Hornung | Schallbruch [Hrsg.]

IT-Sicherheitsrecht

Praxishandbuch

2. Auflage

Nomos

Prof. Dr. Gerrit Hornung, LL.M.
Martin Schallbruch [Hrsg.]

IT-Sicherheitsrecht

Praxishandbuch

2. Auflage

Prof. Dr. Matthias Bäcker, LL.M. | Prof. Dr. Irene Bertschek | RA Dr. David Bomhard | Lars Bostelmann, M.A., Mag.rer.publ. | Matthias Fischer, LL.M. | PD Dr. Christian L. Geminn, Mag. iur. | Dr. Rotraud Gitter, LL.M. Eur. | Jun.-Prof. Dr. Sebastian J. Golla | Prof. Dr. Rüdiger Grimm | Prof. Dr. Annette Guckelberger | Dr. h.c. Marit Hansen | Prof. Dr. Andreas Heinemann | Prof. Dr. Gerrit Hornung, LL.M. | Dr. habil. Silke Jandt | Rebecca Janßen | RA Christian Kuß, LL.M. | Dr. Henning Lahmann | Dr. Philipp Lassahn, LL.M. | Ann-Sophie Letzel | Prof. Dr. Marian Margraf | Prof. Dr. Henning Müller | Johannes Müller MLE. | Prof. Dr. Ralf Poscher | RA Dr. Mansur Pour Rafsendjani | Prof. Dr. Alexander Roßnagel | MinDir a.D. Martin Schallbruch | Dr. Stephan Schindler | RA Dr. Jonas Siglmüller | Prof. Dr. Tobias Singelnstein | Philipp Singler | Dr. Isabel Skierka-Canton | MinDirig a.D. Sylvia Spies-Otto | Prof. Dr. Gerald Spindler† | Prof. Dr. Björn Steinrötter | RA Dr. Thomas Thalhofer | Prof. Dr. Michael Waidner | Louisa Zech

Nomos

Zitiervorschlag: Hornung/Schallbruch IT-SicherheitsR-HdB/Bearbeiter § ... Rn. ...

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

ISBN 978-3-7560-0496-6

2. Auflage 2025

Vorwort

Vier Jahre nach dem Erscheinen der ersten Auflage hat die Relevanz der IT-Sicherheit für nahezu alle Bereiche von Wirtschaft, Verwaltung und Privatleben weiter zugenommen. Leidvolle Erfahrungen mit IT-Sicherheitsvorfällen in allen Bereichen zeigen dies deutlich. Mit der Relevanz der IT-Sicherheit steigt auch die Bedeutung des IT-Sicherheitsrechts. Die entsprechenden Regelungen und das Rechtsgebiet insgesamt erhalten mehr und mehr Aufmerksamkeit. Dies betrifft gesetzgeberische Aktivitäten ebenso wie die Umsetzung in der Praxis und die wissenschaftliche Befassung. Der Bedarf nach Strategien für die effektive Umsetzung der regulatorischen Vorgaben ist enorm. Die rechtskonforme Implementierung von IT-Sicherheit ist mittlerweile unabdingbare Voraussetzung für die sichere Abwicklung von Wirtschafts- und Verwaltungsprozessen.

Die zweite Auflage des Handbuchs erscheint in einer Zeit, in der sich die Entwicklung des IT-Sicherheitsrechts weiter beschleunigt. Etliche neue Rechtsakte des europäischen Gesetzgebers sind in der letzten Zeit ergangen, umgesetzt worden oder harren der Umsetzung. Insbesondere im Zusammenspiel zwischen querschnittlichen und sektoralen Regelungen steht die gesetzgeberische Dynamik in einem Spannungsverhältnis zu der notwendigen Herausbildung eines systematischen und ganzheitlichen IT-Sicherheitsrechts – einem zentralen Anliegen der ersten Auflage dieses Handbuchs. Gleichwohl ist eine gewisse Konsolidierung bei der Gesetzgebung zu beobachten. Die Autorinnen und Autoren und die Herausgeber des Handbuchs hoffen, dass sie für die anstehende Phase der weiteren Konsolidierung der neuen Rechtsgrundlagen für Wissenschaft und Praxis Hinweise und Leitlinien aufzeigen können.

Die neue, vollständig überarbeitete und um etliche Kapitel ergänzte zweite Auflage behält die Grundkonzeption des Werks bei und gliedert sich in drei Teile, die Grundlagen der IT-Sicherheit (Teil 1), Grundlagen und Querschnittsfragen des IT-Sicherheitsrechts (Teil 2) sowie Sektorales IT-Sicherheitsrecht (Teil 3) behandeln. Ergänzt wurden im dritten Teil die Sektoren Justiz (§ 27), Gesundheitswesen (§ 28) und Finanzen (§ 29) sowie ein Kapitel zu den Herausforderungen des Zusammenspiels von IT-Sicherheit und Künstlicher Intelligenz (§ 30). Wir freuen uns sehr, dass wir mit diesen neuen Kapiteln das Handbuch in der zweiten Auflage thematisch ausbauen und aktuelle Entwicklungen berücksichtigen können.

Für diese neuen Kapitel konnten wir erfahrene, hochqualifizierte Autorinnen und Autoren gewinnen, die entsprechend der bisherigen Ausrichtung sowohl aus der Wissenschaft wie aus der Praxis des IT-Sicherheitsrechts stammen, dabei aber jeweils einen deutlichen Fokus auch auf die jeweils andere Dimension haben. Wir freuen uns sehr, dass wir außerdem mit nur ganz wenigen Ausnahmen unseren Autorenstamm erhalten konnten.

Sehr erschüttert hat uns der überraschende Tod unseres herausragenden Kollegen und Autors Gerald Spindler. Seine Kapitel (§§ 10-12) hat er nur wenige Tage vor seinem Tod übermittelt; es handelt sich um eine der letzten noch erscheinenden Publikationen aus seiner Feder. Erforderliche Überarbeitungen im Herstellungsprozess wurden von seinem Team, insbesondere von Dr. Andreas Seidel und Dr. Simon Gerdemann übernommen. Hierfür bedanken wir uns sehr.

Wie bei der ersten Auflage gilt unser Dank außerdem Herrn Dr. Marco Ganzhorn vom Nomos-Verlag für die hervorragende Zusammenarbeit beim Entstehen des Handbuchs. Am Fachgebiet von Gerrit Hornung an der Universität Kassel hat außerdem Max Büscher in besonderer Weise an der Überarbeitung mitgewirkt; auch hierfür bedanken wir uns

sehr herzlich. Für Rückmeldungen und Anregungen zur Neuauflage und zur Weiterentwicklung des Werks in der Zukunft würden wir uns sehr freuen.

Kassel und Berlin, im August 2024

Gerrit Hornung
Martin Schallbruch

Vorwort zur 1. Auflage

Rechtliche Fragestellungen in Bezug auf die IT-Sicherheit stellen sich Juristinnen und Juristen ebenso wie Rechtsanwenderinnen und Rechtsanwendern in steigendem Maße. Sei es bei der Vertragsgestaltung, beim betrieblichen oder behördlichen IT-Management, bei der Implementierung des Datenschutzes, bei der anwaltlichen Risikoberatung, bei der aufsichtsbehördlichen Tätigkeit, bei der Weiterentwicklung sektoraler Gesetzgebung im Hinblick auf die Digitalisierung: IT-Sicherheitsanforderungen, IT-Sicherheitsverfahren und die Konsequenzen nicht ausreichender IT-Sicherheit müssen stets bedacht werden.

Selten erschließt sich das IT-Sicherheitsrecht durch den Blick in eine einzelne, selbständige Rechtsvorschrift. Häufig führt die Zusammenschau verschiedener Aspekte und rechtlicher Regelungen zu den gesuchten Lösungen. Technische, ökonomische und gesellschaftliche Fragestellungen stellen einen Rahmen für eine IT-sicherheitsrechtliche Betrachtung dar. IT-Sicherheitsrecht selbst erschließt sich im Zusammenspiel aus querschnittlichen Regelungen, von der DS-GVO bis zum Zivilrecht, und sektoralen Spezialvorschriften, etwa im Energiesektor oder im Verkehr.

Das vorliegende Handbuch erleichtert die vollständige und ganzheitliche Betrachtung von Rechtsfragen der IT-Sicherheit. Hierbei wird eine wissenschaftliche Perspektive mit Erfahrungen aus der Praxis kombiniert. Gerade bei einer neuen Materie, die in Rechtsprechung und Literatur noch deutlich unterrepräsentiert ist, hilft diese Kombination beim schnellen und problemorientierten Verständnis von Fragestellungen, bereits verfügbaren Lösungen und schon absehbaren künftigen Entwicklungen.

Im ersten Teil des Handbuchs werden die technischen, ökonomischen und gesellschaftlichen Grundlagen der IT-Sicherheit beschrieben, zudem die IT-Sicherheit aus der Perspektive der Menschen, der Nutzerinnen und Nutzer der IT, analysiert.

Der zweite Teil beschreibt alle grundlegenden und querschnittlichen Fragen des IT-Sicherheitsrechts. Beginnend mit völker- und verfassungsrechtlichen Grundlagen über die Querschnittsfrage, welche rechtlichen Instrumente zur Messung und zum Nachweis von IT-Sicherheit sowie für spezielle Sicherheitsinfrastrukturen wie elektronische Signaturen zur Verfügung stehen, bis zur strafrechtlichen Verantwortung für IT-Sicherheitsverstöße werden übergreifende Themen adressiert. Einen besonderen Schwerpunkt nehmen die zivilrechtlichen Fragestellungen ein, vertragliche und deliktsrechtliche IT-Sicherheitsaspekte ebenso wie die speziellen Verantwortlichkeiten von IT-Herstellern, Intermediären oder Nutzerinnen und Nutzern der IT. Ergänzt wird dieser querschnittliche Teil durch die Beschreibung der Rechtsgrundlagen der einschlägigen Behörden und die Analyse des komplexen Zusammenwirkens von IT-Sicherheit und Datenschutz.

Im dritten Teil des Handbuchs werden sektorale Rechtsvorschriften zur IT-Sicherheit beschrieben, Normen für einzelne Branchen und Lebensbereiche, für die öffentliche Verwaltung ebenso wie für die privaten Haushalte.

Die einzelnen Kapitel des Handbuchs sind in sich geschlossene Darstellungen, die für sich genommen verständlich sind. Literaturangaben finden sich jeweils zu Beginn jedes Kapitels. Durch Verweisungen auf die anderen Kapitel wird der Zusammenhang der Themen hergestellt. Ein ausführliches Sachverzeichnis erleichtert zudem den Zugang zu den Kapiteln und den jeweiligen Randnummern.

Für das Handbuch konnten wir erfahrene Autorinnen und Autoren gewinnen, die jeweils auf ihrem Gebiet eine langjährige Expertise vorweisen können. Dem Anspruch des Handbuchs entsprechend stammt die Autorenschaft zu einem Teil aus der Wissenschaft, zu

einem Teil aus der Praxis. Wir konnten praxisorientierte akademische Expertinnen und Experten ebenso gewinnen wie wissenschaftlich interessierte Rechtsanwenderinnen und Rechtsanwender aus Unternehmen und Behörden sowie Verantwortliche aus der Ministerialverwaltung, die an der Gestaltung des IT-Sicherheitsrechts gearbeitet haben und arbeiten.

Das Handbuch befindet sich auf dem Stand April/Mai 2020. Die Autorinnen und Autoren konnten aber auch neuere Entwicklungen bis Juli 2020 berücksichtigen, wie etwa die IT-Sicherheitsfragen, die sich im Zusammenhang mit der SARS-CoV-2-Pandemie ergeben haben.

Herrn Dr. Marco Ganzhorn vom Nomos-Verlag danken wir für die hervorragende Zusammenarbeit beim Entstehen des Handbuchs. Dieses Handbuch ist eine Erstauflage. Für die Weiterentwicklung des Werks würden wir uns über Rückmeldungen jeder Art sehr freuen.

Kassel und Berlin, im August 2020

Gerrit Hornung
Martin Schallbruch

Inhaltsverzeichnis

Vorwort 5

Vorwort zur 1. Auflage 7

Bearbeiterverzeichnis 15

Abkürzungsverzeichnis 19

Teil 1
Grundlagen der IT-Sicherheit

§ 1 Einführung 29

A. IT-Sicherheit als Herausforderung für die Gesellschaft 29
B. Begriffliche Grundlagen 32
C. Spezifika rechtlicher Regelungen zur IT-Sicherheit 36
D. IT-Sicherheitsrecht als Rechtsgebiet im Entstehen 38

§ 2 IT-Sicherheit aus technischer Sicht 42

A. Grundlagen: Computer, Netzwerke und Sicherheit 44
B. Bedrohungen, Sicherheitsanforderungen und ihre Handhabung 49
C. Besondere Angriffstechniken 58
D. Grundlegende Schutzmaßnahmen 62
E. Entwicklungsperspektiven und aktuelle Forschung zur IT-Sicherheit 72

§ 3 IT-Sicherheit aus ökonomischer Perspektive 78

A. Grundlagen der Digitalisierung der Wirtschaft 80
B. Ökonomische Charakteristika der IT-Sicherheit 82
C. Kosten und Wirtschaftlichkeit von IT-Sicherheitsmaßnahmen 83
D. Wirtschaftliches Risiko mangelhafter IT-Sicherheit 86
E. IT-Sicherheit als Wettbewerbsfaktor 90

§ 4 IT-Sicherheit aus Nutzerinnen- und Nutzersicht 93

A. Einführung 93
B. Begrifflichkeiten Usability, Security, Privacy und Trust 94
C. „Usable Privacy and Security" (UPS) 98
D. Zusammenfassung 109

§ 5 IT-Sicherheit aus gesamtgesellschaftlicher Sicht 110

A. Begriffe IT-Sicherheit und Cybersicherheit 111
B. Wahrnehmung der IT-Sicherheit 113
C. Politikfeld IT-Sicherheit 120

Teil 2
Grundlagen und Querschnittsfragen des IT-Sicherheitsrechts

§ 6 Die völkerrechtliche Dimension der IT-Sicherheit 133

A. Einleitung 135
B. UN-Rechtsfindungsprozesse 135
C. Unilaterale und nichtstaatliche Initiativen 138
D. Anwendbarkeit friedensvölkerrechtlicher Regelungen 139
E. IT-Sicherheit durch Internet-Governance und internationales Exportkontrollrecht 155
F. Fazit und Ausblick 159

§ 7 Verfassungsrechtliche Dimensionen der IT-Sicherheit 160

A. Einleitung 161
B. Was ist IT-Sicherheit? 163
C. Besonderheiten und Herausforderungen der IT-Sicherheit 165
D. Verfassungsrechtliche Fragestellungen 168
E. Fazit und Ausblick 184

§ 8 Messung, Prüfung und Nachweis von IT-Sicherheit 185

A. Einleitung 187
B. Grundlagen der Prüfung und Bewertung von IT-Sicherheit 188
C. IT-Sicherheit in Organisationen 191
D. IT-Sicherheit von Software und Hardware 203

§ 9 IT-Sicherheit im Vertragsrecht und in der Vertragsgestaltung 218

A. Einleitung 221
B. IT-Sicherheit: ein Fall der Unmöglichkeit nach § 275 Abs. 1 BGB? 224
C. Cyberrisiko als höhere Gewalt? 225
D. IT-Sicherheit und Bestimmbarkeitsgrundsatz des Vertragsrechts 229
E. Bedürfnis einer vertraglichen Gestaltung der IT-Sicherheit 234
F. Vertragsrechtliche Implementierung von IT-Sicherheit als notwendiger Bestandteil des Cyberrisiko-Managements der Geschäftsleitung eines Unternehmens 239
G. Vertragsrechtliche Einordnung der IT-Sicherheitspflicht 242
H. Gewährleistung und schuldvertragliche Haftung für fehlende IT-Sicherheit 246
I. Inhaltliche Ausgestaltung von Vertragsklauseln zur IT-Sicherheit 267
J. Zusammenfassung und Ausblick 279

§ 10 Grundlagen deliktsrechtlicher Sicherheitspflichten 281

A. Pflichtenbestimmungen 289
B. Öffentlich-rechtliche Anforderungen und zivilrechtliche Haftung 296
C. Mitverschulden und Eigenschutz des Betroffenen 310

§ 11 Verantwortung der IT-Hersteller (produktbezogene Pflichten) 313
A. Überblick 313
B. Verschuldensabhängige Produzentenhaftung 315
C. Produkthaftung infolge Schutzgesetzverletzung (§ 823 Abs. 2 BGB): öffentlich-rechtliche Produktsicherheitsnormen 339
D. Verschuldensunabhängige Produkthaftung (ProdHaftG) 341
E. Haftung bei Open Source Produkten 350

§ 12 Verantwortung der Intermediäre, Betreiber und Nutzer 357
A. Haftung der Intermediäre 357
B. Haftung der Betreiber und Nutzer 362

§ 13 IT-Sicherheitsanforderungen an Kritische Infrastrukturen, Unternehmen im besonderen öffentlichen Interesse und digitale Dienste nach dem BSIG 370
A. Einführung 371
B. Kritische Infrastrukturen 371
C. Unternehmen im besonderen öffentlichen Interesse 402
D. Digitale Dienste nach dem BSIG 403

§ 14 IT-Sicherheitsinfrastrukturen und -dienste 410
A. Sicherheitsbedarf 413
B. Sicherheitsinfrastrukturen und -dienste 414
C. Recht der Sicherheitsinfrastrukturen und -dienste 419
D. Zusammenfassung und Ausblick 443

§ 15 Recht der IT-Sicherheitsbehörden 445
A. Einführung 446
B. Internationaler und europäischer Rahmen 447
C. Nationales Recht 458
D. Ausblick 474

§ 16 Rechtliche Regeln für die IT-Sicherheit in Organisationen 478
A. Gesetzliche Grundlagen 479
B. Innere Verantwortlichkeitsverteilung in Unternehmen 481
C. Typische Konfliktlinien 501
D. Best Practices in Organisationen im Hinblick auf IT 502
E. Ausblick auf zukünftige Gesetzesvorhaben 506

§ 17 IT-Sicherheit als Mittel und als Bedrohung des Datenschutzes 508
A. IT-Sicherheit und Datenschutz 509
B. Rechtliche Grundlagen 511
C. Ambivalenz und Aggregation von IT-Sicherheit und Datenschutz 527
D. Fazit 536

§ 18 Schutz der IT-Sicherheit durch Gefahrenabwehr, Strafverfolgung und nachrichtendienstliche Aufklärung 538
A. Allgemeines 540
B. Rechtsrahmen 540
C. Systematik der sicherheitsbehördlichen Maßnahmen zum Schutz der IT-Sicherheit 545
D. Akteure des behördlichen Schutzes der IT-Sicherheit und ihre Befugnisse 548
E. Fazit und Ausblick 559

§ 19 Aufgaben und Befugnisse der Bundeswehr 560
A. Cyberattacken und hybride Bedrohungen 561
B. Art. 87a GG – Verteidigung 562
C. Art. 24 Abs. 2 GG – Friedenssicherung 573
D. Friedensgebot und parlamentarische Kontrolle 574
E. Art. 35 GG – Amtshilfe und Katastrophennotstand 577
F. Gesetzliche Grundlagen zur Ausübung von Befugnissen gemäß Art. 87a Abs. 1 S. 1 und 2 GG, Art. 24 Abs. 2 GG sowie Art. 87a Abs. 3 GG 580

§ 20 Schutz der IT-Sicherheit durch das Strafrecht 582
A. Grundlagen 585
B. Tatbestände zum Schutz der Vertraulichkeit von Daten 597
C. Tatbestände zum Schutz der Integrität und Verfügbarkeit 606

Teil 3
Sektorales IT-Sicherheitsrecht

§ 21 Telekommunikation und digitale Dienste 617
A. IT-Anwendung und IT-Infrastrukturen 619
B. Besondere Risiken und Bedrohungen 631
C. Sektorale Rechtsvorschriften 639
D. Typische Problemlagen und Konfliktlinien 667
E. Ausblick 669

§ 22 Mobilität und Verkehr 671
A. IT-Anwendungen und IT-Infrastrukturen in den Verkehrsbranchen 674
B. Besondere Risiken und Bedrohungen 687
C. Sektorale Rechtsvorschriften im Bereich des Straßenverkehrs 693
D. Typische Problemlagen und Konfliktlinien 711
E. Fazit 715

§ 23 Energieversorgungsnetze und Energieanlagen 716
A. IT-Anwendungen und IT-Infrastrukturen 716
B. Besondere Risiken und Bedrohungen 718

C. Sektorspezifische Rechtsvorschriften im EnWG, Seitenblick auf das Atomgesetz (AtG) 719
D. Typische Problemlagen und Konfliktlinien 746

§ 24 Smart Metering 748

A. IT-Anwendungen und IT-Infrastrukturen 750
B. Besondere Risiken und Bedrohungen 752
C. Sektorale Rechtsvorschriften im MsbG 753
D. Typische Problemlagen und Konfliktlinien 773

§ 25 Öffentliche Verwaltung 778

A. Einleitung 780
B. Supranationales Recht 782
C. Bundes- und Landesrecht 787
D. Öffentliche Verwaltung als Kritische Infrastruktur 815
E. Zusammenarbeit zwischen Bund und Ländern 822
F. Fazit und Ausblick 828

§ 26 Private Haushalte 830

A. IT-Anwendungen und IT-Infrastrukturen 832
B. Besondere Risiken und Bedrohungen 837
C. Spezielle Rechtsvorschriften 846
D. Typische Problemlagen und Konfliktlinien 858

§ 27 Justiz 860

A. Einleitung 861
B. IT-Sicherheit in der Justizkommunikation 866
C. IT-Sicherheitsaspekte im Scanvorgang 888
D. Fazit und Ausblick 893

§ 28 Gesundheitswesen 894

A. Einleitung 896
B. IT-Anwendungen und IT-Infrastrukturen 896
C. Besondere Risiken und Bedrohungen 897
D. Sektorale Rechtsvorschriften 900
E. Typische Problemlagen und Konfliktlinien 933

§ 29 IT-Sicherheitsrecht im Finanzsektor 935

A. Einleitung 936
B. Anwendung des allgemeinen IT-Sicherheitsrechts im Finanzsektor 937
C. DORA (Digital Operational Resilience Act) 938
D. Besonderes IT-Sicherheitsrecht bei Banken 945
E. Besonderes IT-Sicherheitsrecht bei Versicherungen 957
F. Besonderes IT-Sicherheitsrecht bei Finanzintermediären 961

G. Vertragsgestaltung zu IT-Sicherheit im Finanzsektor 962
H. Fazit 968

§ 30 Zusammen- und Widerspiel von Künstlicher Intelligenz und IT-Sicherheit(srecht) 969

A. „Künstliche Intelligenz" – Annäherung an einen schillernden Begriff 970
B. Spezifische Problemstellungen 974
C. IT-Sicherheit von KI-Systemen 975
D. Gefahr für die IT-Sicherheit: KI als Angriffssystem 986
E. Mittel der IT-Sicherheit: KI als Präventions- und Reaktionsinstrument ... 989
F. Gewährleistungsrechte bei IT-Sicherheitsmängeln 990
G. Deliktische Haftung bei der Verletzung von IT-Sicherheitsanforderungen im Zusammenhang mit dem KI-Einsatz 992

Stichwortverzeichnis 997

Bearbeiterverzeichnis

Prof. Dr. Matthias Bäcker, LL.M. Johannes-Gutenberg-Universität Mainz	§ 18 (zus. mit *Golla*)
Prof. Dr. Irene Bertschek ZEW – Leibniz-Zentrum für Europäische Wirtschaftsforschung, Mannheim	§ 3 (zus. mit *Janßen*)
Dr. David Bomhard Physiker und Rechtsanwalt, München	§ 29 (zus. mit *Siglmüller*)
Lars Bostelmann, M.A., Mag.rer.publ. Leiter Referat IT-Recht, Hessisches Ministerium des Innern, für Sicherheit und Heimatschutz	§ 25
Matthias Fischer, LL.M. Regierungsdirektor, Berlin	§ 13
PD Dr. Christian L. Geminn, Mag. iur. Universität Kassel	§ 22 (zus. mit *Müller*)
Dr. Rotraud Gitter, LL.M. Eur. Regierungsdirektorin, Berlin	§ 15
Jun.-Prof. Dr. Sebastian J. Golla Ruhr-Universität Bochum	§ 18 (zus. mit *Bäcker*)
Prof. Dr. Rüdiger Grimm Universität Koblenz	§ 2 (zus. mit *Waidner*)
Prof. Dr. Annette Guckelberger Universität des Saarlandes, Saarbrücken	§ 23
Dr. h.c. Marit Hansen Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Kiel	§ 26
Prof. Dr. Andreas Heinemann Hochschule Darmstadt	§ 4 (zus. mit *Margraf*)
Prof. Dr. Gerrit Hornung, LL.M. Universität Kassel	§ 1 (zus. mit *Schallbruch*) § 21 (zus. mit *Schindler*)

Dr. habil. Silke Jandt Stellvertretende Referatsleiterin bei dem Landesbeauftragten für den Datenschutz Niedersachsen	§ 17
Rebecca Janßen ZEW – Leibniz-Zentrum für Europäische Wirtschaftsforschung, Mannheim	§ 3 (zus. mit *Bertschek*)
Christian Kuß, LL.M. Rechtsanwalt, Köln	§ 28
Dr. Henning Lahmann Assistant Professor, Center for Law and Digital Technologies, Universiteit Leiden	§ 6
Dr. Philipp Lassahn, LL.M. Oberregierungsrat, Berlin	§ 7 (zus. mit *Poscher*)
Ann-Sophie Letzel Universität Potsdam	§ 30 (zus. mit *Steinrötter*)
Prof. Dr. Marian Margraf Freie Universität Berlin	§ 4 (zus. mit *Heinemann*)
Prof. Dr. Henning Müller Direktor des Sozialgerichts, Darmstadt; Honorarprofessor der Hochschule für Wirtschaft und Gesellschaft, Ludwigshafen	§ 27
Johannes Müller MLE. Staatsanwaltschaft Mühlhausen/Thüringen	§ 22 (zus. mit *Geminn*)
Prof. Dr. Ralf Poscher Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht, Freiburg	§ 7 (zus. mit *Lassahn*)
Dr. Mansur Pour Rafsendjani Rechtsanwalt, München	§ 9
Prof. Dr. Alexander Roßnagel Hessischer Beauftragter für Datenschutz und Informationsfreiheit	§ 14
Martin Schallbruch Ministerialdirektor a.D., Vorstand, govdigital eG, Berlin	§ 1 (zus. mit *Hornung*) § 5

Dr. Stephan Schindler Universität Kassel	§ 21 (zus. mit *Hornung*)
Dr. Jonas Siglmüller Rechtsanwalt und Softwareentwickler, München	§ 29 (zus. mit *Bomhard*)
Prof. Dr. Tobias Singelnstein Goethe-Universität Frankfurt a.M.	§ 20 (zus. mit *Zech*)
Philipp Singler Justiziar und Abteilungsleiter Recht und Datenschutz Stadt Offenburg; Lehrbeauftragter	§ 24
Dr. Isabel Skierka-Canton Digital Society Institute, European School of Management and Technology Berlin	§ 8
Sylvia Spies-Otto Ministerialdirigentin a.D., Bundesministerium der Verteidigung, Brandenburg	§ 19
Prof. Dr. Gerald Spindler Georg-August-Universität Göttingen	§§ 10 bis 12
Prof. Dr. Björn Steinrötter Universität Potsdam	§ 30 (zus. mit *Letzel*)
Dr. Thomas Thalhofer Rechtsanwalt, München	§ 16
Prof. Dr. Michael Waidner ATHENE | TU Darmstadt | Fraunhofer-Institut für Sichere Informationstechnologie SIT, Darmstadt	§ 2 (zus. mit *Grimm*)
Louisa Zech Goethe-Universität Frankfurt a.M.	§ 20 (zus. mit *Singelnstein*)

Autoren in der 1. Auflage:

Marc Schardt Regierungsdirektor, Berlin	§ 25
Dr. Jörg Ohnemus ZEW – Leibniz-Zentrum für Europäische Wirtschaftsforschung, Mannheim	§ 3 (zus. mit *Bertschek/Janßen*)

§ 1 Einführung

Literatur: *Baer*, Das Soziale und die Grundrechte, NZS 2014, 1; *Barczak*, Der nervöse Staat, 2020; *Berman*, Digital transformation: opportunities to create new business models, Strategy & Leadership, Jg. 40, Nr. 2, 2012, 16; *BMDV*, Digitalstrategie, Stand: 25.4.2023, https://digitalstrategie-deutschland.de; *Brill*, Welt- und sicherheitspolitische Trends im Spektrum der Meinungen: Thesen – Antithesen – Synthesen, ZfP 2001, 448; *Debus*, Errichtung der Cybersicherheitsagentur Baden-Württemberg durch neues Cybersicherheitsgesetz, VBlBW 2021, 495; *Eckert*, IT-Sicherheit: Konzepte – Verfahren – Protokolle, 11. Aufl. 2023; *Erbel*, Öffentliche Sicherheit und Ordnung, DVBl 2001, 1714; *Freimuth*, Die Gewährleistung der IT-Sicherheit Kritischer Infrastrukturen, 2018; *Ganz*, Die Netzbewegung. Subjektpositionen im politischen Diskurs der digitalen Gesellschaft, 2018; *Gusy*, Vom „Neuen Sicherheitsbegriff" zur „Neuen Sicherheitsarchitektur", in: Würtenberger/Gusy/Lange (Hrsg.), Innere Sicherheit im europäischen Vergleich. Sicherheitsdenken, Sicherheitskonzepte und Sicherheitsarchitektur im Wandel, 2012, 71; *Gusy/Kugelmann/Würtenberger* (Hrsg.), Rechtshandbuch Zivile Sicherheit, 2017; *Hammer/Pordesch/Roßnagel*, Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet, 1993; *Isensee/Kirchhof* (Hrsg.), Handbuch des Staatsrechts: Band IV, 2006; *Kaufmann*, Zivile Sicherheit: Vom Aufstieg eines Topos, in: Hempel/Krasmann/Bröckling (Hrsg.), Sichtbarkeitsregime. Überwachung, Sicherheit und Privatheit im 21. Jahrhundert, 2011, 101; *Kipker*, Cybersecurity, 2. Aufl. 2023; *Kniesel*, „Innere Sicherheit" und Grundgesetz, ZRP 1996, 482; *Kugelmann*, Polizei- und Ordnungsrecht, 2. Aufl. 2012; *von Lewinski* (Hrsg.), Resilienz des Rechts, 2016; *Matt/Hess/Benlian*, Digital Transformation Strategies, Business & Information Systems Engineering, Jg. 57, Nr. 5, 2015, 339; *National Institute of Standards and Technology (NIST)*, NIST Special Publication 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information, 2022; *Proff/Fojcik* (Hrsg.), Mobilität und digitale Transformation. Technische und betriebswirtschaftliche Aspekte, 2018; *Raabe/Schallbruch/Steinbrück*, Systematisierung des IT-Sicherheitsrechts. Ein Beitrag zu einem konstruktiven Strukturentwurf, CR 2018, 706; *Rehbohm/Kalmbach*, Herausforderungen der föderalen Cybersicherheit vs. Änderung in der Bund-Länder Gewaltenteilung, DuD 2023, 338; *Riznik*, Überlegungen zur Resilienz des Rechts, in: Pelizäus/Nieder (Hrsg.), Das Risiko – Gedanken übers und ins Ungewisse, 2019, 243; *Roßnagel*, Rechtswissenschaftliche Gestaltung der Informationstechnik, in: Kortzfleisch/Bohl (Hrsg.): Wissen, Vernetzung, Virtualisierung, Festschrift für Winand, 2008, 381; *Roßnagel/Hornung/Geminn/Johannes* (Hrsg.), Rechtsverträgliche Technikgestaltung und technikadäquate Rechtsentwicklung, 2018; *Schallbruch*, IT-Sicherheitsrecht – Schutz kritischer Infrastrukturen und staatlicher IT-Systeme, CR 2017, 648; *Schallmo/Rusnjak/Anzengruber/Werani/Jünger* (Hrsg.), Digitale Transformation von Geschäftsmodellen, 2017; *Schumacher/Roedig/Moschgath*, Hacker Contest. Sicherheitsprobleme, Lösungen, Beispiele, 2003; *Simitis/Hornung/Spiecker gen. Döhmann* (Hrsg.), Datenschutzrecht, 2019; *Stiftung Neue Verantwortung*, Deutschlands staatliche Cybersicherheitsarchitektur, 11. Aufl. 2023; *Tanneberger*, Die Sicherheitsverfassung. Eine Systematische Darstellung der Rechtsprechung des Bundesverfassungsgerichts. Zugleich ein Beitrag zu einer induktiven Methodenlehre, 2014; *van Daalen*, The right to encryption: Privacy as preventing unlawful access, CLSR 49 (2023) 105804; *Waechter*, Die Schutzgüter des Polizeirechts, NVwZ 1997, 729; *Winkelhake*, Die digitale Transformation der Automobilindustrie. Treiber – Roadmap – Praxis, 2017; *Wischmeyer*, Informationssicherheit, 2023; *Wittpahl* (Hrsg.), Resilienz. Leben – Räume – Technik, 2022; *Zeuch*, Keine digitale Transformation ohne soziale Innovation, in: Hildebrandt/Landhäußer (Hrsg.), CSR und Digitalisierung. Der digitale Wandel als Chance und Herausforderung für Wirtschaft und Gesellschaft, 2. Aufl. 2021, S. 745.

A. IT-Sicherheit als Herausforderung für die Gesellschaft 1
B. Begriffliche Grundlagen 10
I. IT und IT-Sicherheit 11
II. IT-Sicherheitsrecht 20
C. Spezifika rechtlicher Regelungen zur IT-Sicherheit 24
D. IT-Sicherheitsrecht als Rechtsgebiet im Entstehen 33

A. IT-Sicherheit als Herausforderung für die Gesellschaft

Die **Bedeutung der IT-Sicherheit** hat sich in den letzten Jahren und Jahrzehnten fundamental **gewandelt**. Solange Informationstechnik aus abgrenzbaren, oftmals nicht oder 1

wenig vernetzten Rechenanlagen bestand, bezog sich IT- (oder Computer-)Sicherheit lediglich auf die entsprechende Hard- und Software dieser Anlagen. Diese waren aus heutiger Sicht wenig komplex und gut beherrschbar, IT-Sicherheit damit eine Aufgabe für wenige Spezialisten, Defizite der IT-Sicherheit mithin kein Thema für die Öffentlichkeit, sondern höchstens ein temporäres Problem für die Betreiber von Großrechenanlagen.

2 Mit der Verfügbarkeit von PCs für immer mehr Menschen ab dem Ende der 1970er Jahre und der einsetzenden Vernetzung beginnt IT-Sicherheit eine Materie für **immer mehr Technikbegeisterte** zu werden. Der – in der Szene positiv, ansonsten unterschiedlich besetzte – Begriff des Hackers etabliert sich,[1] und es entstehen feste Gruppierungen wie der deutsche Chaos Computer Club (CCC), der im Jahre 1981 in Hamburg gegründet wird.[2] Mit Aktionen wie dem sog. „Btx-Hack"[3] wird die Szene bekannt und IT-Sicherheit auch ein Thema für die breitere Öffentlichkeit, auch wenn sie für viele Menschen (wie die Informatik insgesamt) für viele Jahre noch mit dem Bild des „Nerds" konnotiert bleibt.

3 Auch in dieser Phase fehlte es für viele Menschen noch an einer unmittelbaren Relevanz der IT-Sicherheit für ihre eigenen Lebenswelten. Dies hat sich in jüngerer Zeit jedoch fundamental geändert. Seit etlichen Jahren – ein genauer Zeitpunkt lässt sich nicht festmachen, da es sich um fortdauernde Prozesse mit vielen miteinander verwobenen Einflussfaktoren handelt – befinden wir uns in einer Phase der umfassenden Einführung immer leistungsfähigerer, immer kleinerer, immer stärker vernetzter Informationstechnologie, die als **Digitalisierung**[4] oder **digitale Transformation**[5] bezeichnet wird.

4 Dieser Prozess betrifft uns alle. Immer mehr Lebensbereiche werden durch Informations- und Kommunikationstechnologie grundlegend verändert. Das gilt für alle Branchen der **Wirtschaft** und die öffentliche **Verwaltung** ebenso wie für den **Alltag der Menschen**. Vom Arbeitsleben über den privaten Haushalt bis zur Freizeitgestaltung spielen Technologien eine wachsende Rolle. Selbst dort, wo die Nutzung digitaler Geräte nicht im Vordergrund steht, wird alltägliches Leben digital begleitet: Rauchmelder funken Betriebszustände, Autos empfangen neue Navigationsinformationen und kommunizieren umfassend mit Backend-Systemen der Hersteller, Insulinpumpen können von Ärzten aus der Ferne gewartet werden.

---

1 Ein guter Abriss der Geschichte des Hacking mit Beispielen findet sich bei Schumacher/Roedig/Moschgath, Hacker Contest, S. 71 ff.

2 Ganz, Die Netzbewegung, S. 26.

3 Ganz, Die Netzbewegung, S. 28.

4 Der Begriff der Digitalisierung hat in den letzten Jahren einen beispiellosen Siegeszug gehalten. Dies betrifft zunächst wissenschaftliche und praktische Diskussionen zu den Fragen der zugrunde liegenden Technologien, hat sich inzwischen aber auf viele andere Felder erstreckt. In verschiedenen Wissenschaftsdisziplinen (einschließlich der Rechtswissenschaften) werden unter dem Begriff inzwischen so unterschiedliche Dinge diskutiert, dass dies hier nicht nachgezeichnet werden kann. Die Bedeutung in der Politik zeigt sich nicht zuletzt daran, dass Regierungen sowohl auf Bundes- wie auf Landesebene „Digitalisierungsstrategien" verabschieden, die jeweils eine Fülle von Digitalisierungsvorhaben zusammenfassen (für den Bund: BMDV, Digitalstrategie, Stand 25.4.2023).

5 Der Begriff der digitalen Transformation wird bislang vor allem in den Wirtschaftswissenschaften verwendet und bezeichnet dort die durch digitale Technologien und die darauf basierenden sozialen Verhaltensweisen bedingten Veränderungsprozesse in Unternehmen (v.a. Digitalisierung bestehender und Entstehung neuer Geschäftsmodelle), s. Berman, Strategy & Leadership 40 (2012) 2, 16; Matt/Hess/Benlian, Business and Information Systems Engineering, 57 (2015) 5, 339; paradigmatische Verwendungen zB: Proff/Fojcik (Hrsg.), Mobilität und digitale Transformation. Technische und betriebswirtschaftliche Aspekte; Schallmo/Rusnjak/Anzengruber/Werani/Jünger (Hrsg.), Digitale Transformation von Geschäftsmodellen; Winkelhake, Die digitale Transformation der Automobilindustrie; zur bisher noch heterogenen Begriffsbildung s. die Nachweise bei Schallmo/Rusnjak in Schallmo/Rusnjak/Anzengruber/Werani/Jünger (Hrsg.), Digitale Transformation von Geschäftsmodellen, S. 3 ff.; zum Zusammenhang mit sozialen Innovationen in Unternehmen Zeuch in Hildebrandt/Landhäußer (Hrsg.), CSR und Digitalisierung, S. 745 ff.

Diese Entwicklung eröffnet **unvergleichliche Chancen** für das Leben der Menschen, hat aber auch eine gewisse Ambivalenz in sich, die das Bundesverfassungsgericht schon vor über 15 Jahren betont hat: „Die jüngere Entwicklung der Informationstechnik hat dazu geführt, dass informationstechnische Systeme allgegenwärtig sind und ihre Nutzung für die Lebensführung vieler Bürger von zentraler Bedeutung ist."[6] Mit der Durchdringung aller Lebensbereiche durch IT-Systeme wächst nämlich auch die **Abhängigkeit** von ihnen. Der Ausfall eines Systems, etwa einer Insulinpumpe, kann ebenso gravierende Folgen haben wie eine Fehlfunktion, etwa eines Fahrassistenten im Auto, das Auslesen von Daten, etwa eines Geschäftsgeheimnisses, oder das Manipulieren von Daten, zB eines Börsenkurses. 5

Neben die individuelle Abhängigkeit jedes Einzelnen von der Integrität, Vertraulichkeit und Verfügbarkeit seiner Systeme[7] treten weitere Abhängigkeiten. Praktisch **alle Unternehmen** sind heute auf die Sicherheit der von ihnen eingesetzten IT angewiesen; in bestimmten Fällen können IT-Sicherheitsvorfälle sogar unmittelbar existenzbedrohlich sein.[8] Ähnliches gilt für andere gesellschaftliche Organisationen und **staatliche Behörden**. Hinzu tritt seit einiger Zeit eine darüber hinausreichende **gesellschaftliche Abhängigkeit** von funktionierender IT, etwa beim Betrieb der Energieversorgung oder auch bei einer fairen und ordnungsgemäßen Durchführung politischer Wahlen.[9] **Kritische Infrastrukturen** können heutzutage nicht mehr sinnvoll ohne IT betrieben werden und sind deshalb essentiell auf IT-Sicherheit angewiesen. 6

Der angemessene Schutz von IT-Systemen aller Art ist damit ein **gesamtgesellschaftlicher Auftrag** geworden, national wie international. Die Bedeutung dieses Auftrags – der sich verfassungsrechtlich aus der Kernaufgabe des modernen Staates zur Gewährleistung von Sicherheit ableitet[10] – ergibt sich aus der wachsenden Abhängigkeit von Individuen, Organisationen und Gesellschaft und wird verschärft durch die gleichfalls wachsenden **Bedrohungen für die IT-Sicherheit** (dazu *Grimm/Waidner* in → § 2 Rn. 17 ff.). In dem Maße, in dem Lebensgestaltung digital erfolgt, steigt die Attraktivität für verschiedenste Akteure, ihre Interessen durch eine Manipulation von IT-Systemen und damit unseres digitalisierten Lebens durchzusetzen. 7

Kriminelle Aktivitäten (Cybercrime) nehmen in Form und Anzahl stetig zu, vom Datendiebstahl über Erpressung bis zur Manipulation von Zahlungsverfahren.[11] Nachrichtendienste führen Cyberoperationen durch, beispielsweise zur Wirtschaftsspionage oder zur Destabilisierung anderer Staaten (*Grimm/Waidner* in → § 2 Rn. 60 ff.). Auch als neuartige Instrumente politischen Aktivismus haben sich das Hacking von IT-Systemen oder die Störung von digitalen Diensten etabliert. Gefährdungen können sich nicht nur aus dem **Missbrauch von IT-Systemen** ergeben, sondern auch aus dem **Gebrauch**. Vernetzte digitale Systeme können ihren Verantwortlichen neue Möglichkeiten einer gefährlichen Manipulation anderer Menschen an die Hand geben, wenn die IT-Systeme nicht verantwortungsvoll eingesetzt werden. 8

Der Schutz der IT-Sicherheit als Kern eines Schutzes unserer digitalen Welt ist spätestens seit den Veröffentlichungen von Edward Snowden im Sommer 2013 eine der Prioritäten 9

6 BVerfGE 120, 274 (303) – Online-Durchsuchung; s. näher Poscher/Lasahn in → § 7 Rn. 25 ff.
7 S. zur Bedeutung von IT-Sicherheit für den Einzelnen Hansen in § 26.
8 Zu den wirtschaftlichen Risiken von Cyberangriffen s. näher Bertschek/Janßen in → § 3 Rn. 21 ff.
9 S. etwa die Warnungen der ENISA im Vorfeld der Europawahlen 2024, https://www.heise.de/-9340315.html.
10 S. BVerfGE 49, 24 (56 f.): Der Staat gewährleistet als „verfasste Friedens- und Ordnungsmacht" die Sicherheit seiner Bevölkerung. Es handelt sich um ein hochrangiges Gut mit Verfassungsrang, aus dem der Staat als Institution „die eigentliche und letzte Rechtfertigung herleitet". IT-Sicherheit ist außerdem Teil der Schutzpflichtendimension der Grundrechte, s. BVerfGE 158, 170 (185 f.); BVerfG NVwZ-RR 2022, 401 Rn. 17; näher Wischmeyer, Informationssicherheit, 2023, S. 77 ff., 184 ff.
11 S. zu den entsprechenden Straftatbeständen Singelnstein/Zech in → § 20 Rn. 37 ff.

deutscher und europäischer Politik. **Rechtliche Instrumente** sind hierbei ganz wesentliche Handlungsmittel. Diese haben sich bisher allerdings vielfach nicht systematisch, sondern ad hoc und anlassbezogen entwickelt und finden sich in vielen verschiedenen hergebrachten Rechtsgebieten. Die Instrumente weisen dennoch viele Gemeinsamkeiten und Querbezüge auf, ergänzen sich gegenseitig und beginnen damit, ein eigentümliches, querschnittsartiges Rechtsgebiet herauszubilden. **Gegenstand dieses Handbuchs sind der derzeitige Stand und die Zukunft dieses „IT-Sicherheitsrechts"**. Hierbei nehmen wir eine im Wesentlichen deutsche, ergänzend auch die europäische Perspektive ein.

B. Begriffliche Grundlagen

10 **Weder in der Informatik noch im Recht** oder in den Rechtswissenschaften existiert ein abschließender, übergreifender Begriff der IT-Sicherheit oder des IT-Sicherheitsrechts. Der konkrete Inhalt variiert nicht nur nach individuellem Vorverständnis, sondern auch nach der Funktion der Begriffsbildung (Beschreibung eines Gegenstandsbereichs, Abgrenzung zu anderen Begriffen etc).[12] Beide Begriffsbestandteile (IT und Sicherheit) lassen sich **eng oder weit verstehen**. Außerdem existieren etliche verwandte, angrenzende und teilweise überlappende Phänomene, zu denen man eine scharfe Abgrenzung versuchen oder für die man eine gegenseitige Überlagerung tolerieren kann. Ersteres führt tendenziell zu einer Verengung, letzteres zu einer Erweiterung des Begriffs.

I. IT und IT-Sicherheit

11 Der Begriff der **Informationstechnik** beschreibt in einem allgemeinen Sinne Systeme aus Hard- und Software sowie die auf ihnen ablaufenden, der Verarbeitung von Informationen dienenden (elektronischen) Datenverarbeitungsprozesse. Das BSI-Gesetz versteht Informationstechnik sogar etwas weiter als „alle technischen Mittel zur Verarbeitung von Informationen" (§ 2 Abs. 1 BSIG), insofern auch nicht-elektronische technische Mittel der Informationsverarbeitung.

12 Was genau **Sicherheit** bezeichnet, ist deutlich schwieriger zu bestimmen. Eine erste, hilfreiche Differenzierung vermag ein Blick auf die englische Sprache zu vermitteln, die über zwei Begriffe verfügt (*Margraf/Heinemann* in → § 4 Rn. 8). „**Safety**" bezeichnet dort die (Betriebs-)Sicherheit, also die Eigenschaft des Systems, bestimmte Funktionen so zu erfüllen, wie dies erwartet wird. Dies kann zB auch vorbeugende Maßnahmen gegen den Ausfall durch Verschleiß oder Schäden für Leib und Leben umfassen. Demgegenüber ist „**Security**" die Eigenschaft eines Systems, gegen missbräuchliche, nicht autorisierte Zugriffe geschützt zu sein. Safety schützt also vor einem technischen Gerät, Security schützt das Gerät selbst vor Einwirkungen (und damit mittelbar auch die Safety).

13 In erster Näherung wird **IT-Sicherheit** üblicherweise mit **drei Schutzzielen** beschrieben, die sich aus diesen beiden Sicherheitsdimensionen ableiten:

- **Vertraulichkeit** bezeichnet die Eigenschaft von Daten und Systemen, nur für autorisierte Benutzer zugänglich zu sein.
- Mit **Integrität** wird beschrieben, dass Daten und Systeme nicht veränderbar sind oder jede Veränderung nachvollziehbar ist.

12 Um Vorverständnisse und Funktionen der Begriffsbildung nicht einzuengen, wurde bewusst darauf verzichtet, den Autorinnen und Autoren dieses Handbuchs einen Begriff der IT-Sicherheit vorzugeben. Dementsprechend finden sich zumindest moderat divergierende Definitionen, was bei der Benutzung des Handbuchs zu beachten ist.

- Auch die **Verfügbarkeit** kann sich sowohl auf Daten als auch auf Systeme beziehen und meint ihre Nutzbarkeit innerhalb definierter Zeiträume.

In diesem relativ generischen Sinne wird „Sicherheit in der Informationstechnik" auch in **§ 2 Abs. 2 Satz 4 BSIG** legaldefiniert. Diese bezeichnet dort „die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen betreffen" und bezieht auch die Zielrichtung entsprechender Sicherheitsvorkehrungen in die Definition mit ein. Diese werden entweder „in informationstechnischen Systemen, Komponenten oder Prozessen" oder „bei der Anwendung" derselben vorgenommen. Der seit einigen Jahren stark verwendete Begriff der **Cybersicherheit** weist sehr hohe Überschneidungen zur IT-Sicherheit auf und wird häufig synonym verwendet.[13] Bezüge und Überlappungen bestehen auch zum Begriff der **Resilienz**, der inzwischen in mehreren Rechtsakten der Europäischen Union verwendet wird.[14] Art. 2 Nr. 2 CER-RL definiert ihn als „Fähigkeit einer kritischen Einrichtung, einen Sicherheitsvorfall zu verhindern, sich davor zu schützen, darauf zu reagieren, einen solchen abzuwehren, die Folgen eines solchen Vorfalls zu begrenzen, einen Sicherheitsvorfall aufzufangen, zu bewältigen und sich von einem solchen Vorfall zu erholen".[15] Über das Ziel der IT-Sicherheit hinaus (die sich v.a. darauf richtet, bestimmte Schutzziele zu erreichen) geht es bei Resilienz auch darum, durch eine Adaption an eine Krisensituation (zB technische Umkonfigurationen) einen Notfallbetrieb mit Basisfunktionalitäten aufrechtzuerhalten oder eine schnelle Wiederherstellung des Betriebs zu ermöglichen.[16] 14

Je nach Technologie und Anwendungsgebiet sind in der Literatur **weitere Schutzziele** der IT-Sicherheit entwickelt worden. Dies betrifft beispielsweise Authentizität (Echtheit und Glaubwürdigkeit), Nichtabstreitbarkeit (einer Handlung) oder – an sich dem Datenschutzrecht zuzuordnen – Anonymität und Pseudonymität.[17] Authentizität und Nichtabstreitbarkeit sind insbesondere im elektronischen Rechtsverkehr von erheblicher Bedeutung. 15

Eine so verstandene IT-Sicherheit lässt sich von angrenzenden, verwandten und teilweise überlappenden Begriffen und Konzepten abgrenzen. So ist der Begriff der „**Informationssicherheit**" insofern weiter, als er nicht die Verwendung von Informationstechnologie beinhaltet und auch die Sicherheit herkömmlich (dh etwa in Papierakten) enthaltener 16

13 Siehe näher Schallbruch in → § 5 Rn. 6 f. Die Definition von „Cybersicherheit" in Art. 2 Nr. 1 des europäischen Rechtsakts zur Cybersicherheit (Verordnung (EU) 2019/881) – „alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen" – machte die hohe Überschneidung zur Cybersicherheit deutlich. Verwendung als Oberbegriff zB bei Kipker Cybersecurity-HdB/Kipker Kap. 1 Rn. 4.

14 S. die RL über die Resilienz kritischer Einrichtungen (im Englischen als „Critical Entities Resilience Directive" bezeichnet, deshalb auch im Deutschen oftmals „CER-Richtlinie") v. 14.12.2022, ABl. L 333, 164 und die als „Cyber Resilience Act" bezeichnete geplante VO über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen, für die im Dezember 2023 eine politische Einigung im Trilog erzielt wurde.

15 Die Definitionen variieren im Übrigen, s. zB NIST Special Publication 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information, S. 40: Cyberresilienz als "The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources".

16 Vgl. zum Begriff der Resilienz im rechtwissenschaftlichen Diskurs: v. Lewinski (Hrsg.), Resilienz des Rechts, 2016; Barczak, Der nervöse Staat, 2020, S. 603 ff.; Pelizäus/Nieder (Hrsg.), Das Risiko – Gedanken übers und ins Ungewisse/Riznik, 2019, S. 243 ff. Eine Übersicht zur Diskussion in anderen Disziplinen bieten die Beiträge in Wittpahl (Hrsg.), Resilienz. Leben – Räume – Technik, 2022.

17 S. insgesamt zB Eckert, IT-Sicherheit: Konzepte – Verfahren – Protokolle, S. 7 ff.

Informationen umfasst.[18] Auch der im Datenschutzrecht häufig verwendete Begriff der „**Datensicherheit**" geht in diese Richtung (s. zB *Jandt* in → § 17 Rn. 3).

17 Zwischen **Datenschutz und IT-Sicherheit** besteht eine enge Wechselbeziehung. Gerade deshalb müssen die Begriffe aber voneinander getrennt werden. Datenschutz bezweckt nach Art. 1 Abs. 2 DS-GVO den Schutz von Grundrechten und Grundfreiheiten natürlicher Personen, insbesondere (aber keineswegs nur)[19] ihres Rechts auf Schutz personenbezogener Daten. Dieser Schutz ist schon seit langem, insbesondere aber in der heutigen Zeit ohne IT-Sicherheit nicht mehr vorstellbar. Deshalb existieren im Datenschutzrecht schon seit dem ersten Bundesdatenschutzgesetz von 1977 (dort § 6 und Anlage) **Vorschriften zur IT-Sicherheit**. Aktuell macht Art. 32 DS-GVO entsprechende Vorgaben („Sicherheit der Verarbeitung"), die bei jeder Verarbeitung personenbezogener Daten zu beachten sind (s. näher *Jandt* in → § 17 Rn. 33 ff.). IT-Sicherheit hat hier also eine dienende Funktion, und ihre Einhaltung ist nur eine von vielen datenschutzrechtlichen Pflichten: Es reicht nicht aus, IT-Sicherheit zu beachten, um sich datenschutzkonform zu verhalten.

18 Dementsprechend ist der Begriff der IT-Sicherheit **einerseits enger** als der des Datenschutzes. Der zentrale Unterschied liegt darin, dass das Datenschutzrecht materielle Verarbeitungsbeschränkungen (zB die Existenz einer Rechtsgrundlage nach Art. 6 DS-GVO und die Einhaltung der Grundsätze nach Art. 5 DS-GVO) und verfahrenstechnische Anforderungen (zB die Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO oder die Bestellung eines Datenschutzbeauftragten nach Art. 37 DS-GVO) enthält, die über die Sicherheit der Verarbeitung weit hinausgehen.

19 Allerdings ist der Begriff der IT-Sicherheit **andererseits** auch **weiter** als der des Datenschutzes. Denn das Datenschutzrecht ist in seinem Schutzzweck (Art. 1 Abs. 2 DS-GVO) und seinem Anwendungsbereich (Art. 2 Abs. 1, Art. 4 Nr. 1 DS-GVO) auf Daten über natürliche Personen beschränkt. M.a.W. ist die Sicherheit der Verarbeitung von Betriebs- und Geschäftsgeheimnissen oder vertraulichen Behördeninformationen nicht erfasst, sondern unterliegt Sonderregimen. Technisch besteht demgegenüber vielfach eine hohe Kongruenz der eingesetzten Sicherungsmaßnahmen.

II. IT-Sicherheitsrecht

20 Der technische Begriff der IT-Sicherheit ist weder auf eine konkrete Technologie noch auf einen bestimmten Lebensbereich bezogen, sondern bezeichnet Eigenschaften von Hard- und Software, die in sehr unterschiedlichen Bereichen eingesetzt werden können. In Verbindung mit der erläuterten umfassenden Bedeutung von IT-Sicherheit für das Leben der Menschen, für ihre Kommunikation mit anderen, für die Funktionsfähigkeit von Unternehmen, Behörden und anderen Organisationen und Organen und letztlich für die Gesellschaft insgesamt bietet sich deshalb auch ein **weites Verständnis** des Begriffs des **IT-Sicherheitsrechts** an. In der Konzeption dieses Handbuchs verstehen wir darunter rechtliche Regelungen, die

- Vorgaben für die Umsetzung der Schutzziele der IT-Sicherheit machen oder Anreize für eine Umsetzung bilden,
- verfahrensrechtliche Bestimmungen zur Kontrolle der Einhaltung derartiger Umsetzungsvorgaben enthalten,

18 Die relevante Norm ISO/IEC 27000:2018 definiert Informationssicherheit ganz allgemein als den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen.

19 Die DS-GVO schützt auch weitere Grundrechte (v.a. im Bereich der Diskriminierungsvermeidung) sowie die Grundfreiheiten, s. Simitis/Hornung/Spiecker gen. Döhmann/Hornung/Spiecker gen. Döhmann DS-GVO Art. 1 Rn. 32, 36 ff.

- individuelle Rechte auf ein bestimmtes Maß an IT-Sicherheit bei IT-Produkten oder digitalen Diensten einräumen,
- staatliche Sanktionen oder private Ansprüche für den Fall bestimmen, dass Pflichten zur Umsetzung von IT-Sicherheitsmaßnahmen verletzt werden,
- rechtlich regulierte Instrumente zur Bewertung von IT-Sicherheit bereitstellen,
- Befugnisse von Behörden, Unternehmen und Privaten vorsehen oder beschränken, IT-Sicherheitsmaßnahmen zu umgehen oder zu brechen,
- die Organisation und die Entscheidungsprozesse von Behörden, Unternehmen und anderen Institutionen regeln, die sich mit IT-Sicherheit befassen.

Dieser weite Begriff des IT-Sicherheitsrechts ist nicht trennscharf zu anderen Begriffen und Rechtsgebieten. So bilden beispielsweise **Datenschutzrecht** und IT-Sicherheitsrecht **überlappende Kreise**: Art. 32 DS-GVO ordnet unter der Überschrift „Sicherheit der Verarbeitung" die Anwendung technischer IT-Sicherheitsmaßnahmen an, die den og Schutzzielen entsprechen; in dieser Hinsicht gehört die Vorschrift zum IT-Sicherheitsrecht im hier verstanden Sinne (engeres Verständnis zB bei *Jandt* in → § 17 Rn. 9). Sinn und Zweck der Norm ist allerdings – wie sich aus Art. 32 Abs. 1 DS-GVO, aber auch aus Art. 1 Abs. 2 DS-GVO ergibt – der Schutz von Grundrechten und Grundfreiheiten, insbesondere des Rechts auf Schutz personenbezogener Daten (Art. 8 GRCh). IT-Sicherheit hat hier also eine dem Datenschutz dienende Funktion[20] und ist deshalb zugleich Teil des Datenschutzrechts. 21

Der **Sicherheitsbegriff** wird im Recht schließlich in vielen weiteren Rechtsgebieten, Zusammenhängen und Kontexten verwendet. Dies umfasst beispielsweise die soziale Sicherheit,[21] die öffentliche Sicherheit,[22] die innere und äußere Sicherheit,[23] den erweiterten und neuen Sicherheitsbegriff[24] sowie seit einiger Zeit den Begriff der Zivilen Sicherheit.[25] Diese Sicherheitsbegriffe verfolgen verschiedene Erkenntnis- und/oder regulatorische Ziele und lassen sich deshalb nicht völlig auf einen Nenner bringen. Zentrales Element von Sicherheit ist aber jedenfalls die **Abwesenheit von Risiken und Gefahren** bzw. die Vermeidung ihrer Realisierung und, wo sich dies nicht verhindern lässt, die Geringhaltung eingetretener Schäden.[26] Mit der Digitalisierung aller Lebensbereiche trägt die 22

20 Dabei darf nicht übersehen werden, dass die Umsetzung von IT-Sicherheitsmaßnahmen oftmals mit der Verarbeitung personenbezogener Daten einhergeht und dann ihrerseits datenschutzrechtliche Herausforderungen aufwirft (s. Jandt in → § 17 Rn. 45 ff.). Die DS-GVO erkennt dies zB in EG 49 S. 1 an, es ist aber vielfach ungeklärt, in welchem Umfang zu diesem Zweck Daten verarbeitet werden dürfen.

21 S. das Sozialstaatsprinzip Art. 20 Abs. 1, 28 Abs. 1 Satz 1 GG sowie § 1 Abs. 1 SGB I; s. Rüfner in Isensee/Kirchhof, StaatsR-Hdb, § 96; Baer NZS 2014, 1.

22 So traditionell in den Generalklauseln des Gefahrenabwehrrechts, s. zB Waechter NVwZ 1997, 729; Erbel DVBl 2001, 1714.

23 Zum Begriff der inneren Sicherheit Kniesel ZRP 1996, 482 (483 f.): Gesetzlich nicht definiert und teilweise als „politischer Kampfbegriff" bezeichnet, ist er nicht mit der öffentlichen Sicherheit identisch, sondern stellt eine „Mixtur" aus Strafverfolgung, Gefahrenvorsorge und Gefahrenabwehr dar, wobei auch die Nachrichtendienste in die Kriminalitätsbekämpfung einbezogen werden; s. a. die Begriffsbestimmung bei Tanneberger, Die Sicherheitsverfassung, S. 11 ff.; Götz in Isensee/Kirchhof, StaatsR-Hdb, § 85 (dort auch zum Verhältnis zur öffentlichen Sicherheit (Rn. 4) und zur äußeren Sicherheit (Rn. 17)); s. a. Kugelmann, Polizei- und Ordnungsrecht, 5. Kap. Rn. 38.

24 Hierzu zB Brill ZfP 2001, 448; zum „Neuen Sicherheitsbegriff" Gusy in Würtenberger/Gusy/Lange (Hrsg.), Innere Sicherheit im europäischen Vergleich, S. 71 ff.: ganzheitliche Orientierung statt materien- und rechtsgüterspezifischer Normen, Erweiterung auf Risiken (Gefahrenvorfeld), zusätzlicher Fokus auf Daseinsvorsorge etc.

25 S. die Beiträge in Gusy/Kugelmann/Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit; zum Aufstieg des Begriffs s. Kaufmann in Hempel et al., Sichtbarkeitsregime, S. 102.

26 S. a. Kugelmann, Polizei- und Ordnungsrecht, 5. Kap. Rn. 38: Sicherheit als Abwesenheit von Gefahr; zum Recht der Kritischen Infrastrukturen als Risikosteuerungsrecht Freimuth, Die Gewährleistung der IT-Sicherheit Kritischer Infrastrukturen, 2018, S. 114 ff.

IT-Sicherheit daher häufig zur Gewährleistung der Sicherheit in ihren vielfältigen anderen Dimensionen bei.

23 Zu den genannten Sicherheitsbegriffen und Rechtsgebieten stehen IT-Sicherheit und IT-Sicherheitsrecht daher teilweise in einem **engeren**, teilweise in einem nur **losen** Zusammenhang. Diese Zusammenhänge werden in vielen Kapiteln des Handbuchs erläutert.

C. Spezifika rechtlicher Regelungen zur IT-Sicherheit

24 Informationstechnische Systeme werden in ihrer praktischen Entwicklung und Anwendung durch Recht weder geschaffen noch gestaltet. **Normadressaten** IT-sicherheitsrechtlicher Regelungen sind nicht IT-Systeme, sondern ihre Hersteller, Anbieter, Betreiber und Nutzer sowie diejenigen, die an der Einhaltung von Verpflichtungen mitwirken oder sie durchsetzen, etwa Prüfunternehmen, IT-Sicherheits- oder Strafverfolgungsbehörden.[27] Regelungen zur IT-Sicherheit können allerdings auf diesem Wege durchaus verbindliche Gestaltungsvorgaben machen und beispielsweise den Einsatz einer konkreten, als sicher betrachteten Technologie vorgeben. Auf verschiedenen Ebenen (Gesetze, Verordnungen, technische Anhänge zu Rechtsakten) kann dies sehr detaillierte Ausmaße bis hin zu konkreten Algorithmen, Schlüssellängen etc annehmen. Außerdem **zielen** IT-sicherheitsrechtliche Bestimmungen indirekt immer auch auf ein **IT-System**. IT-Sicherheitsrecht hat den Anspruch, für sichere IT-Systeme und ihren sicheren Einsatz zu sorgen.

25 Dieser Anspruch begegnet den allgemeinen **Schwierigkeiten des Technikrechts**. Technische Innovationen lassen sich durch Recht nur mittelbar steuern – mit unsicheren Auswirkungen. Präventive Vorgaben des Gesetzgebers können Innovation behindern, reaktive Instrumente können zu spät greifen, wenn unerwünschte Schäden schon eingetreten sind. Bei informationstechnischen Systemen kommt erschwerend hinzu, dass die Informationstechnik im Grundsatz als universelle Technologie, sogenannte „Multi Purpose Technology", ausgestaltet ist. Die meisten IT-Systeme finden in Bereichen großer Gefährdung ebenso Einsatzfelder wie in wenig riskanten Bereichen. Die gleichen Chips finden sich in sprechenden Puppen ebenso wie in kritischen Infrastrukturen, die gleichen Netzwerk-Router im Haushalt ebenso wie in einer Behörde, die gleichen Cloud-Dienste werden für Urlaubsfotos ebenso genutzt wie für die Lohnbuchhaltung eines Unternehmens.

26 Die Risiken der IT, zu deren Bewältigung IT-Sicherheitsrecht beitragen soll, sind mithin sehr vielfältig. **Allgemeine Rechtsvorschriften** wie Art. 32 DS-GVO oder Art. 21 der NIS-2-Richtlinie können nur Verfahren und Grundsätze der Risikobeurteilung und eines risikoangemessenen Schutzes definieren. Dies kann oftmals nur mit unbestimmten Rechtsbegriffen wie einem Verweis auf den Stand der Technik erfolgen. Soll das Risiko konkreter adressiert werden, bleibt nur eine bereichsspezifische Regelung mit näherer Berücksichtigung des jeweiligen Anwendungsfalls der IT. In der Regel nicht möglich ist eine belastbare Messung des Risikos sowie der konkrete Nachweis, in welchem Ausmaß das

27 Neben diesen direkten Normadressaten gibt es die Möglichkeit, rechtliche Regelungen bzw. die hinter ihnen stehenden normativen Ziele zu verwenden, um in mehrschrittigen Konkretisierungen technische Gestaltungsvorschläge für neue, im Entstehen befindliche Technologien abzuleiten. Dies ist insbesondere der Ansatz der Methode KORA (Konkretisierung rechtlicher Anforderungen; entwickelt in Hammer/Pordesch/Roßnagel, Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestalten, S. 43 ff.), s. zB Roßnagel in Kortzfleisch/Bohl (Hrsg.), FS Winand, 2008, S. 381 ff. sowie methodisch und an exemplarischen Forschungsansätzen die Beiträge in Roßnagel/Hornung/Geminn/Johannes (Hrsg.), Rechtsverträgliche Technikgestaltung und technikadäquate Rechtsentwicklung. 30 Jahre Projektgruppe verfassungsverträgliche Technikgestaltung.

Risiko durch die jeweiligen Sicherheitsmaßnahmen reduziert werden kann oder wird.[28] Schon die Vielfalt der IT-Sicherheitsrisiken ist **nicht messbar**, erst Recht nicht die aus der Komplexität der vernetzten Systeme entstehenden Risikoprofile.

Technische Systeme sind aus diesen Gründen im Hinblick auf ihre IT-Sicherheit **nicht eindeutig beurteilbar**. Unmittelbare technische Prüfungen scheitern fast immer schon an der Komplexität des Systems. Selbst kleinste Apps oder einfache Steuerungsgeräte im Haushalt haben eine derart umfangreiche Programmierung, dass eine systematische Überprüfung oder gar ein formaler Beweis der Sicherheit nur in Ausnahmefällen möglich ist. Aussagen über technische IT-Sicherheit lassen sich nur im Hinblick auf eine abstrakte Modellierung eines Zielzustandes machen und sind mit einer gewissen Wahrscheinlichkeit behaftet. Mit jeder Änderung des Systems, etwa einem Softwareupdate, sind Sicherheitsaussagen nur noch eingeschränkt oder gar nicht mehr gültig. Dies gilt umso mehr, wenn IT-Systeme mit Methoden der Künstlichen Intelligenz (KI) ausgestattet sind, weil das Verhalten eines Systems in diesem Fall noch schwieriger beschrieben werden kann (*Steinrötter/Letzel* in → § 30 Rn. 8 ff.). 27

Der Grad an IT-Sicherheit, den ein System aufweist, kann nur zum Preis **höherer Kosten** gesteigert werden.[29] Je sicherer ein System sein soll, desto teurer sind die Sicherheitsmaßnahmen. Daher erfordert ein konkretes Ergreifen von Sicherheitsmaßnahmen immer auch eine Abwägung zwischen Kostenaufwand und Restrisiko. Der Gesetzgeber muss dies bei seiner Regulierung berücksichtigen. 28

Über die Festlegung von Anforderungen an technische Systeme hinaus richten sich IT-sicherheitsrechtliche Regelungen oftmals an das **Verhalten** derjenigen, die mit dem System umgehen, seine **Hersteller** genauso wie **Endnutzer**. Die IT-Sicherheit eines (untechnisch verstandenen) Gesamtsystems ist häufig ein Produkt aus der technischen Sicherheit und dem Verhalten der verschiedenen Beteiligten. Die Sicherheit des Online-Banking kann durch ein schlechtes Verschlüsselungsverfahren ebenso beeinträchtigt werden wie durch mangelnde Wartung bei der Bank, Manipulation bei Intermediären (zB Telekommunikations-Anbietern) oder auch vernachlässigtem Virenschutz beim Endkunden. Rechtliche Regelungen müssen diese Notwendigkeit des Zusammenwirkens und eine entsprechend den jeweiligen Möglichkeiten gestufte Verantwortungsverteilung berücksichtigen. Nur so kann eine angemessene Risiko- und ggf. Schadensallokation erreicht werden. 29

Zu beachten ist hierbei, dass im Bereich der vernetzten digitalen Technologien das Zusammenwirken von Akteuren in **verschiedenen Staaten** der Regelfall ist.[30] Deutscher und europäischer Gesetzgeber können nur Teilbereiche der jeweiligen Verantwortung für IT-Sicherheit unmittelbar adressieren und müssen Lösungen finden, um Sicherheitsziele trotz der Beteiligung internationaler Akteure zu erreichen. Die vielfältigen gesetzgeberischen Aktivitäten der Europäischen Union im Bereich der IT-Sicherheit in den letzten Jahren sind Ausdruck des Bestrebens, dieser Herausforderung zumindest im europäischen Binnenmarkt zu begegnen. 30

Der Schutz der Verfügbarkeit, Vertraulichkeit und Integrität informationstechnischer Systeme durch das Recht dient in vielen Fällen unmittelbar oder mittelbar dem **Grund-** 31

28 Zu Möglichkeiten und Grenzen von Messung, Prüfung und Nachweis von IT-Sicherheit s. Skierka-Canton in → § 8 Rn. 7 ff., 23 ff.

29 Zu den ökonomischen Aspekten der IT-Sicherheit s. Bertschek/Janßen in → § 3 Rn. 1 ff.

30 S. zu den völkerrechtlichen Fragen der IT-Sicherheit Lahmann in § 6.

rechtsschutz (s. näher *Poscher/Lassahn* in → § 7 Rn. 40 ff.).[31] Die Folgen mangelnder IT-Sicherheit können für Menschen zu schwerwiegenden Einschränkungen führen. IT-Sicherheitsmaßnahmen können gleichzeitig aber auch in Grundrechte eingreifen, etwa durch einschränkende Vorschriften für Produkte oder staatliche Befugnisse im digitalen Raum. Gesetzgeber, Gesetzesvollzug und Gerichte müssen also eine verhältnismäßige Ausgestaltung und Anwendung der Vorschriften in diesem Spannungsfeld anstreben.

32 Ein solches Spannungsfeld ergibt sich in besonderem Maße, wenn der Staat aus Sicherheitsgründen, etwa auch zu Zwecken der IT-Sicherheit, seinerseits auf IT-Sicherheitsmechanismen einwirkt, zum Beispiel mit dem Versuch des Brechens von Verschlüsselung, mit der sogenannten Online-Durchsuchung oder sogar in Form von heimlichen **staatlichen Hintertüren** in IT-Systemen. Solche Maßnahmen betreffen die individuelle IT-Sicherheit des Zielsystems, können aber darüber hinaus die IT-Sicherheit insgesamt beeinträchtigen. Dieser Zielkonflikt zwischen dem Interesse von Wirtschaft und Gesellschaft an hoher IT-Sicherheit und dem Interesse nach effektiver Strafverfolgung besteht bereits seit mehreren Jahrzehnten und wird gemeinhin als „Kryptokontroverse" bezeichnet.[32]

D. IT-Sicherheitsrecht als Rechtsgebiet im Entstehen

33 Die Entwicklung des IT-Sicherheitsrechts als **neue Querschnittsmaterie des Rechts** folgte und folgt in Deutschland und Europa bislang keiner übergeordneten Konzeption. Anders als die andere große Querschnittsmaterie der digitalen Welt, das Datenschutzrecht mit der Datenschutz-Grundverordnung (DS-GVO) als grundlegendes Gesetzeswerk, ist IT-Sicherheitsrecht nur als Zusammenschau verschiedener Regelungen zu sehen.[33] Zur fehlenden Durchdringung der Materie trägt auch bei, dass es bisher nur ausgewählte Rechtsprechung zum IT-Sicherheitsrecht gibt.

34 Weder das deutsche IT-Sicherheitsgesetz von 2015, als Artikelgesetz nicht mehr als ein Katalog von Gesetzesänderungen mit IT-Sicherheitsrelevanz, noch der europäische Rechtsakt zur Cybersicherheit von 2019 und die nachfolgenden europäischen Rechtsakte sind als grundlegende Rechtsvorschrift für die IT-Sicherheit zu verstehen. Allenfalls das (durch das IT-Sicherheitsgesetz und das IT-Sicherheitsgesetz 2.0 ausgebaute) **BSI-Gesetz** mit den über die Befugnisse des Amtes hinausgehenden Regelungen für kritische Infrastrukturen und digitale Dienste – im Zusammenspiel mit der europäischen NIS-Richtlinie – kann mittlerweile als materieller **„Kern" des IT-Sicherheitsrechts** verstanden werden. Dies wird sich mutmaßlich mit den absehbaren nationalen Aktivitäten zur Umsetzung der NIS-2-Richtlinie weiter fortsetzen, die eine starke Erweiterung des BSI-Gesetzes vorsehen. Auch in dieser Form wird das Gesetz aller Voraussicht nach aber **nicht** zu einer systematischen Grundlage oder einem **Allgemeinen Teil** eines IT-Sicherheitsrechts.

35 Anforderungen an die Sicherheit der Informationstechnik und ein dementsprechendes Verhalten der Betreiber oder Nutzer ließen sich lange nur aus allgemeinen **deliktsrechtlichen Regelungen** des Zivilrechts herauslesen; mittlerweile wurden und werden sie

31 Das BVerfG betont nunmehr die Schutzpflichtendimension des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, s. BVerfGE 158, 170 (185 f.); BVerfG NVwZ-RR 2022, 401 Rn. 17; s. für den KRITIS-Bereich Freimuth, Die Gewährleistung der IT-Sicherheit Kritischer Infrastrukturen, 2018, S. 129 ff.; näher Wischmeyer, Informationssicherheit, 2023, S. 156 ff.

32 Ausführlich Schallbruch in → § 5 Rn. 65 f., s. auch Schallbruch, Der Staat als Hacker, in Handbuch Digitalisierung in Staat und Verwaltung, 2020, insbesondere S. 533 ff.; zu einem entgegengerichteten Recht auf Verschlüsselung zB van Daalen CLSR 49 (2023) 105804; näher zur Sicherheitsgewährleistung durch Einflussnahme auf Informationstechnik Wischmeyer, Informationssicherheit, 2023, S. 279 ff.

33 Zu Systematisierungsansätzen s. nunmehr Wischmeyer, Informationssicherheit, 2023, S. 183 ff.

durch den Gesetzgeber konkretisiert.[34] Im Strafrecht reagierte die Gesetzgebung schon früh. Mit der Einführung des **Computerstrafrechts** ab dem Jahre 1986 und schrittweisen Erweiterung sind die strafrechtlichen Grenzen eines Handelns im Hinblick auf Nutzung und Manipulation informationstechnischer Systeme markiert und damit auch IT-sicherheitsrechtliche Wirkungen erzielt. Mit der Strafbarkeit des Hackings in Form eines Überwindens von Sicherheitsmechanismen ist ein Anreiz zur Nutzung solcher Mechanismen verbunden, will man den Schutz des Strafrechts für sich in Anspruch nehmen (näher *Singelnstein/Pech* in → § 20 Rn. 38 ff.).

36 Regelungen zum Schutz der IT-Sicherheit sind seit seinem Bestehen ein Teil des **Datenschutzrechtes** (→ Rn. 17). Technisch-organisatorische Maßnahmen sollen den (rechtlichen) Schutz personenbezogener Daten absichern; man spricht in diesem Zusammenhang auch von Datensicherheit oder in der DS-GVO von der „Sicherheit der Verarbeitung" (Art. 32 DS-GVO). Datenschutzrecht ist insofern nicht nur eine verwandte Querschnittsmaterie zum IT-Sicherheitsrecht, sondern weist auch einen erheblichen Überschneidungsbereich auf (→ Rn. 21). Regelungen zum Schutz der Vertraulichkeit und Integrität – seit der DS-GVO auch der Verfügbarkeit – von Systemen, mit denen persönliche Daten verarbeitet werden, stehen neben Regelungen des IT-Sicherheitsrechts zum Schutz der gleichen Systeme, nur eben mit leicht anderen Schutzzielen und Risikoprofilen. In dem Maße, in dem IT-Systeme zunehmend auch persönliche Daten verarbeiten, und in dem Maße, in dem IT-Sicherheitsrecht durch die NIS-2-Richtlinie und ihre Umsetzung, aber auch durch den AI Act, für weitere Arten von Systemen eingeführt wird, wird der **Überschneidungsbereich zunehmen**.

37 Konkrete Anforderungen für IT-Systeme und deren Einsatz sind in Deutschland und Europa zunächst **branchenspezifisch** entstanden, etwa in der Telekommunikation oder im Kreditwesen. Parallel zu den eher querschnittlichen Regulierungen wie dem Ausbau des BSI-Gesetzes, der NIS-Richtlinie nebst ihrer Weiterentwicklung oder dem EU-Rechtsakt zur Cybersicherheit wächst Jahr für Jahr auch der Bestand der bereichsspezifischen Gesetze, die Regelungen zur IT-Sicherheit enthalten. Schon mit Stand Herbst 2017 gab es 63 Gesetze und Verordnungen des Bundes und weitere Rechtsvorschriften der Länder, die dem BSI eine mitwirkende, beratende oder sonstige Rolle zuweisen, mithin für den jeweiligen Regelungsbereich IT-Sicherheits-Regelungen enthalten.[35] Seitdem sind weitere Aufgaben und Befugnisse aus verschiedensten Politikfeldern hinzugekommen.

38 Über alle IT-sicherheitsrechtlichen Regelungen hinweg lässt sich ein **Instrumentenkasten** beschreiben, mit dem der Gesetzgeber den Schutz der IT-Sicherheit erreichen will. Die erste große Abteilung des Instrumentenkastens betrifft **Anforderungen an Systeme** und alle, die mit ihnen **umgehen**. Typische Regulierungsinstrumente sind das Verbot bestimmter IT-Systeme[36] oder IT-bezogener Handlungen[37] oder ihre Erlaubnis nur unter bestimmten Auflagen. Solche Auflagen beziehen sich häufig auf einen Nachweis von Sicherheitseigenschaften oder Sicherheitsmanagement durch **Zertifizierung und Auditierung**.[38] Verbreitet sind mittlerweile auch **Meldepflichten** für den Fall, dass es trotz

34 S. zu den Entwicklungen in der Rspr. und zu neueren gesetzgeberischen Maßnahmen Pour Rafsendjani in → § 9 und Spindler in → § 10 Rn. 4 ff.

35 Schallbruch CR 2017, 648 (649).

36 ZB bestimmter kritischer Komponenten auf Grundlage von § 9b BSIG, derzeit auch noch sogenannter Hacker-Tools durch § 202c Abs. 1 Satz 1 Nr. 2 StGB, aktuell wird zB ein Verbot bestimmter KI-Systeme durch den geplanten AI Act diskutiert, soweit derartige Systeme inakzeptable Risiken verursachen.

37 Etwa § 20 Abs. 3 PAuswG.

38 S. zB § 8a Abs. 3–5 und §§ 9–9c BSIG, § 165 Abs. 4 TKG, § 19 MsbG. Auch der Entwurf der Kommission für einen Cyber Resilience Act enthält weitere Bestrebungen in diese Richtung.

der präventiven Bemühungen zu IT-Sicherheitsvorfällen gekommen ist.[39] Eher selten finden sich explizite Vorgaben für die innere Organisation, zB die Pflicht zur Bestellung eines IT-Sicherheitsbeauftragten.[40] Ebenfalls **unterentwickelt** ist noch das Instrument der **Haftung** als Steuerungselement im IT-Sicherheitsrecht. Die Haftung von Endnutzern ist naturgemäß sehr eingeschränkt, weil ihnen nicht allzu viel technische Expertise zugetraut werden kann, Intermediäre sind in ihrer Haftung rechtlich weitgehend privilegiert, Hersteller von IT-Produkten werden hingegen zunehmend in die Verantwortung genommen (s. im Einzelnen *Spindler* in → § 11 Rn. 1 ff.). Für die Kategorie der Betreiber riskanter Systeme, etwa der kritischen Infrastrukturen, sind Haftungsregelungen verschärft worden,[41] für Betreiber riskanter KI-Systeme sind sie geplant (*Steinrötter/Letzel* in → § 30 Rn. 50 ff.).

39 Die Erweiterung der **Befugnisse von Behörden** ist die zweite große Abteilung des Instrumentenkastens. Vor allem spezialisierte IT-Sicherheitsbehörden wie das BSI oder die europäische Behörde ENISA wurden rechtlich und tatsächlich ausgebaut (s. näher *Gitter* in → § 15 Rn. 30 f. und 43 ff.). Diese haben erweiterte Kompetenzen erhalten, IT-Sicherheit zu beurteilen (einschließlich Untersuchungsbefugnisse wie § 7a BSIG), aber auch durchzusetzen, präventiv durch Anforderungen und Kontrollen, aber auch reaktiv durch Befugnisse bei IT-Sicherheitsvorfällen sowie durch informelles Verwaltungshandeln (v.a. Warnungen wie nach § 7 BSIG). Die Behördenlandschaft wird mit der Einrichtung von Schwesterbehörden in den Ländern[42] deutlich komplexer. Dieser Trend ist angesichts der Bedeutung der Materie nachvollziehbar, die unterschiedlichen Aufgaben und Befugnisse führen aber zu neuen Herausforderungen für die föderale Zusammenarbeit und werfen teilweise auch verfassungsrechtliche Probleme auf.[43] Schließlich haben auch die „klassischen" Sicherheitsbehörden wie Polizeien und Nachrichtendienste ihr Instrumentarium im Hinblick auf die IT-Sicherheit erweitert, Polizeien etwa zur Abwehr von schweren Cyberangriffen oder Nachrichtendienste zur Früherkennung von IT-Sicherheitsgefahren (*Bäcker/Golla* in → § 18 Rn. 1 ff.).

40 Insgesamt leidet die Fortentwicklung des IT-Sicherheitsrechts in Deutschland und Europa an einer **mangelnden Systematisierung**. Es fehlt eine stärkere Unterscheidung zwischen allgemeinen, alle Branchen umfassenden Regelungen und bereichsspezifischem Recht – verknüpft durch eine einheitliche Begrifflichkeit und Regelungsstruktur. Dieses Defizit kann an verschiedenen Problemlagen gezeigt werden. Es beginnt mit den sehr **unterschiedlichen Begrifflichkeiten** für die zu schützenden informationstechnischen Systeme, die eine Anwendung des Rechts erschweren.[44] Begriffe wie kritische Infrastrukturen, digitale Dienste, Mediendienste, Telekommunikations- und Telemediendienste verwischen sich immer mehr. Verfahrensweisen zur Risikoabschätzung in der IT-Sicherheit differieren in den verschiedenen Gesetzen, insbesondere zwischen Datenschutz- und IT-Sicherheitsrecht mit ihren leicht unterschiedlichen Schutzgütern. Gleiches gilt für die in nahezu allen Gesetzen geforderte Einbeziehung des Standes der Technik in die Auswahl der Maß-

39 ZB § 8b Abs. 4, § 8c Abs. 3 und § 8f Abs. 7 und 8 BSIG; § 168 TKG; § 11 Abs. 1c EnWG; Art. 33; 34 DS-GVO.
40 S. etwa § 166 TKG.
41 Durch sektorales Recht wie zB das ZAG für Zahlungsdienstleister.
42 Wie zB das Landesamt für Sicherheit in der Informationstechnik Bayern oder die Cybersicherheitsagentur Baden-Württemberg.
43 S. etwa Debus VBlBW 2021, 495; Rehbohm/Kalmbach DuD 2023, 338; umfassend zu den Akteuren Stiftung Neue Verantwortung, Deutschlands staatliche Cybersicherheitsarchitektur, 11. Aufl. 2023; s. auch Gitter in → § 15 Rn. 35 f., 42; Bostelmann in → § 25 Rn. 33 ff., 178 ff.
44 Etwa die Erfassung von bestimmten Cloud-Diensten als kritische Dienstleistungen im Sinne des § 8a BSIG, als digitale Dienste nach § 8c BSIG ebenso wie als Telemediendienste nach TMG und TTDSG, vgl. Raabe/Schallbruch/Steinbrück CR 2018, 705 (708). Es bleibt abzuwarten, ob diese Unklarheiten im Zuge der Umsetzung der NIS-2-Richtlinie in deutsches Recht bereinigt werden können.

nahmen. Wünschenswert wäre eine stärkere Systematisierung in Form eines **Allgemeinen Teils zum IT-Sicherheitsrecht**.

Stichwortverzeichnis

Die **fetten** Zahlen verweisen auf den Paragrafen (Beitrag), die mageren auf die Randnummer.

3D-Secure **2** 119
3GPP **21** 30
3rd Generation Partnership Project **21** 30

41. Strafrechtsänderungsgesetz **20** 28

5G-Technologie **5** 58, **8** 79, 98, **21** 62

Abfallrecht, Privathaushalt **26** 9, 55 ff.
Abfangen von Daten (§ 202b StGB) **18** 60, **20** 43 f.
Abhängigkeit **5** 9
Abhilfemaßnahmen **29** 40
Abhörfunktion **26** 33
Abhörrisiko **26** 52 ff.
Ablage, sichere **14** 74
Abnahmekriterien **9** 194, **29** 119
Abschreckungseffekt **7** 34
Absenden **14** 63
Absicherungskategorien, IT-Grundschutz **8** 27
Absichtsbekundung **25** 187
Abstimmungsbedarf **25** 97
Abstimmungsprozess, mühsamer **25** 56
Abstrakte Gefährdungen **7** 32 ff.
Abteilungsleiter **16** 59
Abwehrmaßnahmen
– defensive **18** 23 f.
– Grundrechtseingriff **18** 24, 27
– offensive **18** 25 ff.
– staatliche Maßnahmen **18** 26
– Telekommunikation und digitale Dienste **21** 30
Abwehrrecht **7** 30 ff.
Abwehr von Angriffen **2** 123
Access Control
– DAC **2** 121
– MAC **2** 2, 121
– RBAC **2** 121
Access-Provider **21** 9
– Haftung **12** 13 ff.
Accountinhaber
– Geheimhaltungspflichten **12** 18 f.
– Sicherungspflichten **12** 18 f.
ACEA **22** 84
Add-Ons **11** 38
Administrator **4** 39
– Datenschutzrecht **17** 48 f.
– lokale Administratorrechte **16** 81
– Privathaushalt **26** 21 f.
– Systemadministrator **17** 48 f.
Advanced Persistent Threat (APT) **13** 107
AGB
– IT-Sicherheitsklausel **9** 191, **29** 116
– Outsourcing **9** 191, **29** 116
– Transparenzgebot **9** 34, 36
AG Informationssicherheit, AG InfoSic **25** 65, 161, 178
Akkreditierung **8** 13 f., **13** 101
– De-Mail **14** 76
– Prüfstelle **8** 19
Akteneinsicht, Meldung **23** 31
Akteur, nichtstaatlicher **19** 22 ff.
AktG **16** 3
Aktive Cyberabwehr, Europäische Union **15** 10
Aktualisierung **26** 22, 50
Aktualisierungspflicht **26** 50
Aktuator, Privathaushalt **26** 23
All-Gefahrenansatz **13** 4
Allgemeinverfügung
– IT-Sicherheitskatalog **23** 19
– Katalog von Sicherheitsanforderungen **13** 114
– Umsetzungsfrist **13** 117
– zusätzlich zum IT-Sicherheitskatalog **23** 25
All-IP-Netze **21** 18
Allzuständigkeit des Staates **7** 48
Amazon Web Services **13** 154
Ambient Assisted Living **26** 29, 53
Amtshilfe **7** 55, **18** 35 ff., **25** 193
– BSI **18** 35 ff.
– Bundeswehr **19** 39
– Subsidiarität **19** 39 ff.
– technische **19** 41 ff.
Anbieter digitaler Dienste **16** 19 ff., 24

Anforderungen **25** 70, 166, **29** 88
– an technische Mittel **14** 29
– qualifizierter Vertrauensdienst **14** 44
Angabe, berufsbezogene **14** 47
Angemessenes Schutzniveau **28** 68
Angemessenheit **25** 166, **28** 27 f., 64 ff., 72
– Eintrittswahrscheinlichkeit **28** 69 ff.
– Implementierungskosten **28** 76
– Kriterien **28** 68
– Schwere des Risikos **28** 69
– Stand der Technik **28** 74 ff.
Angriff, bewaffneter **19** 1 ff., 26 ff.
– Abwehrmaßnahmen **21** 30
– Mittel **21** 28 f.
– Motive **21** 27
– Selbstverteidigung **19** 9 ff.
– von außen **19** 17 ff.
– Zweckrichtung **19** 11 ff.
Angriff, Qualität **25** 121
Angriffserkennungssystem
– Implementierungspflicht **30** 44 ff.
– KI-basiert **30** 44 ff.
– KRITIS **30** 44 ff.
– Stand der Technik **30** 45 ff.
Angriffskrieg (s.a. Angriff, bewaffneter) **18** 29
– Verbot **19** 33 ff.
Angriffsmethoden **2** 16
Angriffsvektoren **5** 9, **6** 36, **22** 121
Angriffsziel **25** 121
Anlage
– Anlagenteile **13** 63
– Ausfall **13** 53
– Begriff **13** 62 ff.
– gemeinsame **13** 64 f.
– Verfahrensschritte **13** 63
Anlagenbezug **13** 46
Anlagenkategorien, Kritische Infrastruktur **13** 47
Anleitung **29** 95
Anmeldung
– De-Mail-Konto **14** 68
– sichere **14** 73
Anonymisierung **28** 78, 81
– Trainings- und Testdaten **30** 22
Anonymität **1** 15, **2** 20 f., **4** 9
Anordnungen **25** 120
Anscheinsbeweis **14** 94, 99, 101
Anschlussinhaber, Haftung **12** 17
Anschlussklasse **25** 102
Ansprechpartner
– AtG **23** 27
– EnWG **23** 14, 24 ff.
Ansprechpartner in der EU, Telekommunikation **21** 76
Antwort, globale **25** 203
Anwendung, gemeinschaftliche **25** 74
Anwendungsentwicklung **16** 92, **29** 68
Anwendungssicherheit **14** 20
Anzeige, kritische Komponente **23** 33f
Application Service Providing **11** 67
APT **13** 107
Äquivalenzinteresse **11** 2
Arbeitgeber **9** 183
Arbeitnehmer **9** 183
Arbeitsrecht **9** 183
Arbeitsvertrag **9** 183
Archivierung, elektronisch **14** 34a
Archivierungsdienst **14** 59e
– Rechtswirkungen **14** 59f
AtG, erhöhte IT-Sicherheitsanforderungen **23** 27
Attribute **14** 59b f.
Attribution **6** 44 ff.
– von Cyberangriffen **18** 15
Attributionsproblem **6** 44 ff.
Attributsbescheinigung **14** 46, 59a
– Datenschutz **14** 59c
– qualifiziert **14** 59b f., 102
– Rechtswirkungen **14** 59a
Attributzertifikat **14** 47
Audit **29** 54
Auditoren **23** 16
Auditrecht **9** 203, **29** 128
Aufdecken von Angriffen **2** 125 f.
Aufgabenerfüllung **25** 194
Aufmerksamkeit, situationsadäquate Aufmerksamkeit **26** 47
Aufrechterhaltung **25** 28, 181
Aufschalten, Telekommunikation **21** 72
Aufsicht **25** 108, **29** 72
– De-Mail **14** 76
– ex ante **14** 45
– ex post **14** 42
Aufsichts-, Kontroll- und Durchsetzungsbefugnisse, Bußgeldregime **13** 111

Aufsichtsbehörden **9** 49, **29** 6 ff., 28 f., 43, 46, 93, 99, 102 f.
Aufsichtsbehörden, datenschutzrechtliche **3** 28
– Kontrolle dokumentierter IT-Sicherheitsmaßnahmen **21** 123
– Meldepflichten **21** 128 f.
Aufsichtsplan **29** 45
Aufsichtspraktiken **29** 108
Aufsichtsrat
– Haftung **9** 80
– Überwachungspflicht **9** 80
Aufsichtsrechtlich **29** 101
Auftragsverarbeiter **8** 65, **9** 55, 71, **21** 117
Auftragsverarbeitungsvertrag (AVV) **9** 71
Augmented Reality **26** 17
Ausdifferenzierung und Spezialisierung der Gesellschaft **7** 17
Ausfall **25** 202
– einer Anlage **13** 53
– von Staatsfunktionen **19** 12 ff.
Ausführung, schlechte **25** 157
Ausgliederung **29** 4, 100
Auskunftsanspruch **13** 42, **14** 75
– Nachweisverfahren **13** 104
Auskunftserteilungsverpflichtung **13** 42
Auskunftsrechte **29** 103
Auskunftsverlangen **10** 61 f.
Auslagerung **9** 73, 90, 189 ff., **16** 94, **29** 32, 43, 47, 49 f., 57, 75, 80, 84 f., 108, 111, 114 ff.
– Auslagerungsverbot **29** 24
– Risiko **29** 45
– Unternehmen **29** 112
– Vereinbarung **29** 110
– Vertrag **9** 199 f., **29** 38, 53, 124 f.
Auslagerungskonstellation **9** 73, 90, 189 ff., **29** 114 ff.
– Anlagen des Finanzwesens **13** 58
– Betreibereigenschaft **13** 58
– Outsourcing **13** 57
– Unternehmen im Ausland **13** 60
– Versicherungswesen **13** 59
– Vertrag **9** 199 f., **29** 124 f.
– Weisungs- und Durchgriffsrecht des Betreibers **13** 57
Ausnahmecharakter **25** 193
Ausspähen von Daten (§ 202a StGB) **20** 39 ff.
Ausstiegsstrategie **29** 68, 110
Austausch- und Beschlussorgan **25** 61
Auswahlmöglichkeit **25** 140
Authentifizierung **2** 114 ff., **14** 59a
– Technische Richtlinie **24** 26 ff.
– Website **14** 59
– Zwei-Faktor-Authentifizierung (2FA) **2** 40
Authentische Quelle **14** 59b f.
Authentizität **1** 15, **2** 39, **4** 9, **14** 1, 5 f., 13
Auto-ISAC **22** 100
Automatisierte Entscheidungsfindung **30** 26
Automatisierung im Haushalt **26** 14
Automatisierungstechnik, Zertifizierung **8** 80
Automotive SPICE **22** 109
Autonomes Fahren **22** 61a ff.
Autonome Systeme **11** 11
AUTOSAR **22** 110
AVMD-Richtlinie **21** 16
Awareness **25** 46

B3S **28** 29 f., 32 ff.
Backdoors **1** 32, **22** 57, 122
Baden-Württemberg **25** 41, 118
BaFin **16** 43, **29** 80
BAIT **16** 3, 43, 82 ff., 95, **29** 82 f.
– IT-Risikomanagement **16** 47
Bankenaufsicht **29** 91
Bankwesen **13** 26
Basisinfrastruktur, technische **13** 150
Bayerisches Digitalgesetz (BayDiG) **16** 33 f., **25** 115
Bayern **25** 115
BDSG **16** 68, **17** 11
– Strafvorschriften **20** 53 ff.
Beauftragter der Bundesregierung für Informationstechnik (BfIT) **15** 33
beBPo **27** 110 ff.
– einfache Signatur **27** 118 ff.
– Justiz **27** 115 f.
Bedarfsgemeinschaft **26** 6
Bedrohung **9** 1, **25** 38
Bedrohung, existenzielle **25** 153
Bedrohungslage, hybride **25** 129
Beeinflussung eines Datenverarbeitungsvorgangs **20** 85
Beeinträchtigung, erhebliche **13** 107

Beendigung des Dienstes, Plan **14** 44
Befugnisse **25** 120
Befundsicherungspflicht **11** 57
Behörden, Verwaltung und Justiz, Infrastrukturbereich **13** 7
Behördengang, digital **25** 95
Behördenleitung **25** 131
Behördliche Maßnahmen **18** 21
– Grundrechtseingriff **18** 22
Beleihung **14** 71
Bemessungskriterien, Kritische Infrastrukturen **13** 47
Benutzerberechtigungsmanagement **16** 91
Berechtigte Interessen
– im datenschutzrechtlichen Sinne **16** 78, **17** 55 ff., 62 f., **21** 117
– IT-Sicherheit **17** 62 f.
Berechtigter, Schutz der Verfügungsgewalt (§§ 303a, 303b StGB) **20** 64 ff.
Berechtigungskonzept **17** 51
Bereich, gesellschaftlicher **25** 41
Bereiche, Kritische Infrastrukturen **13** 47
Bereinigungsbefehle **21** 95
Berichterstattung **29** 25
Berichtspflichten **29** 89
Berufsgeheimnis(träger) **9** 66 f., **17** 3, 26
Berufsprogrammierer **11** 84 ff.
Beschaffenheit **25** 180
Beschaffenheitsvereinbarung **9** 116, 179 ff.
Beschleunigte Sicherheitszertifizierung, BSI **8** 78
Beschleunigung des Lebens durch IT **7** 16
Beschlüsse, rechtlich verbindliche **25** 64
Beschränkung
– Nutzungsbeschränkung **9** 69
– Zugangsbeschränkung **9** 69
Besonderes Anwaltspostfach (beA) **14** 39, **27** 104 ff.
Besonders schwerer Unglücksfall, ungewöhnliche Ausnahmesituation **19** 44
Bestandsdaten **21** 70
Bestandsdatenauskunft, BSI **15** 54
Bestandsschutz, staatliche Ordnung gegen Angriffe von außen **19** 7
Bestätigung
– Abholung **14** 69
– Eingang **14** 69
– Empfang **14** 23
– Identitätsdaten **14** 73
– qualifiziert signierte **14** 70
– Senden **14** 23
– sichere Anmeldung **14** 69
– Versand **14** 69
Bestimmbarkeit **9** 34 f.
– Anspruch **9** 33
– IT-Sicherheit **9** 52
Bestimmung der Kritikalität einer Infrastruktur **13** 32 ff., 47
– Benennung **13** 36
– Benennungspflicht einer Kontaktstelle **13** 38
– Bestimmungsmethodik **13** 36
– Bestimmungszeitpunkt **13** 68
– Betreiberpflichten **13** 66 ff.
– Handlungspflicht für Betreiber **13** 37 ff.
– Versorgungsgrad **13** 33, 35, 48
Bestimmung des Versorgungsgrades **13** 48 ff.
– Heizwerk **13** 50
Bestimmungsgemäßer Gebrauch **11** 26
Best Practice **9** 50, 220, **11** 29, **16** 80 ff., 95, **22** 87 f., 100
Betätigungsfeld, Kommune **25** 151
Betrachtung, risikobasiert **25** 17
Betreiber
– Begriff **13** 55
– Haftung **12** 13 ff.
Betreibereigenschaft **13** 57 f.
– Anlagen des Finanzwesens **13** 58
– Art der Rechtspersönlichkeit **13** 61
Betreiberpflichten
– Auskunftslast des Betreibers **13** 39
– Auskunftsverpflichtung **13** 39
– Benennung einer Kontaktstelle **13** 38
– Bestimmung der Kritikalität **13** 66 ff.
– Meldepflicht **13** 106, 160, 163 ff.
– Nachweispflicht und Kontrolle **13** 100
– Nachweisverfahren **13** 101 ff.
– organisatorische und technische Vorkehrung **13** 79 ff.
– Schutz personenbezogener Daten **13** 166
– Telemedien **13** 166
Betreiber von Kritischen Infrastrukturen **8** 52 ff.
– Verkehrspflichten **10** 48 ff.