Hornung | Schallbruch [Hrsg.]

IT-Sicherheitsrecht

Praxishandbuch

Nomos

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

IT-Sicherheitsrecht

Praxishandbuch

Prof. Dr. Matthias Bäcker, LL.M., Johannes-Gutenberg-Universität Mainz | **Prof. Dr. Irene Bertschek**, ZEW – Leibniz-Zentrum für Europäische Wirtschaftsforschung, Mannheim | **Dr. David Bomhard**, Rechtsanwalt, München | **Matthias Fischer, LL.M.**, Regierungsdirektor, Berlin | **Dr. Christian L. Geminn, Mag. iur.**, Universität Kassel | **Dr. Rotraud Gitter, LL.M. Eur.**, Regierungsdirektorin, Berlin | **Dr. Sebastian J. Golla**, Ruhr-Universität Bochum | **Prof. Dr. Rüdiger Grimm**, Universität Koblenz-Landau | **Prof. Dr. Annette Guckelberger**, Universität des Saarlandes | **Marit Hansen**, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD) | **Prof. Dr. Andreas Heinemann**, Hochschule Darmstadt | **Prof. Dr. Gerrit Hornung, LL.M.**, Universität Kassel | **PD Dr. Silke Jandt**, Referatsteilleiterin bei der Landesbeauftragten für den Datenschutz Niedersachsen, Privatdozentin Universität Kassel | **Rebecca Janßen**, ZEW – Leibniz-Zentrum für Europäische Wirtschaftsforschung, Mannheim | **Dr. Henning Lahmann**, Digital Society Institute, European School of Management and Technology Berlin | **Dr. Philipp Lassahn, LL.M.**, Regierungsrat, Berlin | **Prof. Dr. Marian Margraf**, Freie Universität Berlin | **Johannes Müller MLE.**, Universität Kassel | **Dr. Jörg Ohnemus**, ZEW – Leibniz-Zentrum für Europäische Wirtschaftsforschung, Mannheim | **Prof. Dr. Ralf Poscher**, Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht, Freiburg | **Dr. Mansur Pour Rafsendjani**, Rechtsanwalt, München | **Prof. Dr. Alexander Roßnagel**, Universität Kassel | **Martin Schallbruch**, Ministerialdirektor a.D., Digital Society Institute, European School of Management and Technology Berlin | **Marc Schardt**, Regierungsdirektor, Berlin | **Stephan Schindler**, Universität Kassel | **Prof. Dr. Tobias Singelnstein**, Ruhr-Universität Bochum | **Philipp Singler**, Datenschutzbeauftragter Stadt Offenburg | **Isabel Skierka**, Digital Society Institute, European School of Management and Technology Berlin | **Sylvia Spies-Otto**, Ministerialdirigentin, Bundesministerium der Verteidigung, Berlin | **Prof. Dr. Gerald Spindler**, Georg-August-Universität Göttingen | **Dr. Thomas Thalhofer**, Rechtsanwalt, München | **Prof. Dr. Michael Waidner**, Fraunhofer-Institut für Sichere Informationstechnologie SIT, Darmstadt | **Louisa Zech**, Ruhr-Universität Bochum

Nomos

Zitiervorschlag: *Autor* in Hornung/Schallbruch IT-SicherheitsR-HdB § ... 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 978-3-8487-5764-0

1. Auflage 2021

Vorwort

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

Inhaltsübersicht

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/Ohnemus*)
Dr. David Bomhard Rechtsanwalt, München	§ 9 (zus. mit *Pour Rafsendjani*)
Matthias Fischer, LL.M. Regierungsdirektor, Berlin	§ 13
Dr. Christian L. Geminn, Mag. iur. Universität Kassel	§ 22 (zus. mit *Müller*)
Dr. Rotraud Gitter, LL.M. Eur. Regierungsdirektorin, Berlin	§ 15
Dr. Sebastian J. Golla Ruhr-Universität Bochum	§ 18 (zus. mit *Bäcker*)
Prof. Dr. Rüdiger Grimm Universität Koblenz-Landau	§ 2 (zus. mit *Waidner*)
Prof. Dr. Annette Guckelberger Universität des Saarlandes, Saarbrücken	§ 23
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*)
PD Dr. Silke Jandt Referatsteilleiterin bei der Landesbeauftragten für den Datenschutz Niedersachsen, Privatdozentin Universität Kassel	§ 17
Rebecca Janßen ZEW – Leibniz-Zentrum für Europäische Wirtschaftsforschung, Mannheim	§ 3 (zus. mit *Bertschek/Ohnemus*)
Dr. Henning Lahmann Senior Researcher, Digital Society Institute, European School of Management and Technology Berlin	§ 6

Dr. Philipp Lassahn, LL.M. Regierungsrat, Berlin	§ 7 (zus. mit *Poscher*)
Prof. Dr. Marian Margraf Freie Universität Berlin	§ 4 (zus. mit *Heinemann*)
Johannes Müller MLE. Universität Kassel	§ 22 (zus. mit *Geminn*)
Dr. Jörg Ohnemus ZEW – Leibniz-Zentrum für Europäische Wirtschaftsforschung, Mannheim	§ 3 (zus. mit *Bertschek/Janßen*)
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 (zus. mit *Bomhard*)
Prof. Dr. Alexander Roßnagel Universität Kassel	§ 14
Martin Schallbruch Ministerialdirektor a.D., Digital Society Institute, European School of Management and Technology Berlin	§ 1 (zus. mit *Hornung*) § 5
Marc Schardt Regierungsdirektor, Berlin	§ 25
Stephan Schindler Universität Kassel	§ 21 (zus. mit *Hornung*)
Prof. Dr. Tobias Singelnstein Ruhr-Universität Bochum	§ 20 (zus. mit *Zech*)
Philipp Singler Justiziar und behördlicher Datenschutzbeauftragter Stadt Offenburg; Lehrbeauftragter	§ 24
Isabel Skierka Digital Society Institute, European School of Management and Technology Berlin	§ 8
Sylvia Spies-Otto Ministerialdirigentin, Bundesministerium der Verteidigung, Berlin	§ 19
Prof. Dr. Gerald Spindler Georg-August-Universität Göttingen	§§ 10 bis 12
Dr. Thomas Thalhofer Rechtsanwalt, München	§ 16

Prof. Dr. Michael Waidner
Fraunhofer-Institut für Sichere Informationstechnologie SIT, Darmstadt

§ 2 (zus. mit *Grimm*)

Louisa Zech
Ruhr-Universität Bochum

§ 20 (zus. mit *Singelnstein*)

§ 1 Einführung

Literatur: *Baer*, Das Soziale und die Grundrechte, NZS 2014, 1; *Berman*, Digital transformation: oppurtunities to create new business models, Strategy & Leadership, Jg. 40, Nr. 2, 2012, 16; *Brill*, Welt- und sicherheitspolitische Trends im Spektrum der Meinungen: Thesen – Antithesen – Synthesen, ZfP 2001, 448; *Eckert*, IT-Sicherheit: Konzepte – Verfahren – Protokolle, 10. Aufl. 2018; *Erbel*, Öffentliche Sicherheit und Ordnung, DVBl 2001, 1714; *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; *Kniesel*, „Innere Sicherheit" und Grundgesetz, ZRP 1996, 482; *Kugelmann*, Polizei- und Ordnungsrecht, 2. Aufl. 2012; *Matt/Hess/Benlian*, Digital Transformation Strategies, Business & Information Systems Engineering, Jg. 57, Nr. 5, 2015, 339; *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; *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/Spieker gen. Döhmann* (Hrsg.), Datenschutzrecht, 2019; *Tannberger*, Die Sicherheitsverfassung. Eine Systematische Darstellung der Rechtsprechung des Bundesverfassungsgerichts. Zugleich ein Beitrag zu einer induktiven Methodenlehre, 2014; *Winkelhake*, Die digitale Transformation der Automobilindustrie. Treiber – Roadmap – Praxis, 2017; *Waechter*, Die Schutzgüter des Polizeirechts, NVwZ 1997, 729; *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, 2017, 721.

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 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. 1

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 2

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

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, Insulinpumpen können von Ärzten aus der Ferne gewartet werden.

5 Diese Entwicklung eröffnet **unvergleichliche Chancen** für das Leben der Menschen, hat aber auch eine gewisse Ambivalenz in sich, die das Bundesverfassungsgericht schon vor über zehn 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.

6 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

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 das Bundesministerium für Wirtschaft und Technologie im Jahre 2017 das von ihm organisierte jährliche Treffen einer Vielzahl von Entscheidungsträgern aus Wirtschaft und Politik rund um den IT-Standort Deutschland nach zehn Jahren von „IT-Gipfel" in „Digital-Gipfel" umbenannte.

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. 721 ff.

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.

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. **Kritische Infrastrukturen** können heutzutage nicht mehr sinnvoll ohne IT betrieben werden und sind deshalb essentiell auf IT-Sicherheit angewiesen.

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[9] – 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.[10] Nachrichtendienste führen Cyberoperationen durch, beispielsweise zur Wirtschaftsspionage oder zur Destabilisierung anderer Staaten (*Grimm/Waidner* in → § 2 Rn. 65 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 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. 9

B. Begriffliche Grundlagen

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).[11] Beide Begriffsbestandteile (IT und Sicherheit) lassen sich **eng oder weit verstehen**. Außerdem existieren etliche verwandte, angrenzende und teilweise überlappende 10

8 Zu den wirtschaftlichen Risiken von Cyberangriffen s. näher *Bertschek/Janßen/Ohnemus* in → § 3 Rn. 21 ff.

9 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".

10 S. zu den entsprechenden Straftatbeständen *Singelnstein/Zech* in → § 20 Rn. 37 ff.

11 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.

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

14 In diesem relativ generischen Sinne wird „Sicherheit in der Informationstechnik" auch in **§ 2 Abs. 2 BSIG** legaldefiniert. Diese bezeichnet dort „die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit 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.[12]

15 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.[13] Authentizität und Nichtabstreitbarkeit sind insbesondere im elektronischen Rechtsverkehr von erheblicher Bedeutung.

16 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 Informationen

12 Noch allgemeiner 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".

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

A. Einleitung

I. Cyberrisiken – Zielscheibe deutsche Wirtschaft

Cyberrisiken sind **omnipräsente Bedrohungen**, die jedes Unternehmen angehen. Diese Risiken müssen Unternehmen managen, nicht nur durch technisch-organisatorische Maßnahmen, sondern auch durch rechtliche, insbesondere vertragliche Maßnahmen. Einerseits beruhen diese Risiken auf menschlichem Fehlverhalten (zB Datenverlust wegen Fehlbedienung von IT-Systemen). Andererseits können Risiken auch aus Systemfehlern der IT-Infrastruktur resultieren (zB Hardwaredefekt, Software-Bugs). Weiterhin gibt es auch externe Ursachen (zB Stromausfall oder Überspannungsschäden).[1] 1

Hinzu kommt **Cyberkriminalität**. Es vergeht kaum ein Tag, an dem kein neuer Cyberangriff auf Unternehmen der deutschen Wirtschaft stattfindet. So gab es schwerwiegende Attacken auf RWE und Pilz (ein schwäbischer Spezialist für Automatisierung).[2] Die Deutsche Telekom registrierte im April 2019 allein an einem Tag 46 Millionen Cyberangriffe. 2

Steigende Risiken ergeben sich insbesondere durch den zunehmenden Einsatz internetfähiger Geräte und von Home-Office-Konzepten (zB während der Corona-Krise) sowie durch mobile und dezentrale Anwendungen (zB Cloud-Computing, Informationsplattformen für Arbeitnehmer und Kunden, Big-Data-Analysen, Zuliefererketten), die über eine Plattform organisiert werden und die auf Produktions- und Vertriebsprozesse einwirken. 3

Mit der steigenden Anzahl an vernetzten Geräten steigen die Eintrittswahrscheinlichkeit und die Höhe eines möglichen Schadens aufgrund von IT-Schwachstellen, insbesondere durch fehlerhafte oder veraltete Firmware auf diesen Geräten.[3] Zudem **verschmilzt** vor allem die **Produktionsumgebung** zunehmend mit IT-Systemen aus dem Büroumfeld. In vielen Bereichen der Industrie kommen zum Messen, Steuern und Regeln von Abläufen sog. **Industrial Control Systems** (industrielle Steuerungssysteme) zum Einsatz. Während diese in der Vergangenheit physisch von anderen IT-Systemen und Netzen entkoppelt und damit vor äußeren Einflüssen geschützt waren, ist nun seit mehreren Jahren sowohl eine zunehmende Vernetzung als auch ein fortschreitender Einzug von IT-Systemen aus dem Büroumfeld in industrielle Umgebungen zu beobachten.[4] 4

Denkt man noch die Cyberangriffe hinzu, die tagtäglich stattfinden, **ohne der Öffentlichkeit oder gar dem betroffenen Unternehmen selbst bekannt zu werden**, wird deutlich, dass kein Unternehmen vor solchen Angriffen sicher ist. Im Gegenteil: Die Anzahl und die **Hartnäckigkeit der Angriffe** nahmen über die letzten Jahre hinweg kontinuierlich zu. Gemäß einer Erhebung des Digitalverbands Bitkom, die im November 2019 veröffentlicht wurde, erleidet die Wirtschaft allein in Deutschland durch Datendiebstahl, Sabotage und Spionage einen Schaden von inzwischen 102,9 Milliarden EUR pro Jahr.[5] Schätzungen zufolge waren im Jahre 2019 ca. 75 Prozent der Unternehmen von derartigen Cyberattacken betroffen. Laut Bitkom-Präsident Achim Berg wird der Industriestandort Deutschland zunehmend zur Zielscheibe von Hackern, so dass IT-Sicherheitsmaßnahmen unabdingbar werden.[6] Ähnliches konstatierte das 5

1 *Wirth* BB 2018, 200; Achenbach VersR 2017, 1493 (1494 f.).

2 S. https://www.zeit.de/wirtschaft/2018-09/rwe-hackerangriff-internetseite-hambacher-forst; https://www.handelsblatt.com/25117634.html?.

3 Der durch das aus mehr als 300.000 IoT-Geräten bestehende Botnet „Mirai" entstandene Schaden wurde im Jahr 2016 auf ca. US-$ 100 Mio. geschätzt (https://www.gdatasoftware.com/blog/2018/09/31124-botnet-no-jailtime-for-mirai-creators).

4 *Rockstroh/Kunkel* MMR 2017, 77.

5 S. https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-100-Milliarden-Euro-Schaden-pro-Jahr; zu den einzelnen Kategorien der wirtschaftlichen Risiken mangelhafter IT-Sicherheit s. *Bertschek/Janßen/Ohnemus* in → § 3 Rn. 21 ff.

6 Bitkom-Studienbericht zum Wirtschaftsschutz in der deutschen Industrie von 2018, S. 12.

Bundeskriminalamt (BKA) in seinem Cybercrime-Bundeslagebild 2018.[7] Ausgehend vom Bericht zur Lage der IT-Sicherheit des Bundesamts für Sicherheit in der Informationstechnik (BSI) von 2019 ist mit einer drastischen Zunahme von Cyberangriffen in den nächsten Jahren zu rechnen, nicht zuletzt aufgrund der fortschreitenden Vernetzung im Zuge der Digitalisierung.[8]

II. Schäden für deutsche Unternehmen

6 Im Ergebnis sehen sich Unternehmen jeder Art und Größe deshalb mit einem enormen **Gefährdungs- und Schadenpotenzial** konfrontiert. Zu nennen sind beispielsweise Imageschäden und Produktionsausfälle. Durch Cyberkriminalität kann es zudem zu unerwünschtem Abfluss von geistigem Eigentum, Geschäftsgeheimnissen sowie Kundendaten, zum Verlust von Wettbewerbsvorteilen (zB durch nachgemachte Produkte oder Patentrechtsverletzungen) sowie zu erheblichen Ermittlungskosten, **Kosten** für die Wiederherstellung von Betriebssystemen, Rechtverfolgungskosten, aber auch zu drakonischen Bußgeldern kommen. Im Ernstfall kann fehlende IT-Sicherheit Unternehmenswerte insgesamt beeinträchtigen.[9]

III. Relevanz der IT-Sicherheit für die Vertragsgestaltung

7 Angesichts zahlreicher bekanntgewordener Datenlecks rückt das Thema **IT-Sicherheit** nicht nur in den Fokus von Politik, Justiz und öffentlicher Wahrnehmung. IT-Sicherheit ist auch für die Wirtschaft und folglich auch für die **anwaltliche Beratung von zunehmender Bedeutung.** Teil der anwaltlichen Tätigkeit ist daher vermehrt auch die Beratung von Unternehmen im Hinblick auf die Gestaltung und Formulierung von IT-Sicherheitsanforderungen in Verträgen sowie die Prüfung der Kompensation von Schäden, die infolge unzureichender IT-Sicherheit bei Unternehmen entstehen (zB wenn aufgrund eines Hackerangriffs auf ein Logistikunternehmen Pakete der Kunden nicht mehr ausgeliefert werden).

8 Dies wirft zunehmend die Frage auf, ob und wie IT-Sicherheit **Eingang in die Vertragsgestaltung** finden kann oder muss. Ist IT-Sicherheit respektive ein Cyberrisiko überhaupt zivilrechtlich adressierbar oder ist dies ein Fall der Unmöglichkeit? Welche Regelungen sind erforderlich, um (Haftungs-)Risiken zu allokieren und zu mitigieren, aber auch Compliance-Verstößen vorzubeugen? Ist die vertragliche Gestaltung von IT-Sicherheit nur ein „nice to have" oder haben Unternehmen gar eine Pflicht, sich vertraglich gegen Cyberrisiken wie zB Cyberangriffe zu schützen? Wenn ja, wie ist diese Pflicht zivilrechtlich einzuordnen? Besteht vor dem Hintergrund bestehender IT-Sicherheitsgesetze, technischer Normen und Praxisleitfäden überhaupt noch ein Bedürfnis für vertragliche Gestaltung? Wenn ja, welche Regelungen müssen IT-Sicherheitsklauseln beinhalten?

9 In dem vorliegenden § 9 werden diese Fragen beantwortet und **Möglichkeiten der vertraglichen Absicherung von IT-Sicherheit** aufgezeigt und diskutiert. Je nach Rechtsgebiet und Vertragstyp kommen unterschiedliche Vertragsgestaltungen im Betracht.

IV. Begriff der IT-Sicherheitspflicht

10 Der Begriff der IT-Sicherheitspflicht bedeutet nach seinem Wortsinn zunächst die rechtsverbindliche Aufgabe eines Rechtssubjekts (= Verpflichtung), für IT-Sicherheit (engl. *Cyber Secu-*

7 BKA – Bundeslagebild Cybercrime 2018, S. 53.

8 BSI Lagebericht zur IT-Sicherheit in Deutschland 2019, S. 75.

9 Der Angriff auf Yahoo!, bei dem Ion Milliarden von Nutzerdaten entwendet wurden, hatte zur Folge, dass sich der Kaufpreis für Yahoo beim Verkauf an Verizon im Jahr 2016 um 350 Million US-Dollar reduzierte; dazu FAZ vom 4.10.2017 https://www.faz.net/aktuell/wirtschaft/unternehmen/yahoo-drei-milliarden-accounts-von-datenklau-betroffen-15229889.html.

5. Angriffe auf den, durch den und in dem privaten Haushalt

Zum einen können die **Bewohner Betroffene von Angriffen** sein, die sich gegen Informationstechnik, Daten oder die Bewohner des privaten Haushalts richten. Zum anderen kann aber die **Informationstechnik im privaten Haushalt selbst zum Vehikel für Angriffe gegen andere** werden: Weist die Informationstechnik Privater Sicherheitslücken auf, kann dies ein **Einfallstor oder Sprungbrett** sein für Angriffe auf andere Systeme. So kann über die Informationstechnik im Haushalt versehentlich Schadsoftware weiterverbreitet werden oder die verwendeten Internet-fähige Geräte können **Teil eines Botnetzes** werden, das Angriffe auf andere IT-Systeme durchführt. Auch wenn ein Nutzer nicht sorgsam mit personenbezogenen oder anderweitig schützenswerten Daten umgeht, zB wenn er Speichermedien wie USB-Sticks mit anvertrauten Informationen verliert oder bei der persönlichen Internetnutzung solche Daten versehentlich Dritten zugänglich macht, weil er keine Sicherheitsmaßnahmen nach dem Stand der Technik (Zugriffsschutz durch Passwörter, Verschlüsselung oÄ) umgesetzt hat, verursacht er Sicherheitsprobleme. Im Gegensatz zu dem Verursachen von sicherheitsrelevanten Ereignissen aus Unkenntnis über Risiken und mögliche Gegenmaßnahmen oder aus mangelnder Fähigkeit, geeignete Maßnahmen wirksam umzusetzen, können Bewohner aber auch vorsätzlich eine aktive Rolle bei einem Angriff auf zu schützende Güter spielen. Interessant mit Fokus rein auf den privaten Haushalt sind solche Angriffe, die durch das Wahrnehmen der Kontrolle über die eingesetzte Informationstechnik ermöglicht werden und auf das Schädigen von Mitbewohnern oder Gästen zielen, beispielsweise durch ein Ausspähen von Daten. Eine **besondere Machtposition** nimmt hier der Bewohner ein, der die Informationstechnik im Haushalt oder zentrale Komponenten betreibt (→ Rn. 35 ff.). Vielfach kann sogar der bestimmungsgemäße Einsatz eine derartige Überwachung ermöglichen. 25

II. Besondere Risiken anhand der Einsatzbereiche

1. Informationstechnik im privaten Haushalt als Sprungbrett für Angriffe

Zwar können Angriffe auf die Informationstechnik eines privaten Haushalts in Ermangelung eines professionellen Sicherheitsmanagements häufig einfacher erfolgreich durchgeführt werden. Jedoch sind die Kommunikation von Familienmitgliedern oder digitale Urlaubsbilder in der Regel weniger monetär für einen Angreifer verwertbar als die Geschäftsgeheimnisse eines Unternehmens oder die Massendaten einer behördlichen Datenbank. Auch würden viele Privatpersonen bei Ransomware – also Verschlüsselung der gespeicherten Daten und erst bei Lösegeldzahlung die Zusage der Entschlüsselung – keine oder keine hohe Zahlung an den Erpresser leisten, während dies von Firmen häufiger in Erwägung gezogen wird, wenn es keine andere Möglichkeit gibt, die Geschäfts- oder Kundendaten wiederherzustellen. Dies schließt nicht gezielte Angriffe auf Einzelpersonen aus, deren Reputation beschädigt werden soll. Doch auch wenn der **Privathaushalt nicht das primäre Ziel eines Angriffs** ist, können die kursierenden **Viren und Trojaner** die dortige Informationstechnik infizieren. 26

Die Privat-IT kann außerdem als **Sprungbrett für weitere Angriffe** dienen, zB um Schadsoftware weiterzuverbreiten. Ebenso können Privatrechner gekapert und als **Teil eines Botnetzes** verwendet werden, beispielsweise um zu einem definierten Zeitpunkt von vielen scheinbar unabhängig voneinander agierenden Computern dieselben Server mit einem „Distributed Denial of Service (DDoS)-Angriff" zu überziehen. Die Privat-IT ist dann also nicht nur einem Angriff zum Opfer gefallen, sondern wird zum **Tatwerkzeug desjenigen, der das Botnetz steuert**. Es kann sein, dass diese Rechneraktivität unbemerkt von den Nutzern im Privathaushalt geschieht und nur **aktualisierte Anti-Virus-Programme** diesen Umstand mitteilen und zu beheben versuchen. Auch die Internet-Service-Provider (ISP) können oft technisch eine vorliegende Botnetz-Aktivität erkennen. Zur Eindämmung der weiteren Verbreitung solcher Schadsoft- 27

ware und zur Beschränkung ihrer Wirkung als Teil eines Botnetzes – also zum Schutz der anderen Netzteilnehmer – bietet sich an, dass die infizierten Privatrechner vom Internet abgekoppelt werden, bis die Computer gesäubert sind. Das bedeutet allerdings, dass in der Zeit der Zugriff auf das Internet abgeschnitten ist; es könnte sogar sein, dass die Nutzer damit Nachteile erleiden, weil sie damit Deadlines für zeitkritische Anträge, Abgabetermine oder Online-Auktionen verpassen. Das BSI empfiehlt den ISP, dass sie mit ihren Kunden vertraglich vereinbaren, dass die Diensteerbringung bei missbräuchlicher Nutzung eingeschränkt werden kann,[15] und sie bei der Entfernung von Schadsoftware unterstützen. Durch eine Regelung in § 109 a Abs. 5 TKG sind die **ISP auch gesetzlich berechtigt, in solchen Fällen den Datenverkehr der Kunden einzuschränken, umzuleiten oder zu unterbinden**.

28 Der Sprungbrett-Effekt lässt sich auch im Smart Home beobachten. Besonders häufig sind **Angriffsmöglichkeiten auf die smarten Glühlampen** dokumentiert, denen Sicherheitsforscher sogar teilweise attestiert haben, „insecure by design"[16] zu sein. Ein Kapern dieser vergleichsweise niedrigpreisigen Geräte kann den Angriff auf andere Smart-Home-Geräte im selben Netz ermöglichen, die ein Angreifer dann fernsteuern kann. Bei diesem Angriffstyp[17] geht es gar nicht um die Funktionalität der Glühlampe, sondern nur um das **Ausnutzen ihrer Vernetzung**.[18] Andere Angriffe richten sich tatsächlich auf die Funktion, also bei Glühlampen ein Ein- und Ausschalten auf Anforderung oder zu definierten Zeiten oder das Verändern der Helligkeit oder der Farbe. Diese **Steuerung** des Lichts machen sich wiederum andere Angriffe auf Glühlampen im Smart Home zunutze, die auf ein **Ausspionieren** gerichtet sind.[19] Doch auch Glühlampen ohne jegliche eigene informationstechnische Funktionalität können durch ihre Vibrationen verraten, was im Raum gesprochen wird: Forscher konnten mit dem Lamphone-Verfahren anhand der Beobachtung einer Glühlampe Unterhaltungen durch Teleskopaufnahmen und optische Sensoren aus 25 Meter Entfernung rekonstruieren.[20]

2. Bildaufnahmen

29 Viele Notebooks sind mit **Webcam-Funktionalität** ausgestattet; Videokonferenzsysteme können per Computer oder Smartphone bedient werden. Hinzukommen Videoüberwachungssysteme, die in vielen Privathäusern eingesetzt werden. Dies betrifft besonders die Haustür zum Zwecke der Kontrolle, wer Einlass begehrt, oder Bereiche am Haus, um Einbrecher abzuschrecken. Aber auch in der Luft per **Drohne** oder im Haus lassen sich Kameras einsetzen. Im Sinne des **„Ambient Assisted Living"** können es die Bewohner ermöglichen, dass sich in Notsituationen ein Wachdienst zuschaltet und per Video schaut, ob ein Rettungsteam alarmiert werden muss. Auch zur Überwachung von Haushaltshilfen oder Babysittern werden Videoüberwachungssysteme angeboten, zB per **„Nannycam" oder „Teddycam"** versteckt in einem Spielzeug. Die Eltern können den Babysitter ihres Kindes darüber beobachten oder im Nachhinein Aufzeichnungen anschauen. Hier ist zu berücksichtigen, dass nicht alle technischen Möglichkeiten rechtlich auch erlaubt sind. Dies betrifft insbesondere **Erfassungen des öffentli-**

15 Beispielsweise in den AGB über eine „Acceptable Use Policy", BSI, Malware-Schutz – Handlungsempfehlungen für Internet-Service-Provider (ISP), BSI-CS 046, 11.7.2018, abrufbar unter https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_046.pdf?__blob=publicationFile&v.=3.

16 *Morgner et al.*, Proc. 10th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec '17), 2017, 230.

17 *Ronen/Shamir*, 2016 IEEE European Symposium on Security and Privacy (EuroS&P), 2016, 3–12.

18 *Zhou et al.*, Discovering and Understanding the Security Hazards in the Interactions between IoT Devices, Mobile Apps, and Clouds on Smart Home Platforms, in Proceedings of the 28th USENIX Security Symposium, 2019, S. 113; *Prasad/Nagarkar,* International Journal of Applied Engineering Research 14 (7), 2019, 75.

19 Dies wird für Geschäfts- oder Staatsgeheimnisse diskutiert, wenn smarte Glühlampen in Unternehmen oder Behörden zum Einsatz kommen, siehe zB *Maiti/Jadliwala*, Article 98, 2019.

20 *Nassi et al.*, Cryptology ePrint Archive, Report 2020/708, 2020.

chen Raums, die heimliche Überwachung oder eine Kopplung mit biometrischen Analysesystemen, die allenfalls unter besonderen Bedingungen rechtmäßig sind. Auch Spiel-, TV- oder Multimediasysteme sind zunehmend mit Kameras ausgestattet, zB um bei interaktiven Spielen die Gestik oder sonstige Bewegungen der Teilnehmer zu erfassen. Für den Smart-TV-Bereich gibt es Patente, die eine **visuelle Auswertung der Zuschauer vor dem Gerät** beinhalten.[21] Dies könnte genutzt werden, um je nach Anzahl der Zuschauer für einen Film verschiedene Preise zu berechnen oder um Jugendschutzvorgaben zu erfüllen. Es könnten aber auch anhand der Mimik der Zuschauer bei TV-Programmen oder Werbung Analysen unternommen werden, was welchem Zuschauer gefällt, um zielgruppengerecht die Inhalte anzupassen oder Produkte zu bewerben.

30 Kameras, die im oder am Haus aufnehmen, zeigen damit viel von den **Gewohnheiten oder den privaten Lebensverhältnissen der einzelnen Haushaltsmitglieder und ihrer Gäste**. Daraus ergibt sich, dass Sorge dafür zu tragen ist, dass auf die Bilddaten nicht unbefugt zugegriffen werden kann. Vielfach bestehen aber **Sicherheitsprobleme**,[22] beispielsweise wenn die Kameras in einem unverschlüsselten oder anderweitig mangelhaft abgesicherten WLAN betrieben werden. Problematisch und auch unter dem Gesichtspunkt der Informationssicherheit relevant kann auch sein, wenn die Daten **zentral beim Anbieter gesammelt werden und darüber auch vereinfacht für einen behördlichen Zugriff (ggf. aus anderen Staaten) zur Verfügung stehen**.[23]

3. Tonaufnahmen und Sprachkommandos

31 Ähnlich wie für Bildaufnahmen sind im Privathaushalt Geräte zu finden, die der **Erfassung von Stimmen oder Geräuschen** dienen. Dazu gehört insbesondere jede Form von **Sprachassistenz**, um mündliche Kommandos an die Geräte zu interpretieren und auszuführen. Sprachassistenzsysteme finden sich beispielsweise in Smartphones oder in Multimediaelektronik. Aus Sicht der Informationssicherheit muss gewährleistet sein, dass vertrauliche Informationen nicht für Unbefugte zugänglich werden, nicht unbefugt Kommandos an die Geräte erteilt werden können und die autorisierten Befehle korrekt umgesetzt werden.[24] Diese Anforderungen sind nicht einfach umzusetzen. Will man beispielsweise erreichen, dass die Sprachassistenz die Befehle nur von bestimmten Personen, zB nur den Haushaltsmitgliedern, akzeptiert, könnte eine Prüfung anhand eingelernter Stimmmuster erfolgen. Damit müssten die **biometrischen Stimmmuster** erhoben werden (je nach System geschieht dies ohnehin), aber ob eine aufgeregte Stimme in einer Notfallsituation korrekt erkannt wird, ist nicht garantiert. Die Ausführung eines von einer befugten Person gegebenen Befehls kann ebenfalls Probleme aufwerfen, besonders wenn zusätzliche Dienste dafür benötigt werden: Ähnlich wie bei einem Tippfehler im Internet-Browser, der auf eine falsche Seite führt, die von einem Angreifer betrieben wird,

21 *Perez/Kipman/Fuller*, Content distribution regulation by viewing user, United States Patent Application Publication No. US 2012/0278904 A1, 1.11.2012, abrufbar unter https://patentimages.storage.googleapis.com/1d/bd/0a/55aa8bf880764e/US20120278904A1.pdf.

22 *Bugeja/Jönsson/Jacobsson*, An Investigation of Vulnerabilities in Smart Connected Cameras, PerLS'18 – Second International Workshop on Pervasive Smart Living Space.

23 In den USA hat die Electronic Frontier Foundation die Umstände einer Kooperation zwischen einem Anbieter eines Videoüberwachungssystems und der Polizei bemängelt. *Guariglia/EFF*, Five Concerns about Amazon Ring's Deals with Police, 30.8.2019, abrufbar unter https://www.eff.org/de/deeplinks/2019/08/five-concerns-about-amazon-rings-deals-police.

24 Besonders beliebt sind „Streiche", in denen Gäste einem Sprachassistenzsystem Kommandos zum Einkauf oder zum Notruf erteilen und die Besitzer versuchen, das Ausführen des Befehls zu stoppen. Siehe auch: *Hui/Leohng*, Lee Kuan Yew School of Public Policy Research Paper No. 17–21, 2017, 7 f.; *Chung et al.*, Computer 50 (9), IEEE 2017, 100.

Stichwortverzeichnis

Fette Zahlen bezeichnen die Paragrafen, magere die Randnummern.