: Abstrakte Gefährdungslagen. Zum Kontext der neuen Polizeigesetze, APuZ 69:21/23 (2019), S. 11–17.
–: Die „drohende Gefahr" als Schlüsselbegriff einer Sekuritisierung des Rechts, Zeitschrift für Rechtssoziologie 40 (2020), S. 3–25.
Krieger, Heike: Krieg gegen anonymus: Völkerrechtliche Regelungsmöglichkeiten bei unsicherer Zurechnung im Cyberwar, AVR 50 (2012), S. 1–20.
Krisch, Nico/Kingsbury, Benedict: Introduction: Global Governance and Global Administrative Law in the International Legal Order, EJIL 17 (2006), S. 1–13.
Kristensen, Kristian Søby: 'The Absolute Protection of our Citizens': Critical Infrastructure Protection and the Practice of Security, in: Myriam Dunn Cavelty/Kristian Søby Kristensen (Hrsg.), Securing 'the Homeland'. Critical infrastructure, risk and (in)security, Abingdon 2008, S. 63–83.
Kröger, Malte: Unabhängigkeitsregime im europäischen Verwaltungsverbund. Eine europa- und verfassungsrechtliche Untersuchung unionsrechtlicher Organisationsregelungen für Mitgliedstaaten anhand von Regulierungsagenturen, Datenschutzbehörden sowie statistischen Ämtern, Baden-Baden 2020.
Kröger, Malte/Pilniok, Arne (Hrsg.): Unabhängiges Verwalten in der Europäischen Union, Tübingen 2016.
Krönke, Christoph: Öffentliches Digitalwirtschaftsrecht. Grundlagen – Herausforderungen und Konzepte – Perspektiven, Tübingen 2020.
Krüger, Herbert: Rechtsetzung und technische Entwicklung, NJW 1966, S. 617–624.
Kube, Hanno: E-Government: Ein Paradigmenwechsel in Verwaltung und Verwaltungsrecht?, in: VVDStRL Bd. 78 (2019), S. 289–332.
Kühling, Jürgen/Buchner, Benedikt (Hrsg.), DS-GVO, 3. Aufl. München 2020.
Kugelmann, Dieter: Polizei und Polizeirecht in der föderalen Ordnung des Grundgesetzes, in: Ines Härtel (Hrsg.), Handbuch Föderalismus – Föderalismus als demokratische Rechtsordnung und Rechtskultur in Deutschland, Europa und der Welt, Bd. III, Heidelberg u. a. 2012, § 52.
–: Entwicklungslinien eines grundrechtsgeprägten Sicherheitsverwaltungsrechts, DV 47 (2014), S. 25–55.
Kulesza, Joanna: International Internet Law, London 2012.
Kulick, Andreas: Gefahr, „Gefährder" und Gefahrenabwehrmaßnahmen angesichts terroristischer Gefährdungslagen, AöR 143 (2018), S. 175–219.
–: Horizontalwirkung im Vergleich. Ein Plädoyer für die Geltung der Grundrechte zwischen Privaten, Tübingen 2020.

Kumar, Niraj/Mishra, Vishnu Mohan/Kumar, Adesh: Smart Grid and Nuclear Power Plant Security by Integrating Cryptographic Hardware Chip, Nuclear Engineering and Technology 53:10 (2021), S. 3327–3334.
Kuner, Christopher: Data Nationalism and its Discontents, Emory Law Journal 64 (2015), S. 2089–2098.
–: Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law, International Data Privacy Law 5:4 (2015), S. 235–245.
–: The Internet and the Global Reach of EU Law, in: Marise Cremona/Joanne Scott (Hrsg.), EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law, Oxford 2018, S. 112–145.
Kurose, James F./Ross, Keith W.: Computer Networking. A Top-Down Approach, 8. Aufl. Boston u. a. 2020.
Kurz, Constanze: Keine Antworten der Festplatten-Hersteller auf NSA-Infiltration, Netzpolitik.org v. 13.5.2015, https://netzpolitik.org/2015/keine-antworten-der-festplatten-hersteller-auf-nsa-infiltration/.
Ladeur, Karl-Heinz: Computerkultur und Evolution der Methodendiskussion in der Rechtswissenschaft, ARSP 74 (1988), S. 218–238.
–: Umweltrecht und technologische Innovation, UTR (1988), S. 305–333.
–: Das Umweltrecht der Wissensgesellschaft, Berlin 1995.
–: Risikobewältigung durch Flexibilisierung und Prozeduralisierung des Rechts – Rechtliche Bindung von Ungewissheit oder Selbstverunsicherung durch Recht, in: Alfons Bora (Hrsg.), Rechtliches Risikomanagement, Berlin 1999, S. 41–64.
–: Datenschutz – vom Abwehrrecht zur planerischen Optimierung von Wissensnetzwerken, DuD 2000, S. 12–19.
–: Das Recht auf informationelle Selbstbestimmung: Eine juristische Fehlkonstruktion?, DÖV 2009, S. 45–55.
–: Die Textualität des Rechts. Zur poststrukturalistischen Kritik des Rechts, Weilerswist 2015.
–: Recht – Wissen – Kultur. Die fragmentierte Ordnung, Berlin 2016.
Ladiges, Manuel: Der Cyberraum – ein (wehr-) verfassungsrechtliches Niemandsland?, NZWehrr 2017, S. 221–244.
Lahmann, Henning: Die völkerrechtliche Dimension der IT-Sicherheit, in: Gerrit Hornung/Martin Schallbruch (Hrsg.), IT-Sicherheitsrecht, Baden-Baden 2021, § 6.
Lallie, Harjinder Singh/Shepherd, Lynsay A. et al.: Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-crime and Cyber-attacks during the Pandemic, Computers & Security 105 (2021), S. 102248.
Land, Molly: Toward an International Law of the Internet, Harv. Int'l L. J. 54 (2013), S. 393–458.
–: The Problem of Platform Law: Pluralistic Legal Ordering on Social Media, in: Paul Schiff Berman (Hrsg.), The Oxford Handbook of Global Legal Pluralism, Oxford 2020, S. 975–994.
Landau, Susan: Exceptional Access: The Devil is in the Details, Lawfare v. 26.12.2018, https://www.lawfareblog.com/exceptional-access-devil-details.
–: Listening In: Cybersecurity in an Insecure Age, New Haven u. a. 2017.
Landis, James M.: The Administrative Process, New Haven 1938.
Landwehr, Achim: Diskurs – Macht – Wissen. Perspektiven einer Kulturgeschichte des Politischen, Archiv für Kulturgeschichte 87 (2003), S. 71–117.
Landwers, Anne-Sophie: Behördliche Öffentlichkeitsarbeit im Recht. Zulässigkeit,

Möglichkeiten und Grenzen am Beispiel des Bundeskartellamts und der Bundesanstalt für Finanzdienstleistungsaufsicht, Baden-Baden 2019.
Lange, Hans-Jürgen: Innere Sicherheit im Politischen System der Bundesrepublik Deutschland, Wiesbaden 1999.
Lange, Hans-Jürgen/Bötticher, Astrid (Hrsg.): Cyber-Sicherheit, Wiesbaden 2015.
Lange, Hans-Jürgen/Endreß, Christian/Wendekamm, Michaela (Hrsg.): Versicherheitlichung des Bevölkerungsschutzes, Wiesbaden 2013.
Lange, Hans-Jürgen/Gusy, Christoph (Hrsg.): Kooperation im Katastrophen- und Bevölkerungsschutz, Wiesbaden 2015.
Langwald, Henning-Timm/Sanders, Jan et al.: Stand der Technik im Bereich der Kritischen Infrastrukturen, BSI Forum 27:6 (2019), S. 35–39.
Lapp, Thomas: Ziviles Haftungsrecht, in: Dennis-Kenji Kipker (Hrsg.), Cybersecurity, München 2020, S. 231–272.
Larenz, Karl: Methodenlehre der Rechtswissenschaft, 6. Aufl. 1991.
Laschet, Armin: Innere Sicherheit als Gemeinschaftsaufgabe für Bund, Länder und die Europäische Union: ein Beitrag aus nordrheinwestfälischer Perspektive, in: Jahrbuch des Föderalismus 2018, S. 21–33.
Leeuw, Karl/Bergstra, Jan (Hrsg.): The History of Information Security. A Comprehensive Handbook, Amsterdam u. a. 2007.
Lehmbruch, Gerhard: Der unitarische Bundesstaat in Deutschland: Pfadabhängigkeit und Wandel, in: Arthur Benz/Gerhard Lehmbruch (Hrsg.), Föderalismus. Politische Vierteljahresschrift Sonderheft, Bd. 32, 2002, S. 53–110
Lehnert, Matthias: Frontex und operative Maßnahmen an den europäischen Außengrenzen. Verwaltungskooperation – materielle Rechtsgrundlagen – institutionelle Kontrolle, Baden-Baden 2014.
Leiner, Barry M./Cerf, Vinton G. et al.: Brief History of the Internet, 2000, http://www.internetsociety.org/brief-history-internet.
Leisner-Egensperger, Anna: Polizeirecht im Umbruch. Die drohende Gefahr, DÖV 2018, S. 677–688.
Leisterer, Hannfried: Internetsicherheit in Europa. Zur Gewährleistung der Netz- und Informationssicherheit durch Informationsverwaltungsrecht, Tübingen 2018.
Lemley, Mark A.: Place and Cyberspace, Calif. L. Rev. 91 (2003), S. 521–542.
Lenk, Hans: Zu neueren Ansätzen der Technikphilosophie, in: Hans Lenk/Simon Moser (Hrsg.), Techne, Technik, Technologie, Pullach 1973, S. 198–231.
Lenk, Klaus: Abschied vom Zuständigkeitsdenken. Bürokratieabbau durch vernetzte Erstellung von Verwaltungsleistungen, VM (2007), S. 235–242.
Lentzos, Filippa/Rose, Nikolas: Die Unsicherheit regieren. Biologische Bedrohungen, Notfallplanung, Schutz und Resilienz in Europa, in: Patricia Purtschert/Katrin Meyer/Yves Winter (Hrsg.), Gouvernementalität und Sicherheit. Zeitdiagnostische Beiträge im Anschluss an Foucault, Bielefeld 2008, S. 75–102.
Lepsius, Oliver: Verwaltungsrecht unter dem Common Law. Amerikanische Entwicklungen bis zum New Deal, Tübingen 1997.
–: Risikosteuerung durch Verwaltungsrecht: Ermöglichung oder Begrenzung von Innovationen?, in: VVDStRL 63 (2004), S. 264–315.
–: Standardsetzung und Legitimation, in: Christoph Möllers/Andreas Voßkuhle/Christian Walter (Hrsg.), Internationales Verwaltungsrecht – Eine Analyse anhand von Referenzgebieten, Tübingen 2007, S. 345–374.

–: Das Computer-Grundrecht: Herleitung – Funktion – Überzeugungskraft, in: Fredrik Roggan (Hrsg.), Online-Durchsuchungen, 2008, S. 21–56.
–: Sicherheit und Freiheit – ein zunehmend asymmetrisches Verhältnis, in: Gunnar Folke Schuppert/Wolfgang Merkel et al. (Hrsg.), Der Rechtsstaat unter Bewährungsdruck, Baden-Baden 2010, S. 23–54.
–: Regulierungsrecht in den USA, in: Michael Fehling/Matthias Ruffert (Hrsg.), Regulierungsrecht, Tübingen 2010, § 1.
–: Parlamentsrechte und Parlamentsverständnisse in der neueren Rechtsprechung des Bundesverfassungsgerichts, RuP 2016, S. 137–149.
–: Gesetzesstruktur im Wandel – Teil 1: Strukturmerkmale der Kodifikation, JuS 2019, S. 14–17.
Lerche, Peter: Föderalismus als nationales Ordnungsprinzip, in: VVDStRL 21 (1964), S. 66–104.
Lessig, Lawrence: The Path of Cyberlaw, Yale L. J. 104 (1995), S. 1743–1755.
–: The Zones of Cyberspace, Stan. L. Rev. 48 (1996), S. 1403–1411.
–: Code and other Laws of Cyberspace, New York 1999.
–: The Architecture of Innovation, Duke L. J. 51 (2002), S. 1783–1801.
–: Code: Version 2.0, New York 2006.
Leuschner, Sebastian: Sicherheit als Grundsatz. Eine grundrechtsdogmatische Rekonstruktion im Unionsrecht am Beispiel der Cybersicherheit, Tübingen 2018.
Levine, Yasha: Surveillance Valley. The Secret Military History of the Internet, London 2018.
Levy, Ian/Robinson, Crispin: Principles for a More Informed Exceptional Access Debate, Lawfare v. 29.11.2018, https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate.
Lewallen, Jonathan: Emerging technologies and problem definition uncertainty: The case of cybersecurity, Regulation & Governance 15 (2021), S. 1035–1052.
von Lewinski, Kai: Geschichte des Datenschutzrechts von 1600 bis 1977, in: Felix Arndt/Nicole Betz et al. (Hrsg.), Freiheit – Sicherheit – Öffentlichkeit. 48. Assistententagung Ö, Baden-Baden 2009, S. 196–220.
–: Resilienz der Verwaltung in Unsicherheits- und Risikosituationen, in: Hermann Hill/Utz Schliesky (Hrsg.), Management von Unsicherheit und Nichtwissen, Baden-Baden 2016, S. 239–252.
– (Hrsg.): Resilienz des Rechts, Baden-Baden 2016.
Libicki, Martin C.: Cyberdeterrence and Cyberwar, Santa Monica u. a. 2009.
Liguori, Carlos: Exploring Lawful Hacking as a Possible Answer to the "Going Dark" Debate, Mich. Telecomm. & Tech. L. Rev. 26 (2020), S. 317–345.
Lin, Herbert: Attribution of Malicious Cyber Incidents: From Soup to Nuts, Columbia SIPA Journal of International Affairs, 2016, https://jia.sipa.columbia.edu/attribution-malicious-cyber-incidents.
Lin, Herbert/Kerr, Jaclyn: On Cyber-Enabled Information/Influence Warfare and Manipulation, in: Paul Cornish (Hrsg.), Oxford Handbook of Cyber Security, Oxford 2021, S. 251–272.
Lin, Herbert/Trachtman, Joel: Diagonal Export Controls to Counter Diagonal Transnational Attacks on Civil Society, EJIL 31:3 (2020), S. 917–939.
Lindahl, Hans: Fault Lines of Globalization. Legal Order and the Politics of A-Legality, Oxford 2013.

Lindsay, Jon R.: Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence Against Cyberattack, Journal of Cybersecurity 1:1 (2015), S. 53–67.
Lindseth, Peter/Rose-Ackerman, Susan (Hrsg.): Comparative Administrative Law, 2. Aufl. Cheltenham 2017.
Linke, Tobias: Rechtsfragen der Einrichtung und des Betriebs eines Nationalen Cyber-Abwehrzentrums als informelle institutionalisierte Sicherheitskooperation, DÖV 2015, S. 128–139.
Lipner, Steven B.: The Birth and Death of the Orange Book, IEEEA 37:2 (2015), S. 19–31.
Lisken, Hans (Begr.)/*Bäcker, Matthias/Denninger, Erhard/Graulich, Kurt* (Hrsg.): Handbuch des Polizeirechts – Gefahrenabwehr, Strafverfolgung, Rechtsschutz, 7. Aufl. München 2021.
Loer, Kathrin/Reiter, Renate/Töller, Annette Elisabeth: Was ist ein Politikfeld und warum entsteht es?, dms 8:1 (2015), S. 7–28.
Löffelmann, Markus: Die Zukunft der deutschen Sicherheitsarchitektur – Vorbild Bayern?, GSZ 2018, S. 85–91.
–: Die Zukunft der deutschen Sicherheitsarchitektur – Vorbild Bayern?, GSZ 2018, S. 85–91.
–: Datenerhebung aus dem „Smart Home" im Sicherheitsrecht, GSZ 2020, S. 244–250.
Loughlin, Martin: Constitutional Pluralism: An Oxymoron?, Global Constitutionalism 3:1 (2014), S. 9–30.
Lübbe-Wolff, Gertrude: Verfassungsrechtliche Fragen der Normsetzung und Normkonkretisierung im Umweltrecht, ZG 6 (1991), S. 219–248.
–: Satzungsrechtliche Betretungsrechte und Art. 13 GG, DVBl. 1993, S. 762–769.
Ludwigs, Markus: Die Bundesnetzagentur auf dem Weg zur Independent Agency? Europarechtliche Anstöße und verfassungsrechtliche Grenzen, DV 44 (2011), S. 41–74.
Luhmann, Niklas: Die Gesellschaft der Gesellschaft, Frankfurt a. M. 1997.
–: Soziologie des Risikos, Berlin u. a. 2003.
–: Ökologische Kommunikation. Kann die moderne Gesellschaft sich auf ökologische Gefährdungen einstellen?, Wiesbaden 2008.
Lukasik, Stephen J.: Why the Arpanet Was Built, IEEEA 33:3 (2011), S. 4–20.
Lundgreen, Peter: Standardization – Testing – Regulation, Bielefeld 1986.
Lüttringhaus, Jan: Das internationale Datenprivatrecht: Baustein des Wirtschaftskollisionsrechts des 21. Jahrhunderts, ZVglRWiss 117 (2018), S. 50–82.
Lutz, Burkart: Das Ende des Technikdeterminismus und die Folgen – soziologische Technikforschung vor neuen Aufgaben und neuen Problemen, in: ders. (Hrsg.), Technik und sozialer Wandel. Verhandlungen des 23. Deutschen Soziologentages in Hamburg 1986, Frankfurt a. M. 1987, S. 34–52.
Lynskey, Orla: The Foundations of EU Data Protection Law: The Dual Objectives of European Data Protection Regulation, Oxford 2015.
Lystrup, Owen: BGP and the System of Trust that Runs the Internet Pt. 1, 21.9.2021, https://umbrella.cisco.com/blog/bgp-and-the-system-of-trust-that-runs-the-internet-pt-1.
Mačák, Kubo: From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers, Leiden Journal of International Law 30:4 (2017), S. 877–899.
MacCormick, Neil: Beyond the Sovereign State, The Modern L. Rev. 56:1 (1993), S. 1–18.
MacKinnon, Rebecca: Consent of the Networked: The Worldwide Struggle for Internet Freedom, New York 2012.

Maddocks, Jennifer: Outsourcing of Governmental Functions in Contemporary Conflict. Rethinking the Issue of Attribution, Va. J. Int'l L. 59 (2019), S. 47–96.
Mager, Ute: Die europäische Verwaltung zwischen Hierarchie und Netzwerk, in: Hans-Heinrich Trute/Thomas Groß et al. (Hrsg.), Allgemeines Verwaltungsrecht – zur Tragfähigkeit eines Konzepts, Tübingen 2008, S. 369–397.
Mai, Manfred: Technikblindheit des Rechts – Technikignoranz der Juristen?, Zeitschrift für Rechtssoziologie 13 (1992), S. 257–270.
Maier, Bernhard: How Has the Law Attempted to Tackle the Borderless Nature of the Internet?, Int'l J. L. & Info. Tech. 18 (2010), S. 142–175.
Maier, Natalie/Pawlowska, Ilona M. et al.: Die Zertifizierung nach der DS-GVO. Transparenz und Vertrauen für Nutzer digitaler Dienste?, ZD 2020, S. 445–449.
Majone, Giandomenico: The Regulatory State and its Legitimacy Problems, West European Politics 22 (1999), S. 1–24.
Makropoulos, Michael: „Sicherheit", in: Joachim Ritter/Karlfried Gründer/Gottfried Gabriel (Hrsg.), Historisches Wörterbuch der Philosophie, Bd. 9, Basel 1995, Sp. 745–750.
Mallmann, Christoph: Datenschutz in Verwaltungs-Informationssystemen, München u. a. 1976.
Marburger, Peter: Die Regeln der Technik im Recht, Köln u. a. 1979.
Marcuse, Herbert: Some Social Implications of Modern Technology, Studies in Philosophy and Social Science 9 (1941), S. 414–439.
–: Industrialisierung und Kapitalismus, in: O. Stammer (Hrsg.), Max Weber und die Soziologie heute: Verhandlungen des 15. Deutschen Soziologentages in Heidelberg, Tübingen 1964, S. 161–180.
–: Industrialization and Capitalism, New Left Review (1965), S. 3–17.
–: Der eindimensionale Mensch, Neuwied u. a. 1967.
Marsch, Nikolaus: Das europäische Datenschutzgrundrecht. Grundlagen – Dimensionen – Verflechtungen, Tübingen 2018.
Martini, Mario: Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz, Berlin 2019.
Martini, Mario/Fröhlingsdorf, Sarah: Catch me if you can: Quellen-Telekommunikationsüberwachung zwischen Recht und Technik, NVwZ-Extra 24 2020, S. 1–15.
Marx, Axel/Maertens, Miet et al. (Hrsg.): Private Standards and Global Governance. Legal and Economic Perspectives, Cheltenham 2012.
Marx, Leo: The Machine in the Garden. Technology and the Pastoral Ideal in America, Oxford 1964.
Marxsen, Christian: Verfassungsrechtliche Regeln für Cyberoperationen der Bundeswehr. Aktuelle Herausforderungen für Einsatzbegriff und Parlamentsvorbehalt, Juristenzeitung 72 (2017), S. 543–552.
Mascolo, Georg: Die gefährlichste Waffe unserer Zeit, SZ, 11.2.2022, https://www.sueddeutsche.de/kultur/pegasus-ueberwachung-smartphone-abhoeren-1.5526140.
Masing, Johannes: Parlamentarische Untersuchungen privater Sachverhalte. Art. 44 GG als staatsgerichtetes Kontrollrecht, Tübingen 1998.
–: Transparente Verwaltung: Konturen eines Informationsverwaltungsrechts, in: VVDStRL 63 (2004), S. 377–441.
–: Grundstrukturen eines Regulierungsverwaltungsrechts – Regulierung netzbezogener Märkte am Beispiel Bahn, Post, Telekommunikation und Strom, DV 36 (2003), S. 1–32.

–: Unabhängige Behörden und ihr Aufgabenprofil, in: Johannes Masing/Gérard Marcou (Hrsg.), Unabhängige Regulierungsbehörden. Organisationsrechtliche Herausforderungen in Frankreich und Deutschland, Tübingen 2010, S. 181–220.
–: Die Ambivalenz von Freiheit und Sicherheit, JZ 66 (2011), S. 753–758.
–: Herausforderungen des Datenschutzes, NJW 2012, S. 2305–2311.
Masing, Johannes/Marcou, Gérard (Hrsg.): Unabhängige Regulierungsbehörden. Organisationsrechtliche Herausforderungen in Frankreich und Deutschland, Tübingen 2010.
Mathew, Aswhin: The Myth of the Decentralised Internet, Internet Policy Review 5:3 (2016), https://doi.org/10.14763/2016.3.425.
Maurer, Tim: Cyber Mercenaries. The State, Hackers, and Power, Cambridge 2018.
May, Christopher: The Information Society: A Skeptical View, Cambridge 2002.
Maybaum, Markus/Tölle, Jens: Arms Control in Cyberspace. Architecture for a Trust-based Implementation Framework Based on Conventional Arms Control Methods, 8th International Conference on Cyber Conflict (CyCon), 2016, S. 159–173.
Mayer, Franz C.: Recht und Cyberspace, NJW 1996, S. 1782–1791.
–: Europe and the Internet: The Old World and the New Medium, EJIL 11 (2000), S. 149–169.
–: Völkerrecht und Cyberspace: Entgrenztes Recht und entgrenzte Medien, in: Udo Thiedeke (Hrsg.), Soziologie des Cyberspace, Wiesbaden 2004, S. 491–521.
Mayntz, Renate: Triebkräfte der Technikentwicklung und die Rolle des Staates, in: Georg Simonis/Renate Martinsen/Thomas Saretzki (Hrsg.), Politik und Technik. Sonderheft 31 Politische Vierteljahresschrift, Opladen 2001, S. 3–18.
–: Die Handlungsfähigkeit des Nationalstaats in Zeiten der Globalisierung, in: Ludger Heidbrink/Alfred Hirsch (Hrsg.), Staat ohne Verantwortung?, Frankfurt a. M. u. a. 2007, S. 267–281.
Mazanec, Brian M./Thayer, Bradley A.: Deterring Cyber Warfare, Basingstoke 2014.
McGowan, David: The Trespass Trouble and the Metaphor Muddle, J. L. Econ. & Pol'y 1 (2005), S. 109–145.
McNeill, William H.: The Pursuit of Power. Technology, Armed Force, and Society since A.D. 1000, Chicago 1982.
Meakins, Joss: A Zero-sum Game: The Zero-day Market in 2018, Journal of Cyber Policy 4:1 (2019), S. 60–71.
Meder, Stephan: Ius non scriptum – Traditionen privater Rechtsetzung, 2. Aufl. Tübingen 2009.
Mehrbrey, Kim Lars/Schreibauer, Marcus: Haftungsverhältnisse bei Cyber-Angriffen – Ansprüche und Haftungsrisiken von Unternehmen und Organen, MMR 2016, S. 75–82.
Meineck, Sebastian/Biselli, Anna: EU-Datenschutzbehörden nehmen Chatkontrolle komplett auseinander, Netzpolitik.org v. 29.7.2022, https://netzpolitik.org/2022/ernste-bedenken-eu-datenschutzbehoerden-nehmen-chatkontrolle-komplett-auseinander.
Meinel, Florian: Der Jurist in der industriellen Gesellschaft. Ernst Forsthoff und seine Zeit, Berlin 2011.
–: Organisation und Kontrolle im Bereich der Regierung. Zur verfassungsrechtlichen Stellung von Kabinettsausschüssen, insbesondere des Bundessicherheitsrats, im parlamentarischen Regierungssystem, DÖV 2015, S. 717–726.
–: Selbstorganisation des parlamentarischen Regierungssystems, Tübingen 2019.

Meister, Andre: BKA nutzt Emotet-Takedown als Türöffner für mehr Befugnisse und neue Gesetze, Netzpolitik.org v. 22.3.2021, https://netzpolitik.org/2021/schadsoftware-bereinigung-bka-nutzt-emotet-takedown-als-tueroeffner-fuer-mehr-befugnisse-und-neue-gesetze/#2021–02–10_Innenausschuss_Protokoll_TOP-14_Emotet.

–: BSI programmierte und arbeitete aktiv am Staatstrojaner, streitet aber Zusammenarbeit ab, Netzpolitik.org v. 16.3.2015, https://netzpolitik.org/2015/geheime-kommunikation-bsi-programmierte-und-arbeitete-aktiv-am-staatstrojaner-streitet-aber-zusammenarbeit-ab/.

Mell, Peter/Scarfone, Karen/Romanosky, Sasha: A Complete Guide to the Common Vulnerability Scoring System, Version 2.0, 2007, https://www.first.org/cvss/v2/guide.

Menzel, Jörg: Internationales Öffentliches Recht. Verfassungs- und Verwaltungsgrenzrecht in Zeiten offener Staatlichkeit, Tübingen 2011.

Mercer, Shannon Togawa: The Limitations of European Data Protection as a Model for Global Privacy Regulation, 114 (2020), S. 20–25.

Meyer, Jürgen/Hölscheidt, Sven (Hrsg.): Charta der Grundrechte der Europäischen Union, 5. Aufl., Baden-Baden 2019.

Meyer-Teschendorf, Klaus G.: Fortentwicklung der Rechtsgrundlagen für den Bevölkerungsschutz, DVBl. 2009, S. 1221–1229.

Miadzvetskaya, Yuliya/Wessel, Ramses A.: The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox, European Papers 7 (2022), S. 413–438.

Michael, Lothar: Rechtsetzende Gewalt im kooperierenden Verfassungsstaat. Normprägende und normersetzende Absprachen zwischen Staat und Wirtschaft, Berlin 2002.

–: Formen- und Instrumentenmix, in: Andreas Voßkuhle/Martin Eifert/Christoph Möllers (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. 2, 3. Aufl. München 2022, § 40.

Michael, Lothar/Morlok, Martin: Grundrechte, 8. Aufl. Baden-Baden 2023.

Michaelis, Patrick: Der „Stand der Technik" im Kontext regulatorischer Anforderungen, DuD 2016, S. 458–462.

–: Cybersecurity: Technische Voraussetzungen der „Maßnahme" nach § 13 Abs. 7 TMG – Herausforderung „Stand der Technik", ITRB 2016, S. 118–119.

Michl, Fabian: Situativ staatsgleiche Grundrechtsbindung privater Akteure – Zugleich Besprechung von BVerfG, Beschluss vom 11.4.2018 – 1 BvR 3080/09, JZ 73 (2018), S. 910–918.

Miller, Arthur R.: The National Data Center and Personal Privacy, The Atlantic 220:5 (1967), S. 53–57.

–: Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society, Mich. L. Rev. 67 (1969), S. 1089–1246.

Miller, Greg: The Intelligence Coup of the Century, Washington Post, 11.2.2020, https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/?itid=hp_ed-picks_crypto211%3Ahomepage%2Fstory-ans.

Minsky, Marvin: Computation: Finite and Infinite Machines., Englewood Cliffs 1967.

Mirowski, Philip: Machine Dreams. Economics Becomes a Cyborg Science, Cambridge 2002.

Mitchell, Bonnie/Kaul, Krystle et al.: Going Dark: Impact to Intelligence and Law Enforcement and Threat Mitigation, 2017, https://www.hsdl.org/?view&did=826441.

Moechel, Erich: EU erhielt die zwölfte Cybersicherheitsorganisation, 4.7.2021, https://fm4.orf.at/stories/3016230/.
Möllers, Christoph: Braucht das öffentliche Recht einen neuen Methoden- und Richtungsstreit?, VerwArch 90 (1999), S. 187–207.
–: Theorie, Praxis und Interdisziplinarität in der Verwaltungsrechtswissenschaft, Verwaltungsarchiv 93 (2002), S. 22–61.
–: Transnationale Behördenkooperation. Verfassungs- und völkerrechtliche Probleme transnationaler administrativer Standardsetzung, ZaöRV 65 (2005), S. 351–389.
–: Materielles Recht – Verfahrensrecht – Organisationsrecht, in: Hans-Heinrich Trute/Thomas Groß et al. (Hrsg.), Allgemeines Verwaltungsrecht. Zur Tragfähigkeit eines Konzepts, Tübingen 2008, S. 489–512.
–: Funktionen des Verfassungsprozessrechts, in: Joachim Münch/Alexander Thiele (Hrsg.), Verfassungsrecht im Widerstreit, Gedächtnisschrift für Werner Heun, Tübingen 2019, S. 149–174.
Möllers, Christoph/Pflug, Ludger: Verfassungsrechtliche Rahmenbedingungen des Schutzes kritischer IT-Infrastrukturen, in: Michael Kloepfer (Hrsg.), Schutz kritischer Infrastrukturen, Baden-Baden 2010, S. 47–66.
Möllers, Christoph/Voßkuhle, Andreas: Die Deutsche Staatsrechtswissenschaft im Zusammenhang der internationalisierten Wissenschaften, DV 26 (2003), S. 321–332.
Möllers, Christoph/Voßkuhle, Andreas/Walter, Christian (Hrsg.): Internationales Verwaltungsrecht, Tübingen 2007.
Monroy, Matthias: Cybersecurity-Initiativen als Teil einer Technologieoffensive, Vorgänge 2015, S. 54–60.
Morozov, Evgeny: The Net Delusion: The Dark Side of Internet Freedom, Cambridge (Mass.) 2011.
Moschovitis, Christos J. P./Poole, Hilary et al.: History of the Internet: A Chronology, 1843 to the Present, Santa Barbara u. a. 1999.
Möslein, Florian (Hrsg.): Regelsetzung im Privatrecht, Tübingen 2019.
Möstl, Markus: Die staatliche Garantie für die öffentliche Sicherheit und Ordnung. Sicherheitsgewährleistung im Verfassungsstaat, im Bundesstaat und in der Europäischen Union, Tübingen 2002.
–: Staatsaufgabe Sicherheit in Zeiten des Terrorismus – der rechtsstaatliche Rahmen, in: Andreas Kulick/Michael Goldhammer (Hrsg.), Der Terrorist als Feind? Personalisierung im Polizei- und Völkerrecht, Tübingen 2020, S. 67–81.
–: Rechtsstaatlicher Rahmen der Terrorabwehr – eine Stellungnahme zum Stand der Diskussion um Gefahr, Gefahrenvorfeld und drohende Gefahr, DVBl. 2020, S. 160–166.
Moulin, Thibault: Reviving the Principle of Non-Intervention in Cyberspace: The Path Forward, Journal of Conflict and Security Law 25:3 (2020), S. 423–447.
Mrozek, Anna: Grenzschutz als supranationale Aufgabe. Der Schutz der europäischen Außengrenzen unter der Beteiligung der Bundespolizei, Baden-Baden 2013.
von zur Mühlen, Nicolas: Zugriffe auf elektronische Kommunikation, 2019.
Müller, Christoph/Nievergelt, Bernhard: Technikkritik in der Moderne, Opladen 1996.
Müller, Michael W./Schwabenbauer, Thomas: Unionsgrundrechte und Datenverarbeitung durch nationale Sicherheitsbehörden, NJW 2021, S. 2079–2085.
–: Verfassungs-, unions- und konventionsrechtliche Vorgaben für die Informationsverarbeitung im Polizei- und Strafverfahrensrecht, in: Lisken/Denninger, HdbPolR, 7. Aufl. 2021, Kap. G.

Mueller, Milton L.: Ruling the Root. Internet Governance and the Taming of Cyberspace, Cambridge (Mass.) u. a. 2002.
–: Networks and States. The Global Politics of Internet Governance, Cambridge (Mass.) u. a. 2010.
–: Gibt es Souveränität im Cyberspace?, Journal of Self-Regulation and Regulation 1 (2015), S. 65–80.
–: Will the Internet Fragment?, Cambridge 2017.
Mueller, Milton/Grindal, Karl/Kuerbis, Brenden/Badiri, Forzanek: Cyber attribution. Can a New Institution Achieve Transnational Credibility?, The Cyber Defense Review 4:1 (2019), S. 107–122.
Müller, Stefan: Homeoffice in der arbeitsrechtlichen Praxis, 2. Aufl. Baden-Baden 2020.
Müller-Mall, Sabine: Legal Spaces. Towards a Topological Thinking of Law, Berlin u. a. 2013.
Müller-Quade, Jörn/Huber, Matthias/Nilges, Tobias: Daten verschlüsselt speichern und verarbeiten in der Cloud, DuD 39 (2015), S. 531–535.
Müllmann, Dirk/Volkamer, Melanie: Meldepflicht von Mitarbeitenden bei IT-Sicherheits- und Datenschutzvorfällen, ZD 2021, S. 8–12.
Münch, Ursula: Wenn Terrorangst auf Bundesstaatlichkeit trifft: Vor- und Nachteile der föderalen Organisation von Innerer Sicherheit, in: Helga Pelizäus/Ludwig Nieder (Hrsg.), Das Risiko – Gedanken übers und ins Ungewisse. Interdisziplinäre Aushandlungen des Risikophänomens im Lichte der Reflexiven Moderne. Eine Festschrift für Wolfgang Bonß, Wiesbaden 2019, S. 271–286.
von Münch, Ingo/Kunig, Philip (Begr.)/*Kämmerer, Jörn Axel/Kotzur, Markus* (Hrsg.): Grundgesetz-Kommentar, 7. Aufl. München 2021.
Münkler, Laura (Hrsg.): Dimensionen des Wissens im Recht, Tübingen 2019.
Murswiek, Dietrich: Die staatliche Verantwortung für die Risiken der Technik. Verfassungsrechtliche Grundlagen und immissionsschutzrechtliche Ausformung, Berlin 1985.
–: Die Bewältigung der wissenschaftlichen und technischen Entwicklungen durch das Verwaltungsrecht, in: VVDStRL 48 (1990), S. 207–234.
–: Dynamik der Technik und Anpassung des Rechts: Kreislaufgesetzgebung, in: Burkhardt Ziemske (Hrsg.), Festschrift für Martin Kriele, München 1997, S. 651–676.
Musil, Andreas/Kirchner, Sören: Katastrophenschutz im föderalen Staat, DV 39 (2006), S. 373–391.
Nai Fovino, Igor/Barry, Geraldine et al. (Hrsg.): Cybersecurity, our digital anchor, 2020, https://publications.jrc.ec.europa.eu/repository/bitstream/JRC121051/cybersecurity_online.pdf.
Nakashima, Ellen/Timberg, Craig: NSA officials worried about the day its potent hacking tool would get loose. Then it did, Washington Post, 16.5.2017, https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-IT-did/2017/05/16/50670b16–3978–11e7-a058-ddbb23c75d82_story.html.
National Security Agency/Cybersecurity and Infrastructure Security Agency/Federal Bureau of Investigation: Russian SVR Targets U.S. and Allied Networks, April 2021, https://media.defense.gov/2021/Apr/15/2002621240/-1/-1/0/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF.

Nettesheim, Martin: Grundrechtsschutz der Privatheit, in: VVDStRL 70 (2011), S. 7–49.

Neubert, Carl Wendelin: Grundrechtliche Schutzpflicht des Staates gegen grundrechtsbeeinträchtigende Maßnahmen fremder Staaten am Beispiel der Überwachung durch ausländische Geheimdienste, AöR 141 (2015), S. 267–304.

Neuffer, Simon Gabriel: Zwecklose Technik, Berlin 2019.

Neuhöfer, Daniel: Der Zugriff auf serverbasiert gespeicherte E-Mails beim Provider. Verfassungsrechtliche Anforderungen an eine strafverfahrensrechtliche Ermächtigungsgrundlage, Hamburg 2011.

von Neumann, John: First Draft of a Report on the EDVAC (1945), IEEEA 15 (1993), S. 27–75.

Neumann, Volker: Der harte Weg zum sanften Ziel. Ernst Forsthoffs Rechts- und Staatstheorie als Paradigma konservativer Technikkritik, in: Alexander Roßnagel (Hrsg.), Recht und Technik im Spannungsfeld der Kernenergiekontroverse, Opladen 1984, S. 88–99.

Neusel, Hans: Aktivitäten der Bundesregierung zur IT-Sicherheit, RDV 1990, S. 161–167.

Newman, Lily Hay: The Leaked NSA Spy Tool that Hacked the World, Wired, 7.3. 2018, www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/.

NIS Cooperation Group: Cybersecurity of 5G networks. EU Toolbox of risk mitigating measures, 29.1.2020, https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

Nissenbaum, Helen: Where Computer Security Meets National Security, Ethics and Information Technology 7 (2005), S. 61–73.

–: From Preemption to Circumvention: If Technology Regulates Why Do We Need Regulation (and Vice Versa)?, Berkeley Tech. L. J. 26 (2011), S. 1367–1386.

NIST: Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, Special Publication 800–160 Vol. 1, November 2016, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800–160v1.pdf.

Nitz, Gerhard: Private und öffentliche Sicherheit, Berlin 2000.

NSO: Pegasus – Product Description, 2019, https://s3.documentcloud.org/documents/4599753/NSO-Pegasus.pdf.

Null, Linda/Lobur, Julia: The Essentials of Computer Organization and Architecture, 5. Aufl. Boston u. a. 2018.

Nye, Joseph S.: The Future of Power. Its Changing Nature and Use in the Twenty-first Century, New York 2011.

Oberleitner, Gerd: Human Security: Idea, Policy and Law, in: Mary Martin/Taylor Owen (Hrsg.), Routledge Handbook on Human Security, London 2013, S. 319–330.

Oberthür, Sebastian/Gehring, Thomas: Institutional Interaction. Ten Years of Scholarly Development, in: Sebastian Oberthür/Olav Schram Stokke (Hrsg.), Managing Institutional Complexity: Regime Interplay and Global Environmental Change, Cambridge (Mass.) 2011, S. 25–58.

Odendahl, Kerstin/Giegerich, Thomas (Hrsg.): Räume im Völker- und Europarecht, Berlin 2014.

Odermatt, Jed: The European Union as a Cybersecurity Actor, in: Steven Blockmans/Panos Koutrakos (Hrsg.), Research Handbook on the EU's Common Foreign and Security Policy, Cheltenham 2018, S. 354–373.

Offe, Claus: Technik und Eindimensionalität. Eine Version der Technokratiethese?, in: Jürgen Habermas (Hrsg.), Antworten auf Herbert Marcuse, Frankfurt a. M. 1968, S. 73–85.

Office of the Director of National Intelligence: A Guide to Cyber Attribution, 14.9. 2018, https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf.

Oftinger, Karl: Punktationen für eine Konfrontation der Technik mit dem Recht, in: Festschrift der Rechts- und Staatswissenschaftlichen Fakultät der Universität Zürich zum Zentenarium des Schweizerischen Juristenvereins, Zürich 1961, S. 1–34.

–: Konfrontation der Technik mit dem Recht, in: Hans Freyer/Johannes Chr. Papalekas/Georg Weippert (Hrsg.), Technik im technischen Zeitalter, Düsseldorf 1965, S. 248–270

Ogus, Anthony: Regulation. Legal Form and Economic Theory, Oxford u. a. 2004.

Ohler, Christoph: Die Kollisionsordnung des Allgemeinen Verwaltungsrechts. Strukturen des deutschen Internationalen Verwaltungsrechts, Tübingen 2005.

Opitz, Sven: Zwischen Sicherheitsdispositiv und Securitization: Zur Analytik illiberaler Gouvernementalität, in: Patricia Purtschert/Katrin Mayer/Yves Winter (Hrsg.), Gouvernementalität und Sicherheit. Zeitdiagnostische Beiträge im Anschluss an Foucault, Bielefeld 2008, S. 201–228.

Orator, Andreas: Möglichkeiten und Grenzen der Einrichtung von Unionsagenturen, Tübingen 2017.

Orsini, Amandine/Morin, Jean-Frédéric/Young, Oran: Regime Complexes: A Buzz, a Boom, or a Boost for Global Governance?, Global Governance 19 (2013), S. 27–39.

Ossenbühl, Fritz: Die Not des Gesetzgebers im naturwissenschaftlich-technischen Zeitalter, Wiesbaden 2000.

Ossenbühl, Fritz: Autonome Rechtsetzung der Verwaltung, in: Josef Isensee/Paul Kirchhof (Hrsg.), Handbuch des Staatsrechts, Bd. V, 3. Aufl. 2007, § 104.

Oster, Jan: Internationale Zuständigkeit und anwendbares Recht im Datenschutz, ZEuP 2021, S. 275–306.

Paal, Boris: Sanktion durch behördliche Öffentlichkeitsinformation – eine datenschutzrechtliche Betrachtung, K&R 2020, S. 8–13.

Paal, Boris/Pauly, Daniel (Hrsg.): DS-GVO, 3. Aufl. 2021.

Paefgen, Franziska: Der von Art. 8 EMRK gewährleistete Schutz vor staatlichen Eingriffen in die Persönlichkeitsrechte im Internet, Berlin u. a. 2017.

Pahlow, Louis: Industrialisierung als Staatsaufgabe. Zum Verhältnis von Wirtschaft und Staat im Staatsrecht des Vormärz, Rechtsgeschichte 15 (2009), S. 109–125.

Park, Byungwoog: Wandel des klassischen Polizeirechts zum neuen Sicherheitsrecht. Eine Untersuchung am Beispiel der Entscheidung über sogenannte Online-Durchsuchungen, Berlin 2013.

Park, Sangchul: Why Information Security Law Has Been Ineffective in Addressing Security Vulnerabilities: Evidence from California Data Breach Notifications and Relevant Court and Government Records, International Review of Law and Economics 58 (2019), S. 132–145.

Pearce, Katy E.: Democratizing kompromat. The Affordances of Social Media for State-sponsored Harassment, Information, Communication & Society 18:10 (2015), S. 1158–1174.

Peine, Franz-Josef: Gerätesicherheitsrecht, in: Martin Schulte/Rainer Schröder (Hrsg.), Handbuch des Technikrechts, Berlin u. a. 2011, S. 405–454.

Pernice, Ingolf: Global Cybersecurity Governance. A Constitutionalist Analysis, Global Constitutionalism (2018), S. 112–141.
Peters, Anne: Wettbewerb von Rechtsordnungen, in: VVDStRL 69 (2010), S. 7–56.
–: The Refinement of International Law: From Fragmentation to Regime Interaction and Politicization, I•CON 15 (2017), S. 671–704.
Peters, Benjamin: How Not to Network a Nation. The Uneasy History of the Soviet Internet, Cambridge (Mass.) 2016.
Petrlic, Ronald: HTTPS im Lichte der DSGVO, DuD 2018, S. 691–693.
Peuker, Enrico: Verfassungswandel durch Digitalisierung. Digitale Souveränität als verfassungsrechtliches Leitbild, Tübingen 2020.
Pfefferkorn, Riana: The EARN IT Act is back, and it's more dangerous than ever, 4.2. 2022, http://cyberlaw.stanford.edu/blog/2022/02/earn-IT-act-back-and-it's-more-dangerous-ever.
Pfister, Patrick: Regimekomplexe. Neue Kooperationsformen zur Regulierung globaler Risiken, Frankfurt a. M. 2012.
Pistorius, Boris: Föderalismus und Cybersicherheit: Plädoyer für eine moderne Cybersicherheitsarchitektur, in: Jahrbuch des Föderalismus 2018, S. 74–87.
Pitschas, Rainer: Allgemeines Verwaltungsrecht als Teil der öffentlichen Informationsordnung, in: Wolfgang Hoffmann-Riem/Eberhard Schmidt-Aßmann/Gunnar Folke Schuppert (Hrsg.), Reform des Allgemeinen Verwaltungsrechts, Baden-Baden 1993, S. 219–306.
–: Technikentwicklung und -implementierung als rechtliches Steuerungsproblem. Von der administrativen Risikopotentialanalyse zur Innovationsfunktion des Technikrechts, in: Michael Kloepfer (Hrsg.), Technikentwicklung und Technikrechtsentwicklung, Berlin 2000, S. 73–102.
–: Polizeirecht im kooperativen Staat. Der Schutz innerer Sicherheit zwischen Gefahrenabwehr und kriminalpräventiver Risikovorsorge, in: Rainer Pitschas (Hrsg.), Kriminalprävention und „Neues Polizeirecht" – Zum Strukturwandel des Verwaltungsrechts in der Risikogesellschaft, Berlin 2002, S. 241–268.
Plischka, Hans Peter: Technisches Sicherheitsrecht. Die Probleme des technischen Sicherheitsrechts, dargestellt am Recht der überwachungsbedürftigen Anlagen (§ 24 GewO), 1969.
Podlech, Adalbert: Verfassungsrechtliche Probleme öffentlicher Datenbanken, DÖV 1970, S. 473–475.
–: Verfassungsrechtliche Probleme öffentlicher Informationssysteme, Datenverarbeitung im Recht 1 (1972), S. 149–169.
–: Datenschutz im Bereich der öffentlichen Verwaltung. Beiheft 1, Datenverarbeitung im Recht, Berlin 1973.
Poelzig, Dörte: Normdurchsetzung durch Privatrecht, Tübingen 2012.
Pohle, Jörg: Datenschutz und Technikgestaltung, Diss. HU Berlin 2018.
Pohlmann, Kristine: Bundeskompetenzen im Bevölkerungsschutz, in: Hans-Jürgen Lange/Christian Endreß/Michaela Wendekamm (Hrsg.), Versicherheitlichung des Bevölkerungsschutzes, Wiesbaden 2013, S. 249–266.
Pollicino, Oreste/Bassini, Marco: The law of the Internet between globalisation and localisation, in: Miguel Maduro/Kaarlo Tuori/Suvi Sankari (Hrsg.), Transnational Law. Rethinking European Law and Legal Thinking, 2014, S. 346–380.
Poscher, Ralf: Grundrechte als Abwehrrechte. Reflexive Regelung rechtlich geordneter Freiheit, Tübingen 2003.

–: Das Verfassungsrecht vor den Herausforderungen der Globalisierung, in: VVDStRL 67 (2008), S. 163–192.
–: Eingriffsschwellen im Recht der inneren Sicherheit. Ihr System im Licht der neueren Verfassungsrechtsprechung, DV 41 (2008), S. 345–374.
–: Sicherheitsverfassungsrecht im Wandel, in: Thomas Vesting/Stefan Korioth (Hrsg.), Der Eigenwert des Verfassungsrechts, 2011, S. 245–262.
–: Die Zukunft der informationellen Selbstbestimmung als Recht auf Abwehr von Grundrechtsgefährdungen, in: Hans-Helmuth Gander/Walter Perron et al. (Hrsg.), Resilienz in der offenen Gesellschaft, Baden-Baden 2012, S. 167–190.
–: Sicherheitsverfassungsrecht im Wandel, in: Christopher Daase/Stefan Engert/Georgios Kolliarakis (Hrsg.), Politik und Unsicherheit – Strategien in einer sich wandelnden Sicherheitskultur, Frankfurt a. M. u. a. 2014, S. 165–187.
Poscher, Ralf/Buchheim, Johannes: Staatsaufsicht und Datenschutz. Ein letzter weißer Fleck auf der datenschutzrechtlichen Landkarte?, DVBl. 2015, S. 1273–1282.
Poscher, Ralf/Lassahn, Philipp: Verfassungsrechtliche Dimensionen der IT-Sicherheit, in: Gerrit Hornung/Martin Schallbruch (Hrsg.), IT-Sicherheitsrecht, Baden-Baden 2021, § 7.
Post, David: Governing Cyberspace, Wayne L. Rev. 43 (1996), S. 155–171.
Pozen, David E.: Deep Secrecy, Stan. L. Rev. 62 (2010), S. 257–340.
Preuß, Ulrich K.: Risikovorsorge als Staatsaufgabe, in: Dieter Grimm (Hrsg.), Staatsaufgaben, Baden-Baden 1994, S. 523–551.
Pünder, Hermann: Zertifizierung und Akkreditierung. Private Qualitätskontrolle unter staatlicher Gewährleistungsverantwortung, ZHR 170 (2006), S. 567–598.
Raab, Charles D./De Hert, Paul: Tools for Technology Regulation: Seeking Analytical Approaches Beyond Lessig and Hood, in: Roger Brownsword/Karen Yeung (Hrsg.), Regulating Technologies. Legal Futures, Regulatory Frames and Technological Fixes, Oxford 2008, S. 263–285.
Rabin, Robert L.: Federal Regulation in Historical Perspective, Stan. L. Rev. 38 (1986), S. 1189–1326.
Rachor, Frederik/Roggan, Fredrik: Organisation der Sicherheitsbehörden und Geheimdienste in Deutschland, in: Lisken/Denninger, HdbPolR, 7. Aufl. 2021, Kap. C.
Rademacher, Timo: Predictive Policing im deutschen Polizeirecht, AöR 142 (2017), S. 366–416.
–: Wenn neue Technologien altes Recht durchsetzen: Dürfen wir es unmöglich machen, rechtswidrig zu handeln?, JZ 74 (2019), S. 702–710.
Rademacher, Timo/Perkowski, Lennart: Staatliche Überwachung, neue Technologien und die Grundrechte, JuS 2020, S. 713–720.
Radkau, Joachim: Technik in Deutschland. Vom 18. Jahrhundert bis heute, 2. Aufl. Frankfurt a. M. 2008.
Radu, Roxana/Chenou, Jean-Marie/Weber, Rolf H. (Hrsg.): The Evolution of Global Internet Governance. Principles and Policies in the Making, Zürich 2014.
Rafsendjanim, Mansur Pour/Bomhard, David: IT-Sicherheit im Zivilrecht und in der Vertragsgestaltung, in: Gerrit Hornung/Martin Schallbruch (Hrsg.), IT-Sicherheitsrecht, Baden-Baden 2021, § 9.
Ralston, William: The untold story of a cyberattack, a hospital and a dying woman, Wired, 11.11.2020, https://www.wired.co.uk/article/ransomware-hospital-death-germany.
Ramsay, Stephen: Reading Machines. Toward an Algorithmic Criticism, Urbana 2011.

Rapp, Friedrich: Analytische Technikphilosophie, Freiburg u. a. 1978.
Rapp, Friedrich/Ropohl, Günter: Historische und systematische Übersicht, in: Christoph Hubig/Alois Huning/Günter Ropohl (Hrsg.), Nachdenken über Technik. Die Klassiker der Technikphilosophie und neuere Entwicklungen, 3. Aufl. 2013, S. 41–52.
Rat der Europäischen Union: Entschließung zur Verschlüsselung: Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung, 13084/1/20 REV 1, 24.11.2020.
Rattray, Gregory: Strategic Warfare in Cyberspace, Cambridge (Mass.) 2001.
Räuker, Kaya/Dombert, Matthias: Am Beispiel der deutschen Sicherheitsarchitektur: Zum Grundrechtsschutz durch Organisation, DÖV 2014, S. 414–420.
Raustiala, Kal: Governing The Internet, AJIL 110 (2017), S. 491–503.
Reiberg, Abel: Netzpolitik. Genese eines Politikfeldes, Baden-Baden 2018.
Reich, Johannes: Regulierung, Regulierungsrecht und Regulatory State – Rechtsdogmatische Potenziale des Regulierungsbegriffs in verwaltungsrechtsvergleichender, rechtshistorischer und sozialwissenschaftlicher Perspektive, Forum Historiae Iuris v. 22.5.2013, http://www.forhistiur.de/it/2013–05-reich.
Reichert, Johannes: Der Schutz des Kernbereichs privater Lebensgestaltung in den Polizeigesetzen des Bundes und der Länder, Tübingen 2015.
Reimer, Ekkehart: Der Ort des Unterlassens. Die ursprungsbezogene Behandlung von Entgelten für Untätigkeit im internationalen Steuerrecht, München 2004.
Renner, Moritz: Zwingendes transnationales Recht. Zur Struktur der Wirtschaftsverfassung jenseits des Staates, Baden-Baden 2011.
Repasi, René: Das Recht des Raums der Freiheit, der Sicherheit und des Rechts, in: Armin Hatje/Peter-Christian Müller-Graff (Hrsg.), Europäisches Organisations- und Verfassungsrecht (Enzyklopädie Europarecht), Bd. 1, 2. Aufl. Baden-Baden 2022, § 10.
Reuter, Markus: EU will eigenen DNS-Server mit Filterlisten und Netzsperren, Netzpolitik.org v. 24.1.2022, https://netzpolitik.org/2022/dns4eu-eu-will-eigenen-dns-server-mit-filterlisten-und-netzsperren/.
–: Europas digitale Bürgerrechtsorganisationen gegen neue Form der Massenüberwachung, Netzpolitik.org v. 17.3.2022, https://netzpolitik.org/2022/chatkontrolle-europas-digitale-buergerrechtsorganisationen-gegen-neue-form-der-massenueberwachung/.
Reyngaert, Cedric: Jurisdiction in International Law, 2. Aufl. Oxford 2015.
Richter, Frederick: Zertifizierung unter der DS-GVO, ZD 2020, S. 84–87.
Rid, Thomas: Cyber War Will Not Take Place, Journal of Strategic Studies 35:1 (2012), S. 5–32.
Rid, Thomas/Buchanan, Benjamin: Attributing Cyber Attacks, Journal of Strategic Studies 38 (2015), S. 4–37.
Riedl, Jasmin: Innere Sicherheit in Wahlkampfzeiten: Ein Garant für Zentralisierungsforderungen der Bundesparteien, in: Jahrbuch des Föderalismus 2017, S. 221–237.
–: Entwicklungslinien der Politik Innerer Sicherheit in Deutschland, in: Jahrbuch des Föderalismus 2018, S. 37–50.
Riehm, Thomas/Meier, Stanislaus: Rechtliche Durchsetzung von Anforderungen an die IT-Sicherheit. Behörden, Private und Verbände in der Gesamtverantwortung, MMR 2020, S. 571–576.
Riescher, Gisela: Resilienz. Demokratietheoretische Überlegungen zu einem neuen Sicherheitskonzept, in: Dirk Heckmann/Ralf P. Schenke/Gernot Sydow (Hrsg.), Verfassungsstaatlichkeit im Wandel. Festschrift für Thomas Würtenberger, Berlin 2013, S. 1067–1078.

Ringen, Stein: The Perfect Dictatorship: China in the 21st Century, Hong Kong 2016.
Ritter, Steve (Hrsg.): Die Weiterentwicklung des IT-Sicherheitsgesetzes, Frankfurt a. M. 2022.
Ritter, Steve/Schulte, Laura: Rechtliche Anforderungen an Anbieter digitaler Dienste, die zugleich kritische Infrastrukturen sind: Zur Mindest- und Vollharmonisierung durch die NIS-Richtlinie, CR 2019, S. 617–624.
Robbers, Gerhard: Sicherheit als Menschenrecht. Aspekte der Geschichte, Begründung und Wirkung einer Grundrechtsfunktion, Baden-Baden 1987.
Rockstroh, Sebastian/Peschel, Christopher: Sicherheitslücken als Mangel, NJW 2020, S. 3345–3350.
Roggan, Fredrik: Die strafprozessuale Quellen-TKÜ und Online-Durchsuchung: Elektronische Überwachungsmaßnahmen mit Risiken für Beschuldigte und die Allgemeinheit, StV 2017, S. 821–828.
Roguski, Przemysław: An Inspection Regime for Cyber Weapons: A Challenge Too Far?, AJIL Unbound 115 (2021), S. 111–115.
Röhl, Hans Christian: Soll das Recht der Regulierungsverwaltung übergreifend geregelt werden?, JZ 61 (2006), S. 831–839.
–: Internationale Standardsetzung, in: Christoph Möllers/Andreas Voßkuhle/Christian Walter (Hrsg.), Internationales Verwaltungsrecht – Eine Analyse anhand von Referenzgebieten, Tübingen 2007, S. 319–344.
– (Hrsg.): Wissen – Zur kognitiven Dimension des Rechts Berlin 2010.
Romanosky, Sasha: Examining the costs and causes of cyber incidents, Journal of Cybersecurity 2:2 (2016), S. 121–135.
Romanosky, Sasha/Boudreaux, Benjamin: Private-Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government, International Journal of Intelligence and CounterIntelligence 34 (2021), S. 463–493.
Rönne, Ludwig von: Das Staatsrecht der preußischen Monarchie, Bd. 2: Das Verwaltungs-Recht, Leipzig 1863.
Roos, Philipp: Das IT-Sicherheitsgesetz – Wegbereiter oder Tropfen auf den heißen Stein, MMR 2015, S. 636–645.
Ropohl, Günter: Allgemeine Technologie. Eine Systemtheorie der Technik, 3. Aufl. Karlsruhe 2009.
Roscini, Marco: Cyber Operations and the Use of Force in International Law, Oxford 2014.
Rossen-Stadtfeld, Helge: Kontrollfunktion der Öffentlichkeit – ihre Möglichkeiten und ihre rechtlichen Grenzen, in: Eberhard Schmidt-Aßmann/Wolfgang Hoffmann-Riem (Hrsg.), Verwaltungskontrolle, Baden-Baden 2001, S. 117–204.
Rössler, Beate: Der Wert des Privaten, Frankfurt a. M. 2001.
Roßnagel, Alexander: Bedroht die Kernenergie unsere Freiheit?, 2. Aufl. München 1983.
–: Radioaktiver Zerfall der Grundrechte?, München 1984.
–: Rechtswissenschaftliche Technikfolgenforschung. Umrisse einer Forschungsdisziplin, Baden-Baden 1993.
–: Das De-Mail-Gesetz – Grundlage für mehr Rechtssicherheit im Internet, NJW 2011, S. 1473–1477.
–: Das IT-Sicherheitsgesetz, DVBl. 2015, S. 1206–1212.
–: Das Vertrauensdienstegesetz. Neue Regelungen zur Anpassung des deutschen Rechts an die EU-eIDAS-VO, MMR 2018, S. 31–35.

–: IT-Sicherheitsinfrastrukturen und -dienste, in: Gerrit Hornung/Martin Schallbruch (Hrsg.), IT-Sicherheitsrecht, Baden-Baden 2021, § 14.
Roßnagel, Alexander/Bizer, Johann: Sicherheit in der Informationstechnik. Aufgabe für ein neues Bundesamt, Kritische Justiz 23 (1990), S. 436–448.
Roßnagel, Alexander/Bizer, Johann et al.: Ein Bundesamt für die Sicherheit in der Informationstechnik. Kritische Bemerkungen zum Gesetzentwurf der Bundesregierung, DuD 14 (1990), S. 178–186.
Roßnagel, Alexander/Wedde, Peter et al.: Digitalisierung der Grundrechte? Zur Verfassungsverträglichkeit der Informations- und Kommunikationstechnik, Wiesbaden 1990.
Roth, Alexander: EncroChat und kein Ende – Die Verwendung von „Fertig-Beweismitteln" ausländischer Herkunft im deutschen Strafprozess, GSZ 2021, S. 238–248.
Röthel, Anne: Europarechtliche Vorgaben für das Technikrecht, in: Martin Schulte/Rainer Schröder (Hrsg.), Handbuch des Technikrechts, Berlin u. a. 2011, S. 201–236.
Rottleuthner, Hubert: Rechtswissenschaft als Sozialwissenschaft, Frankfurt a. M. 1973.
Rottmeier, Christian: Kernbereich privater Lebensgestaltung und strafprozessuale Lauschangriffe, Tübingen 2017.
Ruffert, Matthias: Regulierung im System des Verwaltungsrechts, AöR 124 (1999), S. 237–281.
–: Die Globalisierung als Herausforderung an das Öffentliche Recht, Stuttgart u. a. 2004.
–: The Transformation of Administrative Law as a Transnational Methodological Project, in: Matthias Ruffert (Hrsg.), The Transformation of Administrative Law in Europe, Munich 2007, S. 3–52.
–: Verselbständigte Verwaltungseinheiten: Ein europäischer Megatrend im Vergleich, in: Hans-Heinrich Trute/Thomas Groß et al. (Hrsg.), Allgemeines Verwaltungsrecht – zur Tragfähigkeit eines Konzepts, Tübingen 2008, S. 431–460.
–: Begriff, in: Michael Fehling/Matthias Ruffert (Hrsg.), Regulierungsrecht, Tübingen 2010, § 7.
–: Die neue Unabhängigkeit: Zur demokratischen Legitimation von Agenturen im europäischen Verwaltungsrecht, in: Peter-Christian Müller-Graff/Stefanie Schmahl/Vassilios Skouris (Hrsg.), Europäisches Recht zwischen Bewährung und Wandel. Festschrift für Dieter H. Scheuing, Baden-Baden 2011, S. 399–414.
–: Grundfragen der Wirtschaftsregulierung, in: Dirk Ehlers/Michael Fehling/Hermann Pünder (Hrsg.), Besonderes Verwaltungsrecht, Bd. 1, 4. Aufl. Heidelberg 2019, S. 835–859.
Rusteberg, Benjamin: Zivile Sicherheit in der Sicherheitsarchitektur des deutschen Bundesstaates, in: Christoph Gusy/Dieter Kugelmann/Thomas Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, Berlin u. a. 2017, S. 113–136.
–: Wissensgenerierung in der personenbezogenen Prävention – Zwischen kriminalistischer Erfahrung und erkenntnistheoretischer Rationalität, in: Laura Münkler (Hrsg.), Dimensionen des Wissens im Recht, Tübingen 2019, S. 233–264.
Ryngaert, Cedric/Taylor, Mistale: The GDPR as Global Data Protection Regulation?, AJIL Unbound 114 (2020), S. 5–9.
Sabel, Charles/Simon, William: Minimalism and Experimentalism in the Administrative State, Georgetown LJ 100 (2011), S. 53–93.
Sachs, Michael: Abwehrrechte, in: K. Stern, Das Staatsrecht der Bundesrepublik Deutschland, Bd. III/1, München 1988, § 66.

–: Abwehrrechte, in: Detlef Merten/Hans-Jürgen Papier (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa, Bd. 2, 2006, § 39.
– (Hrsg.): Grundgesetz: Kommentar, 9. Aufl., München 2021.
Sachs, Michael/Krings, Thomas: Das neue „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme", JuS 2008, S. 481–486.
Sales, Nathan Alexander: Regulating Cyber-Security, Nw. U. L. Rev. 107 (2013), S. 1503–1568.
–: Privatizing Cybersecurity, UCLA L. Rev. Discourse 65 (2018), S. 620–689.
Sanger, David E./Barnes, Julian E./Perlroth, Nicole: White House Weighs New Cybersecurity Approach After Failure to Detect Hacks, 15.3.2021, https://www.nytimes.com/2021/03/14/us/politics/us-hacks-china-russia.html.
Santamarta, Ruen: SATCOM terminals under attack in Europe. A plausible analysis, 7.3.2022, https://www.reversemode.com/2022/03/satcom-terminals-under-attack-in-europe.html.
Saurer, Johannes: Die Errichtung von Europäischen Agenturen auf Grundlage der Binnenmarktharmonisierungskompetenz des Art. 114 AEUV, DÖV 2014, S. 549–555.
Schallbruch, Martin: IT-Sicherheitsrecht – Schutz kritischer Infrastrukturen und staatlicher IT-Systeme, Zur Entwicklung des IT-Sicherheitsrechts in der 18. Wahlperiode (Teil 1), CR 2017, S. 648–656.
–: IT-Sicherheitsrecht – Schutz digitaler Dienste, Datenschutz und Datensicherheit (Folge 2), CR 2017, S. 798–804.
–: IT-Sicherheitsrecht – Abwehr von IT-Angriffen, Haftung und Ausblick. Zur Entwicklung des IT-Sicherheitsrechts in der 18. Wahlperiode (Folge 3), CR 2018, S. 215–224.
–: Das IT-Sicherheitsgesetz 2.0 – neue Regeln für Unternehmen und IT-Produkte. Neue Rechtslage im IT-Sicherheitsrecht (Teil I), CR 2021, S. 450–458.
–: Das IT-Sicherheitsgesetz 2.0 – Befugnisse des BSI und Schutz der Bundesverwaltung. Neue Rechtslage im IT-Sicherheitsrecht (Teil II), CR 2021, S. 516–523.
Schardt, Marc: Öffentliche Verwaltung, in: Gerrit Hornung/Martin Schallbruch (Hrsg.), IT-Sicherheitsrecht, Baden-Baden 2021, § 25.
Scharpf, Fritz W.: Optionen des Föderalismus in Deutschland und Europa, Frankfurt a. M. 1994.
Scharpf, Fritz W./Reissert, Bernd/Schnabel, Fritz: Politikverflechtung: Theorie und Empirie des kooperativen Föderalismus in der Bundesrepublik, Kronberg i. Ts. 1976.
Schelsky, Helmut: Der Mensch in der wissenschaftlichen Zivilisation, Köln u. a. 1961.
Schemmel, Jakob: Die demokratische Weisung – Geschichte und europäischer Vergleich eines Konzepts deutscher Verwaltungslegitimation, in: Eva Ellen Wagner/et al. (Hrsg.), Pfadabhängigkeit hoheitlicher Ordnungsmodelle, Baden-Baden 2016, S. 155–172.
–: Europäische Finanzmarktverwaltung: Dogmatik und Legitimation der Handlungsinstrumente von EBA, EIOPA und ESMA, Tübingen 2018.
Scherzberg, Arno: Risikosteuerung durch Verwaltungsrecht: Ermöglichung oder Begrenzung von Innovationen?, in: VVDStRL 63 (2004), S. 214–263.
–: Innovationen und Recht. Zum Stand der rechtswissenschaftlichen Innovationsforschung, in: W. Hoffmann-Riem, Offene Rechtswissenschaft, 2010, S. 273–308.
–: Öffentlichkeitskontrolle, in: Wolfgang Hoffmann-Riem/Eberhard Schmidt-Aßmann/Andreas Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. 3, 2. Aufl. München 2012, § 49.

Schewe, Christoph: Das Sicherheitsgefühl und die Polizei, Berlin 2009.
Schiff Berman, Paul: Global Legal Pluralism. A Jurisprudence of Law Beyond Borders, Cambridge u. a. 2012.
–: Understanding Global Legal Pluralism: From Local to Global, from Descriptive to Normative, in: Paul Schiff Berman (Hrsg.), The Oxford Handbook of Global Legal Pluralism, Oxford 2020, S. 1–36.
Schläger, Uwe/Thode, Jan-Christoph (Hrsg.): Handbuch Datenschutz und IT-Sicherheit, Berlin 2022.
Schlegel, Arndt: Normative Grenzen für internetbasierte Ermittlungsmethoden. Zugleich ein Beitrag zur Technikoffenheit strafprozessualer Ermächtigungsgrundlagen, Wiesbaden 2019.
Schlink, Bernhard: Die Bewältigung der wissenschaftlichen und technischen Entwicklungen durch das Verwaltungsrecht, in: VVDStRL 48 (1990), S. 235–264.
Schmahl, Stefanie: Zwischenstaatliche Kompetenzabgrenzung im Cyberspace, AVR 47 (2009), S. 284–327.
–: Cybersecurity, in: Nina Dethloff/Georg Nolte/August Reinisch (Hrsg.), Freiheit und Regulierung in der Cyberwelt, Heidelberg 2016, S. 159–196.
Schmalenbach, Kirsten: Völker- und unionsrechtliche Anstöße zur Entterritorialisierung des Rechts, in: VVDStRL 76 (2017), S. 245–276.
Schmid, Alexander: IT- und Rechtssicherheit automatisierter und vernetzter cyberphysischer Systeme. Event Data Recording und integrierte Produktbeobachtung als Maßnahmen der IT-Risikominimierung am Beispiel automatisierter und vernetzter Luft- und Straßenfahrzeuge, Berlin 2019.
Schmidt, Reiner: Staatliche Verantwortung für die Wirtschaft, in: Josef Isensee/Paul Kirchhof (Hrsg.), Handbuch des Staatsrechts, Bd. IV, 3. Aufl. 2006, § 92.
Schmidt-Aßmann, Eberhard: Regulierte Selbstregulierung und verwaltungsrechtliche Systembildung, DV Beiheft 4 (2001), S. 253–271.
–: Das allgemeine Verwaltungsrecht als Ordnungsidee. Grundlagen und Aufgaben der verwaltungsrechtlichen Systembildung, 2. Aufl. Berlin u. a. 2006.
–: Principles of an International Order of Information, in: Gordon Anthony/Jean-Bernard Auby et al. (Hrsg.), Values in Global Administrative Law, Oxford 2011, S. 117–124.
Schmidt-Bleibtreu, Bruno (Begr.)/*Hofmann, Hans/Henneke, Hans-Günter* (Hrsg.): GG – Grundgesetz: Kommentar, 15. Aufl. Köln 2022.
Schmidt-Preuß, Matthias: Verwaltung und Verwaltungsrecht zwischen gesellschaftlicher Selbstregulierung und staatlicher Steuerung, in: VVDStRL 56 (1997), S. 160–234.
–: Private technische Regelwerke. Rechtliche und politische Fragen, in: Michael Kloepfer (Hrsg.), Selbst-Beherrschung im technischen und ökologischen Bereich, 1998, S. 89–101.
–: Technikermöglichung durch Recht, in: Michael Kloepfer (Hrsg.), Kommunikation – Technik – Recht, 2002, S. 175–202.
–: Europäische und internationale Ansätze zum Schutz kritischer IT- und Energie-Infrastrukturen, in: Michael Kloepfer (Hrsg.), Schutz kritischer Infrastrukturen, Baden-Baden 2010, S. 67–84.
Schmidt-Radefeldt, Roman: Rechtsdurchsetzung mit militärischen Mitteln – Inlandseinsätze der Armee und Militarisierung der Polizei. Landesbericht Deutschland, in: Uwe Kischel/Sebastian Graf von Kielmansegg (Hrsg.), Rechtsdurchsetzung mit militärischen Mitteln, 2018, S. 1–56.

Schmitt, Carl: Das Zeitalter der Neutralisierungen und Entpolitisierungen (1929), in: ders., Positionen und Begriffe, 4. Aufl. Berlin 2014, S. 138–150.
Schmitt, Michael N.: Cybersecurity and International Law, in: Robin Geiß/Nils Melzer (Hrsg.), The Oxford Handbook of the International Law of Global Security, Oxford 2021, S. 661–678
– (Hrsg.): Tallinn Manual on the International Law Applicable to Cyber Warfare. Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge u. a. 2013.
– (Hrsg.): Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge 2017.
Schmitt, Michael N./Vihul, Liis: International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms, Just Security v. 30.6.2017, www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.
Schmitz, Sandra/Schiffner, Stefan: Responsible Vulnerability Disclosure under the NIS 2.0 Proposal, JIPITEC 12 (2021), S. 447–457.
Schmoeckel, Mathias: Dauerhaft engpassfreie Märkte durch «Regulierung»? Erfolgsgeschichte eines Begriffs, Forum Historiae Iuris v. 6.2.2009, https://forhistiur.net/2009–02-schmoeckel/?l=de.
Schneider, Bastian: Fernmeldegeheimnis und Fernmeldeaufklärung, Berlin 2020.
Schneider, Florian: Meldepflichten im IT-Sicherheitsrecht. Datenschutz, Kritische Infrastrukturen und besondere IT-Dienste, Baden-Baden 2017.
Schneider, Gerhard J. A.: Some Thoughts on Harming Privacy by Protecting Critical Infrastructures, in: Hans-Helmuth Gander/Walter Perron et al. (Hrsg.), Resilienz in der offenen Gesellschaft, Baden-Baden 2012, S. 133–137.
Schneider, Jens-Peter: Regulation and Europeanisation as Key Patterns of Change in Administrative Law, in: Matthias Ruffert (Hrsg.), The Transformation of Administrative Law in Europe, Munich 2007, S. 309–323.
–: Stand und Perspektiven des Europäischen Datenverkehrs- und Datenschutzrechts, DV 44 (2011), S. 499–524.
–: Informationssysteme als Bausteine des Europäischen Verwaltungsverbunds, NVwZ 2012, S. 65–70.
–: Amtshilfe und Informationsmanagement als Gegenstände der Bücher V und VI des ReNEUAL-Musterentwurfs, in: Jens-Peter Schneider/Klaus Rennert/Nikolaus Marsch (Hrsg.), ReNEUAL Musterentwurf für ein EU-Verwaltungsverfahrensrecht – Tagungsband, München 2016, S. 197–208.
–: Information exchange and its problems, in: Carol Harlow/Päivi Leino/Giacinto della Cananea (Hrsg.), Research Handbook on EU Administrative Law, Cheltenham 2017, S. 81–112.
Schneider, Volker/Janning, Frank: Politikfeldanalyse. Akteure, Diskurse und Netzwerke in der öffentlichen Politik, 2006.
Schneier, Bruce: There's No Real Difference Between Online Espionage and Online Attack, The Atlantic, 6.3.2014, https://www.theatlantic.com/technology/archive/2014/03/theres-no-real-difference-between-online-espionage-and-online-attack/284233.
–: Simultaneous discovery of vulnerabilities, 2016, https://www.schneier.com/blog/archives/2016/02/simultaneous_di.html.
Schober, Konrad: Europäische Polizeizusammenarbeit zwischen TREVI und Prüm. Mehr Sicherheit auf Kosten von Freiheit und Recht?, Heidelberg 2017.

Schoch, Friedrich: Diskussionsbemerkung, in: VVDStRL 73 (2014), S. 431.
–: Abschied vom Polizeirecht des liberalen Rechtsstaats? – Vom Kreuzberg-Urteil des Preußischen Oberverwaltungsgerichts zu den Terrorismusbekämpfungsgesetzen unserer Tage, Der Staat 43 (2004), S. 347–369.
–: Die Unverletzlichkeit der Wohnung nach Art. 13 GG, JURA 2010, S. 22–31.
Schöndorf-Haubold, Bettina: Netzwerke in der deutschen und europäischen Sicherheitsarchitektur, in: Sigrid Boysen/Ferry Bühring et al. (Hrsg.), Netzwerke, Baden-Baden 2007, S. 149–170.
–: Europäisches Sicherheitsverwaltungsrecht, Baden-Baden 2010.
–: Auf dem Weg zum Sicherheitskooperationsrecht?, in: Jan-Hendrik Dietrich/Klaus Ferdinand Gärditz et al. (Hrsg.), Nachrichtendienste in vernetzter Sicherheitsarchitektur, Tübingen 2020, S. 3–33.
–: Europäisches Sicherheitsrecht, in: Dirk Ehlers/Michael Fehling/Hermann Pünder (Hrsg.), Besonderes Verwaltungsrecht, 4. Aufl. Heidelberg 2021, § 68.
–: Europäisches Polizei- und Sicherheitsrecht, in: Jörg Philipp Terhechte (Hrsg.), Verwaltungsrecht der Europäischen Union, Baden-Baden 2022, § 35.
Schreiber, Kristina/Esser, Julia: Einheitliche Update-Zyklen im Spannungsfeld der §§ 327f, 327r BGB, RDi 2022, S. 317–323.
Schroeder, Friedrich-Christian: An der Unterkante des Rechts, JZ 65 (2010), S. 361.
Schröder, Markus: Der risikobasierte Ansatz in der DS-GVO. Risiko oder Chance für den Datenschutz?, ZD 2019, S. 503–506.
Schröder, Meinhard: Die Bereiche der Regierung und der Verwaltung, in: Josef Isensee/Paul Kirchhof (Hrsg.), Handbuch des Staatsrechts, Bd. V, 3. Aufl. 2007, § 106.
Schröder, Rainer: Verfassungsrechtliche Rahmenbedingungen des Technikrechts, in: Martin Schulte/Rainer Schröder (Hrsg.), Handbuch des Technikrechts, Berlin u. a. 2011, S. 237–280.
Schucht, Carsten: Safety & Security bei smarten Produkten. Weichenstellungen zur IT-Sicherheit durch den Ausschuss für Produktsicherheit, NVwZ 2021, S. 532–535.
Schulenberg, Sebastian: Der Schutz des Kernbereichs privater Lebensgestaltung bei heimlichen staatlichen Überwachungsmaßnahmen, in: Fabian Scheffczyk/Kathleen Wolter (Hrsg.), Linien der Rechtsprechung des Bundesverfassungsgerichts IV, 2017, S. 123–171.
Schulte, Laura/Wambach, Tim: Zielkonflikte zwischen Datenschutz und IT-Sicherheit im Kontext der Aufklärung von Sicherheitsvorfällen, DuD 2020, S. 462–468.
Schulte, Martin: Technikssteuerung durch Technikrecht – rechtsrealistisch betrachtet, in: Klaus Vieweg (Hrsg.), Technikssteuerung und Recht, Köln 2000, S. 23–34.
–: Wissensgenerierung im Technikrecht, in: Indra Spiecker gen. Döhmann/Peter Collin (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, Tübingen 2008, S. 259–269.
Schulte, Martin/Schröder, Rainer (Hrsg.): Handbuch des Technikrechts, 2. Aufl. Berlin u. a. 2011.
Schulz, Sönke E.: Die „Datenautobahn" als Infrastruktur: Gewährleistungs- und Verkehrssicherungspflichten des Staates, in: Hermann Hill/Utz Schliesky (Hrsg.), Die Vermessung des virtuellen Raums, Baden-Baden 2012, S. 265–305.
Schulz, Sönke E./Tischer, Jakob: Das Internet als kritische Infrastruktur. Handlungsbedarf für den Gesetzgeber, ZG 2013, S. 339–357.
Schulze, Matthias: Going Dark? Dilemma zwischen sicherer, privater Kommunikation und den Sicherheitsinteressen von Staaten, Parl Beilage, Nr. 46–47 2017, S. 23–28.

–: Governance von 0-Day-Schwachstellen in der deutschen Cyber-Sicherheitspolitik, SWP-Studie, Mai 2019, https://www.swp-berlin.org/publications/products/studien/2019S10_she.pdf.
–: The State of Cyber Arms Control. An International Vulnerabilities Equities Process as the Way to go Forward?, S&F Sicherheit und Frieden 38:1 (2020), S. 17–21.
Schulze, Sven-Hendrik: Cyber-„War" – Testfall der Staatenverantwortlichkeit, Tübingen 2015.
Schulze, Tillmann: Bedingt abwehrbereit. Schutz kritischer Informations-Infrastrukturen in Deutschland und den USA, Wiesbaden 2006.
Schulze-Fielitz, Helmuth: Zeitoffene Gesetzgebung, in: Wolfgang Hoffmann-Riem/Eberhard Schmidt-Aßmann (Hrsg.), Flexibilität und Innovationsoffenheit im Verwaltungsrecht, Baden-Baden 1994, S. 139–198.
–: Technik und Umweltrecht, in: Martin Schulte/Rainer Schröder (Hrsg.), Handbuch des Technikrechts, Berlin u. a. 2011, S. 455–504.
Schumacher, Oskar: Relevanzzuschreibungen im Recht der Pandemie, GSZ 2021, S. 155–161.
Schüneman, Wolf J.: E-Government und Netzpolitik – eine konzeptionelle Einführung, in: Wolf J. Schüneman/Marianne Kneuer (Hrsg.), E-Government und Netzpolitik im europäischen Vergleich, Baden-Baden 2019, S. 17–50.
Schuppert, Gunnar Folke: Gute Gesetzgebung. Bausteine einer kritischen Gesetzgebungslehre, Heidelberg 2003.
–: Verwaltungsrecht und Verwaltungsrechtswissenschaft im Wandel. Von Planung über Steuerung zu Governance?, AöR 133 (2008), S. 79–106.
–: Governance und Rechtsetzung. Grundfragen einer modernen Regelungswissenschaft, Baden-Baden 2011.
– (Hrsg.): Der Gewährleistungsstaat – ein Leitbild auf dem Prüfstand, Baden-Baden 2004.
Schütz, Erhard: Faszination der blaßgrauen Bänder, in: Wolfgang Emmerich/Carl Wege (Hrsg.), Der Technikdiskurs in der Hitler-Stalin-Ära, Stuttgart u. a. 1995, S. 123–145.
Schwab, Martin: Rechtsfragen der Politikberatung im Spannungsfeld zwischen Wissenschaftsfreiheit und Unternehmensschutz, Berlin 1999.
Schwabenbauer, Thomas: Kommunikationsschutz durch Art. 10 GG im digitalen Zeitalter, AöR 137 (2012), S. 1–41.
–: Heimliche Grundrechtseingriffe. Ein Beitrag zu den Möglichkeiten und Grenzen sicherheitsbehördlicher Ausforschung, Tübingen 2013.
Schwartz, Paul M.: Global Data Privacy Law, N.Y.U. L. Rev. 94 (2019), S. 771–818.
Schwarze, Jürgen/Becker, Ulrich/Hatje, Armin/Schoo, Johann (Hrsg.): EU-Kommentar, 4. Aufl. Baden-Baden 2019.
Schwind, Manuel: Netzwerke im Europäischen Verwaltungsrecht. Ein Beitrag zu Theorie und Dogmatik der Behördenkooperation in der EU, Tübingen 2017.
Scott, Colin/Cafaggi, Fabrizio/Senden, Linda (Hrsg.): The Challenge of Transnational Private Regulation. Conceptual and Constitutional Debates, Malden (Mass.) 2011.
Scott, Joanne: Extraterritoriality and Territorial Extension in EU Law, Am. J. Comp. L. 62 (2014), S. 87–125.
Seckelmann, Margrit: Industrialisierung, Internationalisierung und Patentrecht im Deutschen Reich, 1871–1914, Frankfurt a. M. 2006.
–: Evaluation und Recht. Strukturen, Prozesse und Legitimationsfragen staatlicher Wissensgewinnung durch (Wissenschafts-)Evaluationen, Tübingen 2018.

Seibel, Benjamin: Berechnendes Regieren. Karl W. Deutschs Entwurf einer politischen Kybernetik, Zeithistorische Forschungen/Studies in Contemporary History 9 (2012), S. 334–339.
–: Cybernetic Government. Informationstechnologie und Regierungsrationalität von 1943–1970, Wiesbaden 2016.
–: Staat am Draht, Zeitschrift für Ideengeschichte 11:1 (2017), S. 5–12.
Seidel, Ulrich: Persönlichkeitsrechtliche Probleme der elektronischen Speicherung privater Daten, NJW 1970, S. 1581–1583.
Selznick, Philip: Focusing Organisational Research on Regulation, in: Roger Noll (Hrsg.), Regulatory Policy and the Social Sciences, Berkeley u. a. 1985, S. 363–367.
Severson, Daniel: The Encryption Debate in Europe, Lawfare v. 21.3.2017, https://www.lawfareblog.com/encryption-debate-europe-0.
Shane, Peter M./Hunker, Jeffrey Allen (Hrsg.): Cybersecurity. Shared Risks, Shared Responsibilities, Durham 2013.
Shires, James: Enacting Expertise: Ritual and Risk in Cybersecurity, Politics and Governance 6:2 (2018), S. 31–40.
Sieferle, Rolf Peter: Fortschrittsfeinde? Opposition gegen Technik und Industrie von der Romantik bis zur Gegenwart München 1984.
Siehr, Angelika: Das Recht am Öffentlichen Raum, Tübingen 2017.
Simantiras, Nikolaos: Netzwerke im Europäischen Verwaltungsverbund: Legitimation durch Verantwortung polyzentrischer Governance-Strukturen, Tübingen 2016.
Simitis, Spiros: Automation in der Rechtsordnung: Möglichkeiten und Grenzen. Vortrag gehalten vor der Juristischen Studiengesellschaft in Karlsruhe am 14. Februar 1967, Karlsruhe 1967.
– (Hrsg.): Bundesdatenschutzgesetz, 2014.
Simitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra (Hrsg.): Datenschutzrecht, Baden-Baden 2019.
Simon, Herbert A.: The Shape of Automation for Men and Management, New York 1965.
Simonis, Georg: Konzepte und Verfahren der Technikfolgenabschätzung, Wiesbaden 2013.
Singelnstein, Tobias: Logik der Prävention. Eine kriminologische Perspektive auf das Strafrecht und andere Formen sozialer Kontrolle, in: Beatrice Brunhöber (Hrsg.), Strafrecht im Präventionsstaat, Stuttgart 2014, S. 41–57.
–: Predictive Policing, NStZ 2018, S. 1–9.
Singelnstein, Tobias/Stolle, Peer: Die Sicherheitsgesellschaft. Soziale Kontrolle im 21. Jahrhundert, 3. Aufl. Wiesbaden 2012.
Singelnstein, Tobias/Zech, Louisa: Schutz der IT-Sicherheit durch das Strafrecht, in: Gerrit Hornung/Martin Schallbruch (Hrsg.), IT-Sicherheitsrecht, Baden-Baden 2021, § 20.
Singer, Peter Warren/Friedman, Allan: Cybersecurity and Cyberwar. What everyone needs to know, Oxford 2014.
Sivakumar, Niranjan: Generative Security: Adversarial Design and Conflict of Laws, AJIL Unbound 110 (2017), S. 358–363.
Skopik, Florian/Pahi, Timea: Under False Flag. Using Technical Artifacts for Cyber Attack Attribution, Cybersecurity 3:1 (2020), S. 1–8.
Slayton, Rebecca: Measuring Risk: Computer Security Metrics, Automation, and Learning, IEEEA 37:2 (2015), S. 32–45.

Sliwinski, Krzysztof Feliks: Moving beyond the European Union's Weakness as a Cyber-Security Agent, Contemporary Security Policy 35:3 (2014), S. 468–486.
Smeddinck, Ulrich: Gesetzgebungsmethodik und Gesetzestypen, in: Winfried Kluth/Günter Krings (Hrsg.), Gesetzgebung. Rechtsetzung durch Parlamente und Verwaltungen sowie ihre gerichtliche Kontrolle, Heidelberg 2014, § 3.
Smith, Clifton L./Brooks, David J.: Security Science: The Theory and Practice of Security, Kidlington u. a. 2013.
Sohr, Karsten/Kemmerich, Thomas: Technische Grundlagen der Informationssicherheit, in: Dennis-Kenji Kipker (Hrsg.), Cybersecurity, München 2020, Kap. 2.
Soiné, Michael: Die strafprozessuale Online-Durchsuchung, NStZ 2018, S. 497–504.
von Solms, Rossouw/van Niekerk, Johan: From Information Security to Cyber Security, Computers & Security 38 (2013), S. 97–102.
Solove, Daniel: A Taxonomy of Privacy, U. Penn L. Rev. 154 (2006), S. 477–560.
–: Understanding Privacy, Cambridge (Mass.) 2010.
Solum, Lawrence B./Chung, Minn: The Layers Principle: Internet Architecture and the Law, Notre Dame L. Rev. 79 (2004), S. 815–948.
Somek, Alexander: Rechtstheorie zur Einführung, Hamburg 2017.
Sommer, Peter/Brown, Ian: Reducing Systemic Cybersecurity Risk, 14.1.2011, https://www.oecd.org/gov/risk/46889922.pdf.
Sommerer, Lucia: Personenbezogenes Predictive Policing. Kriminalwissenschaftliche Untersuchung über die Automatisierung der Kriminalprognose, Baden-Baden 2020.
Sommerfeld, Alisa: Verwaltungsnetzwerke am Beispiel des Gemeinsamen Terrorismusabwehrzentrums des Bundes und der Länder (GTAZ), Berlin 2015.
Sommermann, Karl-Peter: Objectives and Methods of a Transnational Science of Administrative Law, in: Hermann-Josef Blanke/Pedro Cruz Villalón et al. (Hrsg.), Common European Legal Thinking, Berlin 2015, S. 543–561.
Sonntag, Matthias: IT-Sicherheit kritischer Infrastrukturen. Von der Staatsaufgabe zur rechtlichen Ausgestaltung, München 2005.
SPD/Bündnis 90/Die Grünen/FDP: Mehr Fortschritt wagen, 2021, https://www.bundesregierung.de/resource/blob/974430/1990812/04221173eef9a6720059cc353d759a2b/2021–12–10-koav2021-data.pdf.
Specht, Louisa: Diktat der Technik. Regulierungskonzepte technischer Vertragsinhaltsgestaltung am Beispiel von Bürgerlichem Recht und Urheberrecht, Baden-Baden 2019.
Specht-Riemenschneider, Louisa: Herstellerhaftung für nicht-datenschutzkonform nutzbare Produkte – Und er haftet doch! Überlegungen zur Anwendbarkeit der deliktischen Produzentenhaftung bei Inverkehrbringens datenschutzrechtlich relevanter Produkte, MMR 2020, S. 73–78.
Spehr, Michael: Maschinensturm. Protest und Widerstand gegen technische Neue-rungen am Anfang der Industrialisierung, Münster 2000.
Spiecker gen. Döhmann, Indra: Wissensverarbeitung im Öffentlichen Recht, Rechtswissenschaft 1 (2010), S. 247–282.
–: Rechtliche Begleitung der Technikentwicklung im Bereich moderner Infrastrukturen und Informationstechnologien, in: Hermann Hill/Utz Schliesky (Hrsg.), Die Vermessung des virtuellen Raums, Baden-Baden 2012, S. 137–161.
Spiecker gen. Döhmann, Indra/Collin, Peter (Hrsg.): Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, Tübingen 2008.
Spiekermann, Sarah: Digitale Ethik. Ein Wertesystem für das 21. Jahrhundert, München 2019.

Spies-Otto, Sylvia: Die verfassungsrechtliche Dimension staatlichen Verhaltens im Cyber-Raum, NZWehrr 2016, S. 133–150.
–: Aufgaben und Befugnisse der Bundeswehr, in: Gerrit Hornung/Martin Schallbruch (Hrsg.), IT-Sicherheitsrecht, Baden-Baden 2021, § 19.
Spindler, Gerald: IT-Sicherheit und Produkthaftung – Sicherheitslücken, Pflichten der Hersteller und der Softwarenutzer, NJW 2004, S. 3145–3150.
–: Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären 2007, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITSicherheitUndRecht/Gutachten_pdf.pdf?__blob=publicationFile&v=2.
–: IT-Sicherheit – Rechtliche Defizite und rechtspolitische Alternativen, MMR 2008, S. 7–13.
–: IT-Sicherheit und kritische Infrastrukturen – Öffentlich-rechtliche und zivilrechtliche Regulierungsmodelle, in: Michael Kloepfer (Hrsg.), Schutz kritischer Infrastrukturen, Baden-Baden 2010, S. 85–120.
–: IT-Sicherheitsgesetz und zivilrechtliche Haftung, CR 2016, S. 297–312.
–: Weltweite Löschungspflichten bei Persönlichkeitsrechtsverletzungen im Internet, NJW 2019, S. 3274–3277.
–: Grundlagen deliktsrechtlicher Sicherheitspflichten, in: Gerrit Hornung/Martin Schallbruch (Hrsg.), IT-Sicherheitsrecht, Baden-Baden 2021, § 10.
–: Verantwortung der IT-Hersteller (produktbezogene Pflichten), in: Gerrit Hornung/Martin Schallbruch (Hrsg.), IT-Sicherheitsrecht, Baden-Baden 2021, § 11.
Staff, Ilse: Die Wahrung staatlicher Ordnung. Ein Beitrag zum technologischen Staat und seinen rechten Propheten Carl Schmitt und Ernst Forsthoff, Leviathan 15 (1987), S. 141–162.
Stam, Fabian: Die Strafbarkeit des Aufbaus von Botnetzen, ZIS 2017, S. 547–552.
Stark, Alexander: Interdisziplinarität der Rechtsdogmatik, Tübingen 2020.
Stark, Holger: BKA kaufte heimlich NSO-Spähsoftware, Die Zeit, 7.9.2021, https://www.zeit.de/politik/deutschland/2021–09/spionagesoftware-pegasus-nso-israel-bundeskriminalamt-kauf-innenauschuss-bundestag-unterrichtung.
Steffens, Timo: Attribution of Advanced Persistent Threats. How to Identify the Actors Behind Cyber-Espionage, Berlin 2020.
Stein, Ekkehart: Die Wirtschaftsaufsicht, Tübingen 1967.
Steinmüller, Wilhelm/Lutterbeck, Bernd et al.: Grundfragen des Datenschutzes. Techn. Ber. Gutachten im Auftrag des Bundesministeriums des Innern, BT-Drs. VI/3826, Anlage 1, Juli 1971.
Steinmüller, Wilhelm/Wolter, Henner: Besonderheiten elektronischer Datenverarbeitung, in: Ulrich Dammann/Mark O. Karhausen et al. (Hrsg.), Datenbanken und Datenschutz, Frankfurt a. M. 1974, S. 51–61.
Stevens, Tim: Cybersecurity and the Politics of Time, Cambridge 2016.
Stigler, George J.: The Theory of Economic Regulation, The Bell Journal of Economics and Management Science 2 (1971), S. 3–21.
Stinner, Julia: Staatliche Schutzpflichten im Rahmen informationstechnischer Systeme, Baden-Baden 2018.
Stober, Rolf/Eisenmenger, Sven: Katastrophenverwaltungsrecht – Zur Renaissance eines vernachlässigten Rechtsgebietes, NVwZ 2005, S. 121–130.
Stockton, Paul N./Golabek-Goldman, Michele: Curbing the Market for Cyber Weapons, Yale L. & Pol'y Rev. 32:1 (2013), S. 239–266.
Stoll, Peter-Tobias: Sicherheit als Aufgabe von Staat und Gesellschaft. Verfassungsord-

nung, Umwelt- und Technikrecht im Umgang mit Unsicherheit und Risiko, Tübingen 2003.
Stollberg-Rilinger, Barbara: Der Staat als Maschine. Zur politischen Metaphorik des absoluten Fürstenstaates Berlin 1986.
Stolle, Peer: Das (Un-)Sicherheitsgefühl – ein untauglicher Begründungszusammenhang für eine Politik der Inneren Sicherheit, Kritische Justiz 44 (2011), S. 16–24.
Stolleis, Michael: Geschichte des öffentlichen Rechts in Deutschland. Band 3. Staats- und Verwaltungsrechtswissenschaft in Republik und Diktatur 1914 bis 1945, München 1999.
Stone, M. G./Warner, Malcolm: Politics, Privacy, and Computers, The Political Quarterly 40 (1969), S. 256–267.
Stradomsky, Christopher: KRITIS – Der Weg zum Audit, DuD 2021, S. 589–593.
Stritzel, Holger: Security in Translation. Securitization Theory and the Localization of Threat, Basingstoke u. a. 2014.
Stuckenberg, Carl-Friedrich: Viel Lärm um nichts? – Keine Kriminalisierung der „IT-Sicherheit" durch § 202c StGB, wistra 2010, S. 41–46.
Sukumar, Arun M.: The UN GGE Failed: Is International Law in Cyberspace Doomed as Well?', Lawfare v. 4.7.2017, www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well.
Sunstein, Cass: After the Rights Revolution: Reconceiving the Regulatory State, Cambridge (Mass.) 1990.
Szczekalla, Peter: Die sogenannten grundrechtlichen Schutzpflichten im deutschen und europäischen Recht. Inhalt und Reichweite einer „gemeineuropäischen Grundrechtsfunktion", Berlin 2002.
T-Systems International GmbH: Forensics Report: Vorläufiger forensischer Abschlussbericht zur Untersuchung des Incidents beim Berliner Kammergericht, 23.12.2019, https://www.berlin.de/sen/justva/presse/pressemitteilungen/2020/pm-11–2020-t-systems-forensik_bericht_public_v1.pdf.
Taeger, Jürgen: Außervertragliche Haftung für fehlerhafte Computerprogramme, Tübingen 1995.
Taeger, Jürgen/Gabel, Detlev (Hrsg.), BDSG, 2. Aufl. Frankfurt a. M. 2013.
Taeihagh, Araz/Ramesh, M./Howlett, Michael: Assessing the regulatory challenges of emerging disruptive technologies, Regulation & Governance 15 (2021), S. 1009–1019.
Tamanaha, Brian Z.: A Non-Essentialist Version of Legal Pluralism, Journal of Law and Society 27:2 (2000), S. 296–321.
Tanneberger, Steffen: Die Sicherheitsverfassung. Eine systematische Darstellung der Rechtsprechung des Bundesverfassungsgerichts – zugleich ein Beitrag zu einer induktiven Methodenlehre, Tübingen 2014.
TeleTrusT: Handreichung: Stand der Technik in der IT-Sicherheit, September 2021, https://www.teletrust.de/fileadmin/user_upload/2021–09_TeleTrusT-Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DE.pdf.
Tettinger, Peter J.: Verfassungsrecht und Techniksteuerung, in: Klaus Vieweg (Hrsg.), Techniksteuerung und Recht, Köln u. a. 2000, S. 287–306.
Teubner, Gunther: Global Law without a State, Aldershot u. a. 1997.
–: Global Private Regimes: Neo-spontaneous Law and Dual Constitution of Autonomous Sectors?, in: Karl-Heinz Ladeur (Hrsg.), Public Governance in the Age of Globalization, London 2004, S. 71–88.
Thalhofer, Thomas: Rechtliche Regeln für die IT-Sicherheit in Organisationen, in: Ger-

rit Hornung/Martin Schallbruch (Hrsg.), IT-Sicherheitsrecht, Baden-Baden 2021, § 16.
Thatcher, Mark: Regulation After Delegation: Independent Regulatory Agencies in Europe, Journal of European Public Policy 9 (2002), S. 954–972.
Thaw, David: The Efficacy of Cybersecurity Regulation, Georgia State U. L. Rev. 30 (2014), S. 287–347.
Thiel, Markus: Die „Entgrenzung" der Gefahrenabwehr. Grundfragen von Freiheit und Sicherheit im Zeitalter der Globalisierung, Tübingen 2011.
Thiele, Alexander: Zivile Sicherheit im Katastrophenrecht, in: Christoph Gusy/Dieter Kugelmann/Thomas Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, Berlin u. a. 2017, S. 539–562.
Thiele, Carmen: Fragmentierung des Völkerrechts als Herausforderung für die Staatengemeinschaft, AVR 46 (2008), S. 1–41.
Thierer, Adam/Crews, Clyde Wayne (Hrsg.): Who Rules the Net? Internet Governance and Jurisdiction, Washington 2003.
Thompson, Andi Wilson: Assessing the Vulnerabilities Equities Process, Three Years After the VEP Charter, Lawfare v. 13.1.2021, https://www.lawfareblog.com/assessing-vulnerabilities-equities-process-three-years-after-vep-charter.
Thon, Marian: Transnationaler Datenschutz, RabelsZ 84 (2020), S. 24–61.
Thümmel, Juliane: Computernetzwerkoperationen innerhalb internationaler bewaffneter Konflikte, Baden-Baden 2013.
Töller, Annette Elisabeth: Regieren als Problemlösung oder als eigendynamischer Prozess? Überlegungen zu einer Überwindung des Problemlösungsbias in der Politikfeldanalyse, in: Björn Egner/Michael Haus/Georgios Terizakis (Hrsg.), Regieren. Festschrift für Hubert Heinelt, Wiesbaden 2012, S. 171–190.
Tran, Delbert: The Law of Attribution. Rules for Attributing the Source of a Cyber-Attack, Yale J. L. & Tech. 20 (2017), S. 376–441.
Tribe, Laurence H.: Channeling Technology Through Law, Chicago 1973.
Trotter Hardy, I.: The Proper Legal Regime for "Cyberspace", U. Pitt. L. Rev. 55 (1994), S. 993–1055.
Trute, Hans-Heinrich: Der Schutz personenbezogener Daten in der Informationsgesellschaft, JZ 53 (1998), S. 822–831.
–: Die Erosion des klassischen Polizeirechts durch die polizeiliche Informationsvorsorge, in: Wilfried Erbguth/Friedrich Müller/Volker Neumann (Hrsg.), GS Bernd Jeand'Heur, 1999, S. 403–427.
–: Gefahr und Prävention in der Rechtsprechung zum Polizei- und Ordnungsrecht, DV 36 (2003), S. 501–522.
–: Katastrophenschutzrecht. Besichtigung eines verdrängten Rechtsgebiets, KritV 88 (2005), S. 342–363.
–: Wirtschaft und Technik, in: Josef Isensee/Paul Kirchhof (Hrsg.), Handbuch des Staatsrechts, Bd. IV, 2006, § 88.
–: Grenzen des präventionsorientierten Polizeirechts in der Rechtsprechung des Bundesverfassungsgerichts, DV 42 (2009), S. 85–104.
–: Die demokratische Legitimation der Verwaltung, in: Andreas Voßkuhle/Martin Eifert/Christoph Möllers (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. 1, 3. Aufl. München 2022, § 9.
Trute, Hans-Heinrich/Denkhaus, Wolfgang/Kühlers, Doris: Governance in der Verwaltungsrechtswissenschaft, DV 37 (2004), S. 451–474.

Tsagourias, Nicholas: Cyber attacks, self-defence and the problem of attribution, Journal of conflict and security law, 17:2 (2012), S. 229–244.
–: The Slow Process of Normativizing Cyberspace, AJIL Unbound 113 (2019), S. 71–75.
Tsagourias, Nicholas/Farrell, Michael: Cyber Attribution. Technical and Legal Approaches and Challenges, EJIL 31:3 (2020), S. 941–967.
Tsagourias, Nicholas/Buchan, Russell (Hrsg.): Research Handbook on International Law and Cyberspace, Cheltenham, UK 2015.
Tschentscher, Axel: Das Grundrecht auf Computerschutz, AJP/PJA 2008, S. 383–393.
Turner, Fred: From counterculture to cyberculture. Stewart Brand, the Whole Earth Network, and the rise of digital utopianism, Chicago 2006.
U.S. Department of Justice: Report on the Investigation into Russian Interference in the 2016 Presidential Election, Bd. I, Washington, D.C. 2019, https://www.justice.gov/storage/report.pdf.
U.S. President's Commission on Critical Infrastructure Protection (PCCIP): Critical Foundations: Protecting America's Infrastructures, 1997, https://bit.ly/3kst1mN.
Uerpmann-Wittzack, Robert: Principles of International Internet Law, German L. J. 11 (2010), S. 1245–1263.
– (Hrsg.): Das neue Computergrundrecht, Münster 2009.
United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Report, U.N. Doc. A/70/174, 22.7.2015.
–: Report, U.N. Doc. A/76/135, 14.7.2021.
Valeriano, Brandon/Maness, Ryan C.: Cyber War versus Cyber Realities: Cyber Conflict in the International System, New York 2015.
–: How We Stopped Worrying about Cyber Doom and Started Collecting Data, Politics and Governance 6:2 (2018), S. 49–60.
van der Wees, Arthur/Stefanatou, Dimitra/Pathania, Prakriti: Work Package 4: Policy and the European Dimension Deliverable D4.2, 2020, https://www.concordia-h2020.eu/wp-content/uploads/2021/03/Deliverables_D4.2.pdf.
van Schewick, Barbara: Internet Architecture and Innovation, Cambridge (Mass.) 2010.
Varju, Marton: 5G Networks, (Cyber)security Harmonisation and the Internal Market: The Limits of Article 114 TFEU, European L. Rev. 45 (2020), S. 471–486.
Vatanparast, Roxana: Designed to Serve Mankind? The Politics of the GDPR as a Global Standard and the Limits of Privacy, ZaöRV 80 (2020), S. 819–846.
Vec, Miloš: Recht und Normierung in der Industriellen Revolution. Neue Strukturen der Normsetzung in Völkerrecht, staatlicher Gesetzgebung und gesellschaftlicher Selbstnormierung, Frankfurt a. M. 2006.
–: Kurze Geschichte des Technikrechts, in: Martin Schulte/Rainer Schröder (Hrsg.), Handbuch des Technikrechts, 2. Aufl. Berlin u. a. 2011, S. 3–92.
Vesting, Thomas: Zur Entwicklung einer „Informationsordnung", in: Peter Badura/Horst Dreier (Hrsg.), Festschrift 50 Jahre Bundesverfassungsgericht, Bd. 2, 2001, S. 219–240.
–: Nachbarwissenschaftlich informierte und reflektierte Verwaltungsrechtswissenschaft – „Verkehrsregeln" und „Verkehrsströme", in: Eberhard Schmidt-Aßmann/Wolfgang Hoffmann-Riem (Hrsg.), Methoden der Verwaltungsrechtswissenschaft, Baden-Baden 2004, S. 253–292.

–: Die Medien des Rechts: Buchdruck, Weilerswist 2013.
–: Rechtstheorie, 2. Aufl. München 2015.
–: Die Medien des Rechts: Computernetzwerke, Weilerswist 2015.
–: Instituierte und konstituierte Normativität. Prozeduralisierung und multi-normative Systeme, in: Tatjana Sheplyakova (Hrsg.), Prozeduralisierung des Rechts, Tübingen 2018, S. 101–122.
–: Die Bedeutung von Information und Kommunikation für die verwaltungsrechtliche Systembildung, in: Martin Eifert/Christoph Möllers/Andreas Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. 1, 3. Aufl. München 2022, § 20.
Viellechner, Lars: Transnationalisierung des Rechts, Weilerswist 2013.
Vieweg, Klaus: Produkthaftungsrecht in: Martin Schulte/Rainer Schröder (Hrsg.), Handbuch des Technikrechts, Berlin u. a. 2011, S. 337–383.
Vogel, Klaus: Der räumliche Anwendungsbereich der Verwaltungsrechtsnorm. Eine Untersuchung über die Grundfragen des sogenannten internationalen Verwaltungs- und Steuerrechts, Frankfurt a. M. 1965.
Voigt, Paul: IT-Sicherheitsrecht. Pflichten und Haftung im Unternehmen, 2. Aufl. Köln 2022.
Volkmann, Uwe: Polizeirecht als Sozialtechnologie, NVwZ 2009, S. 216–222.
vom Feld, Ina: Kontrollierte Staatsentlastung im Technikrecht – Dampfkesselgesetzgebung und Dampfkesselüberwachung in Preußen 1831–1914, Frankfurt a. M. 2007.
Voskamp, Friederike: Datenschutz, in: Dennis-Kenji Kipker (Hrsg.), Cybersecurity, München 2020, Kap. 5.
Voßkuhle, Andreas: Rechtstatsachenforschung und Verwaltungsdogmatik, Verwaltungsarchiv 85 (1994), S. 567–585.
–: Behördliche Betretungs- und Nachschaurechte. Versuch einer dogmatischen Klärung, DVBl. 1994, S. 611–620.
–: Die Reform des Verwaltungsrechts als Projekt der Wissenschaft, DV 32 (1999), S. 545–554.
–: Der Wandel von Verwaltungsrecht und Verwaltungsprozeßrecht in der Informationsgesellschaft, in: Wolfgang Hoffmann-Riem/Eberhard Schmidt-Aßmann (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, Baden-Baden 2000, S. 349–404.
–: „Regulierte Selbstregulierung" – Zur Karriere eines Schlüsselbegriffs, DV Beiheft 4 (2001), S. 197–200.
–: „Schlüsselbegriffe" der Verwaltungsrechtsreform. Eine kritische Bestandsaufnahme, VerwArch 93 (2002), S. 184–215.
–: Methode und Pragmatik im Öffentlichen Recht, in: Hartmut Bauer/Detlef Czybulka et al. (Hrsg.), Umwelt, Wirtschaft und Recht, Tübingen 2002, S. 171–195.
–: Strukturen und Bauformen neuer Verwaltungsverfahren, in: Wolfgang Hoffmann-Riem/Eberhard Schmidt-Aßmann (Hrsg.), Verwaltungsverfahren und Verwaltungsverfahrensgesetz, Baden-Baden 2002, S. 277–347.
–: Beteiligung Privater an der Wahrnehmung öffentlicher Aufgaben und staatliche Verantwortung, in: VVDStRL 62 (2003), S. 266–335.
–: Das Konzept des rationalen Staates, in: ders./Gunnar Folke Schuppert (Hrsg.), Governance von und durch Wissen, Baden-Baden 2008, S. 13–32.
–: Das Verhältnis von Freiheit und Sicherheit – Hat der 11. September 2001 das deutsche Verfassungsrecht verändert?, in: Dirk Heckmann/Ralf P. Schenke/Gernot Sydow (Hrsg.), Verfassungsstaatlichkeit im Wandel. Festschrift für Thomas Würtenberger, Berlin 2013, S. 1101–1120.

–: Präventive Richtervorbehalte, in: Detlef Merten/Hans-Jürgen Papier (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa, Bd. V, Heidelberg 2013, § 131.
–: Staatsaufgabe Infrastruktur, in: Mathias Habersack/Karl Huber/Gerald Spindler (Hrsg.), Festschrift für Eberhard Stilz zum 65. Geburtstag, München 2014, S. 675–688.
–: Neue Verwaltungsrechtswissenschaft, in: ders./Martin Eifert/Christoph Möllers (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. 1, 3. Aufl. München 2022, § 1.
Voßkuhle, Andreas/Wischmeyer, Thomas: The 'Neue Verwaltungsrechtswissenschaft' against the backdrop of traditional administrative law scholarship in Germany, in: Peter Lindseth/Susan Rose-Ackerman (Hrsg.), Comparative Administrative Law, 2. Aufl. Cheltenham 2017, S. 85–101.
Voßkuhle, Andreas/Schuppert, Gunnar Folke (Hrsg.): Governance von und durch Wissen, Baden-Baden 2008.
Wæver, Ole: Securitization and Desecuritization, in: Ronnie Lipschutz (Hrsg.), On Security, 1995, S. 46–86.
Wagener, Frido: Typen der verselbständigten Erfüllung öffentlicher Aufgaben, in: Frido Wagener (Hrsg.), Verselbständigung von Verwaltungsträgern, Bonn 1976, S. 31–50.
Wahl, Rainer: Forschungs- und Anwendungskontrolle technischen Fortschritts als Staatsaufgabe?, UTR 14 (1991), S. 7–36.
–: Die Aufgabenabhängigkeit von Verwaltung und Verwaltungsrecht, in: Wolfgang Hoffmann-Riem/Eberhard Schmidt-Aßmann/Gunnar Folke Schuppert (Hrsg.), Reform des Allgemeinen Verwaltungsrechts – Grundfragen, Baden-Baden 1993, S. 177–218
–: Die zweite Phase des Öffentlichen Rechts in Deutschland. Die Europäisierung des Öffentlichen Rechts, Der Staat 38 (1999), S. 495–518.
Wahl, Rainer/Masing, Johannes: Schutz durch Eingriff, JZ 45 (1990), S. 553–563.
Waldhoff, Christian: Die reformierte Kontrolle der Nachrichtendienste durch das Parlamentarische Kontrollgremium und das Unabhängige Gremium, in: Jan-Hendrik Dietrich/Klaus Ferdinand Gärditz et al. (Hrsg.), Nachrichtendienste in vernetzter Sicherheitsarchitektur, Tübingen 2020, S. 73–89.
Walker, Neil: Intimations of Global Law, Cambridge 2015.
Wallach, Wendell/Asaro, Peter (Hrsg.): Machine Ethics and Robot Ethics, Abingdon 2017.
Walter, Christian: Cyber Security als Herausforderung für das Völkerrecht, JZ 70 (2015), S. 685–693.
Walter, Tasia: Der Staat als Sicherheitsgarant? Sicherheitsverständnisse, Sicherheitserwartungen und Sicherheitsverheißungen des Staates im Umgang mit neuen terroristischen Bedrohungslagen des 21. Jahrhunderts, Baden-Baden 2019.
Warner, Michael: Cybersecurity: A Pre-history, Intelligence and National Security 27:5 (2012), S. 781–799.
–: Notes on the Evolution of Computer Security Policy in the US Government, 1965–2003, IEEEA 37:2 (2015), S. 8–18.
Warren, Samuel D./Brandeis, Louis D.: The Right to Privacy, Harv. L. Rev. 4 (1890), S. 193–220.
Waxman, Matthew C.: Cyber-Attacks and the Use of Force. Back to the Future of Article 2(4), Yale J. Int'l L. 36 (2011), S. 421–460.
Weaver, Nicholas: The GCHQ's Vulnerabilities Equities Process, Lawfare v. 3.6.2019, https://www.lawfareblog.com/gchqs-vulnerabilities-equities-process.

–: Encryption and Combating Child Exploitation Imagery, Lawfare v. 23.10.2019, https://www.lawfareblog.com/encryption-and-combating-child-exploitation-imagery.
Weber, Max: Wirtschaft und Gesellschaft. Grundriß der verstehenden Soziologie. Besorgt von Johannes Winckelmann. Studienausgabe, 5. Aufl. Tübingen 1980.
–: Parlament und Regierung im neugeordneten Deutschland, in: Gesammelte politische Schriften (hrsg. von Johannes Winckelmann), 5. Aufl. Tübingen 1988, S. 306–443.
Weber, Rolf H.: Shaping Internet Governance: Regulatory Challenges, Wien u. a. 2009.
Weber, Valentin: Linking Cyber Strategy with Grand Strategy: The Case of the United States, Journal of Cyber Policy 3 (2018), S. 236–257.
Webster, Frank: Theories of the Information Society, 4. Aufl. London 2014.
Weidenhammer, Detlef/Gundlach, Rocco: Wer kennt den „Stand der Technik"?, DuD 2018, S. 106–110.
Weingart, Peter (Hrsg.): Technik als sozialer Prozeß, Frankfurt a. M. 1989.
Weiß, Holger Tobias: Die rechtliche Gewährleistung der Produktsicherheit, Baden-Baden 2008.
Weißgärber, Kirsten: Die Legitimation unabhängiger europäischer und nationaler Agenturen, Baden-Baden 2016.
Weitzenboeck, Emily M.: Hybrid Net: The Regulatory Framework of ICANN and the DNS, Int'l J. L. & Info. Tech. 22:1 (2014), S. 49–73.
Wenger, Etienne: Communities of Practice. Learning, Meaning, and Identity, Cambridge 1999.
Wengeroth, Ulrich: Technik der Moderne, 2015, https://www.mcts.tum.de/research/technik-der-moderne/.
Wenzelburger, Georg/Zohlnhöfer, Reimut (Hrsg.): Handbuch Policy-Forschung, Wiesbaden 2015.
Wessel, Ramses: Towards EU Cybersecurity Law: Regulating a New Policy Field, in: Nikolaos K. Tsagourias/Russell Buchan (Hrsg.), Research Handbook on International Law and Cyberspace, Cheltenham 2015, S. 403–425.
–: European Law and Cyberspace, in: Nikolaos K. Tsagourias/Russell Buchan (Hrsg.), Research Handbook on International Law and Cyberspace, 2. Aufl. Cheltenham 2021, S. 491–508.
Westermann, Eike: Legitimation im europäischen Regulierungsverbund. Zur demokratischen Verwaltungslegitimation im europäischen Regulierungsverbund für elektronische Kommunikation, Tübingen 2017.
Westin, Alan: Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I – The Current Impact of Surveillance on Privacy, Colum. L. Rev. 66 (1966), S. 1003–1050.
–: Privacy and Freedom, New York 1967.
White House: Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process, 2010, https://www.eff.org/files/2016/01/18/37–3_vep_2016.pdf.
–: Renewing America's Advantages: Interim National Security Strategic Guidance, March 2021, https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.
–: Vulnerabilities Equities Policy and Process for the United States Government, 15.11.2017, https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

Whitt, Richard S.: A Deference to Protocol: Fashioning a Three-Dimensional Public Policy Framework for the Internet Age, Cardozo Arts & Entertainment Law Journal 31 (2013), S. 689–768.
Whitten, Alma/Tygar, J. D.: Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0, in: Lori Cranor/Simpson Garfinkel (Hrsg.), Security and Usability: Designing Systems that People Can Use, Sebastapol 2005, S. 669–690.
Whyte, Christopher: Cyber conflict or democracy "hacked"? How cyber operations enhance information warfare, Journal of Cybersecurity 6:1 (2020), S. 1–17.
Wiater, Patricia: Sicherheitspolitik zwischen Staat und Markt. Der Schutz kritischer Infrastrukturen, Baden-Baden 2013.
Wiebe, Gerhard: Produktsicherheitsrechtliche Pflicht zur Bereitstellung sicherheitsrelevanter Software-Updates, NJW 2019, S. 625–630.
–: IT-sicherheitsbezogene Pflichten von Herstellern smarter Produkte, InTeR 2021, S. 66–70.
Wiegand, Nicolai: IT-Vertragsrecht, in: in: Dennis-Kenji Kipker (Hrsg.), Cybersecurity, München 2020, Kap. 7.
Wihl, Tim: Die Entwicklung „neuer" Grundrechte, in: Dieter Grimm (Hrsg.), Vorbereiter – Nachbereiter?, Tübingen 2019, S. 307–337.
Wikipedia-Autoren: Domain Name System Security Extensions: IETF publications, in: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 28. März 2022, https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions#IETF_publications.
–: IPsec: Alleged NSA interference, in: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 20. Januar 2022, https://en.wikipedia.org/wiki/IPsec#Alleged_NSA_interference.
–: IPsec: IETF documentation, in: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 20. Januar 2022, https://en.wikipedia.org/wiki/IPsec#IETF_documentation.
–: The Shadow Brokers, in: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 15. März 2022, https://en.wikipedia.org/wiki/The_Shadow_Brokers.
–: Transmission Control Protocol: RFC documents, in: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 13. März 2022, https://en.wikipedia.org/wiki/Transmission_Control_Protocol#RFC_documents.
Winkler, Günther: Raum und Recht. Dogmatische und theoretische Perspektiven eines empirisch-rationalen Rechtsdenkens, Wien u. a. 1999.
Winner, Langdon: Do Artifacts Have Politics?, Daedalus 109 (1980), S. 121–136.
–: The Whale and the Reactor. A Search for Limits in an Age of High Technology, Chicago u. a. 1986.
–: Upon Opening the Black Box and Finding It Empty. Social Constructivism and the Philosophy of Technology, Science, Technology, & Human Values 18 (1993), S. 362–378.
Winter, Nico: Meldepflichten bei Cyberangriffen, CR 2020, S. 576–584.
Wischmeyer, Thomas: Zwecke im Recht des Verfassungsstaates. Geschichte und Theorie einer juristischen Denkfigur, Tübingen 2015.
–: Überwachung ohne Grenzen. Zu den rechtlichen Grundlagen nachrichtendienstlicher Tätigkeiten in den USA, Baden-Baden 2017.
–: Informationssicherheitsrecht. IT-Sicherheitsgesetz und NIS-Richtlinie als Elemente eines Ordnungsrechts für die Informationsgesellschaft, DV 50 (2017), S. 155–188.
–: Formen und Funktionen des exekutiven Geheimnisschutzes, DV 51:3 (2018), S. 393–426.

–: Predictive Policing. Nebenfolgen der Automatisierung des Sicherheitsrechts, in: Andreas Kulick/Michael Goldhammer (Hrsg.), Der Terrorist als Feind? Personalisierung in Polizei- und Völkerrecht, Tübingen 2019, S. 189–209.
–: Der Verfassungsschutzverbund: Verfassungsrechtliche Rahmenbedingungen und Entwicklungsperspektiven, in: Jan-Hendrik Dietrich/Klaus Ferdinand Gärditz et al. (Hrsg.), Nachrichtendienste in vernetzter Sicherheitsarchitektur, Tübingen 2020, S. 35–79.
–: Informationsbeziehungen in der Verwaltung, in: Andreas Voßkuhle/Martin Eifert/Christoph Möllers (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. 1, 3. Aufl. München 2022, § 24.
–: Gewaltenteilung und institutionelles Gleichgewicht, in: Wolfgang Kahl/Markus Ludwigs (Hrsg.), Handbuch des Verwaltungsrechts, Bd. 3, Heidelberg 2022, § 78.
Wischmeyer, Thomas/Herzog, Eva: Digitale Ethik in der Demokratie, JZ 74 (2019), S. 696–701.
–: Daten für alle? – Grundrechtliche Rahmenbedingungen für Datenzugangsrechte, NJW 2020, S. 288–293.
Wischmeyer, Thomas/Mohnert, Alica: Recht der Informationssicherheit, in: Walter Frenz (Hrsg.), Handbuch Industrie 4.0: Recht, Technik, Gesellschaft, Berlin 2019, S. 215–236.
Wischmeyer, Thomas/Schumacher, Oskar: Schutz kritischer Infrastrukturen, in: Jan-Hendrik Dietrich/Matthias Fahrner/Nikolaos Gazeas/Bernd von Heintschel-Heinegg (Hrsg.), Handbuch Sicherheits- und Staatsschutzrecht, München 2022, § 14.
Wissenschaftliche Dienste des Deutschen Bundestages: Gemeinsames Terrorismusabwehrzentrum (GTAZ). Rechtsgrundlagen und Vergleichbarkeit mit anderen Kooperationsplattformen, Sachstand, WD 3–3000–406/18, 19.12.2018, https://www.bundestag.de/resource/blob/594538/8aff4300410fcac3f2e414d67922d5a9/WD-3-406-18-pdf-data.pdf.
Wißmann, Hinnerk: Die Anforderungen an ein zukunftsfähiges Infrastrukturrecht, in: VVDStRL 73 (2014), S. 369–427.
Woitke, Annika: Prüfgrundlagen nach § 8a, DuD 2021, S. 584–588.
Wolf, Marty J./Fresco, Nir: Ethics of the Software Culnerabilities and Exploits Market, The Information Society 32:4 (2016), S. 269–279.
Wolf, Rainer: Der Stand der Technik. Geschichte, Strukturelemente und Funktion der Verrechtlichung technischer Risiken am Beispiel des Immissionsschutzes, Opladen 1986.
–: Zur Antiquiertheit des Rechts in der Risikogesellschaft, Leviathan 15 (1987), S. 357–391.
–: „Herrschaft kraft Wissen" in der Risikogesellschaft, Soziale Welt 39 (1988), S. 164–187.
–: Die Risiken des Risikorechts, in: Alfons Bora (Hrsg.), Rechtliches Risikomanagement, Berlin 1999, S. 65–91.
Wolfers, Arnold: "National" Security as an Ambiguous Symbol, Political Science Quarterly 67:5 (1952), S. 481–502.
Wolff, Heinrich Amadeus: Prävention durch Verwaltungsrecht: Sicherheit, in: VVDStRL 81 (2022), S. 437–499.
Wolff, Josephine: Cyberinsurance Policy. Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks, Cambridge (Mass.), 2022.
Wollenschläger, Burkard: Wissensgenerierung im Verfahren, Tübingen 2009.

Woltag, Johann-Christoph: Cyber Warfare, 2014.
World Economic Forum: Global Risks Report 2021, 2021, http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf.
–: Global Risks Report 2022, 2022, http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf.
Wu, Tim: Cyberspace Sovereignty. The Internet and the International System, Harv. J. L. & Tech. 10 (1997), S. 647–666.
–: The Master Switch: The Rise and Fall of Information Empires, New York 2011.
Würtenberger, Thomas: Resilienz, in: Peter Baumeister/Wolfgang Roth/Josef Ruthig (Hrsg.), Staat, Verwaltung und Rechtsschutz. Festschrift für Wolf-Rüdiger Schenke zum 70. Geburtstag, Berlin 2011, S. 561–578.
Würtenberger, Thomas/Tanneberger, Steffen: Sicherheitsarchitektur als interdisziplinäres Forschungsfeld, in: Gisela Riescher (Hrsg.), Sicherheit und Freiheit statt Terror und Angst. Perspektiven einer demokratischen Sicherheit, Baden-Baden 2010, S. 97–125.
Yates, JoAnne/Murphy, Craig: Engineering Rules. Global Standard Setting Since 1880, Baltimore 2019.
Yost, Jeffrey R.: History of Computer Security Standards, in: Karl Leeuw/Jan Bergstra (Hrsg.), The History of Information Security. A Comprehensive Handbook, Amsterdam u. a. 2007, S. 595–621.
–: The Origin and Early History of the Computer Security Software Products Industry, IEEEA 37:2 (2015), S. 46–58.
Young, Alasdair R.: The European Union as a global regulator? Context and comparison, Journal of European Public Policy 22 (2015), S. 1233–1252.
Zähle, Kai: Der Bundessicherheitsrat, Der Staat 44 (2005), S. 462–482.
Zeidler, Karl: Über die Technisierung der Verwaltung. Eine Einführung in die juristische Beurteilung der modernen Verwaltung, Karlsruhe 1959.
Ziolkowski, Katharina: Attribution von Cyber-Angriffen, GSZ 2019, S. 51–57.
Zittrain, Jonathan: The Generative Internet, Harv. L. Rev. 119 (2006), S. 1974–2040.
–: The Future of the Internet and How to Stop It, New Haven u. a. 2008.
Zöller, Mark: Informationssysteme und Vorfeldmaßnahmen von Polizei, Staatsanwaltschaft und Nachrichtendiensten, Heidelberg 2002.
Zuboff, Shoshana: The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power New York 2019.
Zumbansen, Peer (Hrsg.): The Oxford Handbook of Transnational Law, Oxford 2021.

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