HANNFRIED LEISTERER

Internetsicherheit in Europa

Internet und Gesellschaft
12

Mohr Siebeck

Internet und Gesellschaft

Schriften des Alexander von Humboldt Institut
für Internet und Gesellschaft

Herausgegeben von
Jeanette Hofmann, Ingolf Pernice,
Thomas Schildhauer und Wolfgang Schulz

12

Hannfried Leisterer

Internetsicherheit in Europa

Zur Gewährleistung der Netz- und Informationssicherheit durch Informationsverwaltungsrecht

Mohr Siebeck

Hannfried Ulrich Leisterer, geboren 1986; Studium der Rechtswissenschaften an der Freien Universität sowie Humboldt-Universität zu Berlin; DFG-Forschungsstudent am Graduiertenkolleg „Verfassung jenseits des Staates“; Kollegiat im Kompetenznetzwerk für das Recht der zivilen Sicherheit in Europa (KORSE) des Bundesministeriums für Bildung und Forschung und wiss. Mitarbeiter am Alexander von Humboldt Institut für Internet und Gesellschaft, Berlin; 2017 Promotion; Referendar am Kammergericht Berlin.

ISBN 978-3-16-155976-1 / eISBN 978-3-16-156266-2
DOI 10.1628/978-3-16-156266-2

ISSN 2199-0344 (Internet und Gesellschaft)

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

Das Buch wurde von Gulde Druck in Tübingen gesetzt, auf alterungsbeständiges Werkdruckpapier gedruckt und gebunden.

Wenn die ökonomische und soziale Entwicklung nicht als unabänderliches Schicksal hingenommen, sondern als permanente Aufgabe verstanden werden soll, bedarf es einer umfassenden, kontinuierlichen sowie laufend aktualisierten Information über die wirtschaftlichen, ökologischen und sozialen Zusammenhänge. Erst die Kenntnis der relevanten Daten und die Möglichkeit, die durch sie vermittelten Informationen mit Hilfe der Chancen, die eine automatische Datenverarbeitung bietet, für die Statistik zu nutzen, schafft die für eine am Sozialstaatsprinzip orientierte staatliche Politik unentbehrliche Handlungsgrundlage.

– BVerfG 65, 1 (47) – Volkszählungsurteil

Vorwort

Die Juristischen Fakultät der Humboldt-Universität zu Berlin hat die vorliegende Arbeit im Mai 2017 als Dissertation angenommen. Literatur und Rechtsprechung sind bis zu diesem Zeitpunkt berücksichtigt.

Herrn Professor Dr. Dr. h.c. Ingolf Pernice danke ich sehr herzlich dafür, dass er die Arbeit betreut und mich seit der Zeit des Studiums gefördert hat. Nicht zuletzt seine positive Haltung dient mir immer als Vorbild.

Herrn Professor Dr. Matthias Ruffert danke ich für die zügige Erstellung des Zweitgutachtens.

Die Arbeit ist im Rahmen des mit Mitteln des Bundesministeriums für Bildung und Forschung geförderten Kompetenznetzwerks für das Recht der Zivilen Sicherheit in Europa (KORSE) entstanden. Für die großzügige Förderung bedanke ich mich sehr. Das Bundesministerium des Innern hat durch einen Druckkostenzuschuss die Veröffentlichung der Arbeit ermöglicht. Dafür bin ich ebenfalls dankbar.

Eingeflossen in die Arbeit ist der Austausch mit vielen Personen. Ihnen schulde ich Dank für die Begegnungen, Erfahrungen und Erkenntnisse.

Viele Überlegungen verdanke ich meinen Kollegen Emma Peters, Dr. Adrian Haase sowie Dr. Sebastian Leuschner. In verschiedenen Abschnitten der Arbeit waren mir Marie-Luise Weckerling, Maria Rothämel, Hanna Soditt und Theresa Behrendt eine besondere Hilfe.

Für wertvolle Gespräche und die freundschaftliche Begleitung seit meinem Studium danke ich Rainer Ziemann und Kai Schmidt. Für die technische Expertise und Klärung technischer Fragen danke ich Richard Spreng. Steve Ritter vom Bundesamt für Sicherheit in der Informationstechnik danke ich für die freundlichen und geduldigen Gespräche, die mir den praktischen Hintergrund zu den rechtlichen Überlegungen deutlich machten. Für methodische Hinweise danke ich Herrn Professor Dr. Edmundt Brandt.

Nicht zuletzt möchte ich Dr. Karina Preiß sowie allen Kollegen am Alexander von Humboldt Institut für Internet und Gesellschaft (Berlin) für die wunderbare Zeit, die ich am Institut als Wissenschaftlicher Mitarbeiter hatte, danken.

Meinen Eltern, Ingeburg und Hanns-Ulrich Leisterer, und meiner Ehefrau Dorina ist diese Arbeit in Dankbarkeit gewidmet.

Hamburg im Januar 2018 Hannfried Leisterer

Inhaltsverzeichnis

§ 1 Einleitung

A. Internetsicherheit als Wissensproblem

Das Internet vernetzt mit dem bislang dominierenden Internet-Protokoll weltweit Individuen und Dinge. Alle wesentlichen Bereiche und Funktionen in heutigen Gesellschaften sind abhängig von der Informations- und Kommunikationstechnologie Internet. Daten- und Informationsinfrastrukturen bilden die Nervenbahnen des gesellschaftlichen Lebens. Das Funktionieren des Internet hat mittlerweile essenzielle Bedeutung für den Einzelnen, die Gesellschaft, die Wertschöpfungsketten und die öffentliche Aufgabenerfüllung. Die Anzahl der Nutzer und Teilnehmer steigt und es kann davon ausgegangen werden, dass das Internet für Jahrzehnte die entscheidende Infrastruktur bleiben wird.

Ein Grundproblem, das es erschwert, die Sicherheit der das Internet bildenden Netz- und Informationssysteme zu gewährleisten, ist Komplexität. Im Laufe der Entwicklung des Internets haben sich ein Maß an Komplexität und ein Grad an Kopplung desselben mit sozialen Prozessen entwickelt, die für die Infrastruktur ebenso wie für Nutzer zur Gefahr werden können.[1] Komplex sind sowohl die Informationsinfrastrukturen als auch die Angriffe auf sie. Im Zuge von Innovationszyklen und damit einhergehenden technologischen Neuentwicklungen sowie inkrementellen Verbesserungen verringert sich die die Systemkomplexität keineswegs, sondern erhöht sich tendenziell weiter. Angreifer sind innovativ und professionell und arbeiten mit leicht bedienbaren Werkzeugen. Vernetzte Systeme sind kaum isolierbar, IT-Sicherheitsumgebungen können durch manipulierte Hardware und Software kompromittiert werden und sind damit inhärent unsicher. Verschlüsselungen können schnell mit mittlerweile häufig angewandten Brute-Force-Methoden umgangen werden. Die Sicherheitslage erscheint auch deshalb als prekär, weil es als unmöglich gilt, Software zu schreiben, die keine Fehler enthält. Je nach Programmqualität liegt die Fehler-

[1] *Palfrey*/*Gasser*, Interop – The Promise and Perils of highly interconnected systems, 2012, S. 76; *Schneier*, Complexity the Worst Enemy of Security, CWHK, 17.12.2012; *King*, Science of Cyber-Security, Mitre Report JSR-10-102, 2010, S. 14; vgl. Erwägungsgrund 1 VO (EU) Nr. 526/2013; *Brown*, Research Handbook on Governance of the Internet, 2013, S. 152; Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland, 2016, S. 7.

quote zwischen 5 und 0,0001 Prozent.[2] Bei anspruchsvolleren Programmen mit mehreren hundert Millionen Zeilen Code kann dies zu einer beträchtlichen Quantität an Angriffswegen führen. Die Anzahl an Sicherheitslücken, die für einen Hack ausgenutzt werden können, liegt bei ungefähr 5 Prozent. Hinzu kommt, dass nicht nur stetig neue Sicherheitslücken, sondern ebenso konstant neue Exploittechniken geschaffen werden, also Techniken, die dazu dienen, Sicherheitslücken auszunutzen.[3]

Die Ubiquität und gleichzeitige Interdependenz von Informationstechnologien lassen Kaskadeneffekte als ein realistisches und nicht zu ignorierendes Szenario erscheinen.[4] Denn nicht nur ermöglicht die Vernetzung Angriffe aus großer Entfernung, sondern sie steigert die Anfälligkeit und Verwundbarkeit von Systemen und potenziert damit Angriffsvektoren.[5]

Aufgrund der Dynamik der digitalen Entwicklung lassen sich die Folgen von Störungen kaum vorhersagen. Denn zur Eigenschaft komplexer Systeme gehört auch, dass sich das Verhältnis von Ursache und Wirkung aufgrund des Grades der Abhängigkeiten und Wechselwirkungen der die Systeme konstituierenden Elemente nicht linear verhält und demnach Kausalverläufe keineswegs immer überschaubar und transparent sind.[6] Kleine Veränderungen können disproportionale Auswirkungen haben. Das Ideal von Voraussage und Kontrolle ist weitgehend unerreichbar, da die Faktoren, von denen individuelle Ereignisse abhängen, in der Regel so zahlreich sind, dass sie in ihrer Gesamtheit nicht ermittelt werden können.[7] In der Cyber-Sicherheitsforschung wird aus diesem Grund zunehmend nach analogen Bewältigungsstrategien und erklärenden Mustern in

---

[2] *Gaycken*, Cybersecurity in der Wissensgesellschaft, in: Daase/Engbert/Junk (Hrsg.), Verunsicherte Gesellschaft – Überforderter Staat, 2013, S. 109 (115 f.).

[3] *Gaycken*/*Lindner*, Zero Day Governance – A(n Inexpensive) Solution to the Cyber Security Problem, in: Cyber Dialogue – What is Stewardship in Cyberspace, 2012, S. 13.

[4] *Petermann*/*Bradke*/*Lüllmann*/*Poetzsch*/*Riehm*, Was bei einem Blackout geschieht, Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag, 2011, S. 31, 70 ff.

[5] Vgl. Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2015, 2015, S. 35; Kommission, Impact Assessment accompanying the Proposal for a NIS Directive, SWD(2013) 32 final, S. 13; Bundeskriminalamt, Cybercrime, Bundeslagebild, 2014, S. 12 ff.

[6] Vgl. BVerfGE 120, 274 (306): „Informationstechnische Systeme haben mittlerweile einen derart hohen Komplexitätsgrad erreicht, dass ein wirkungsvoller sozialer und technischer Selbstschutz erhebliche Schwierigkeiten aufwerfen und zumindest den durchschnittlichen Nutzer überfordern kann."

[7] *von Hayek*, Die Theorie komplexer Phänomene, in: Kerber (Hrsg.), Die Anmaßung von Wissen, 1996, S. 281 (295); *Gaycken*, Cybersecurity in der Wissensgesellschaft, in: Daase/Engbert/Junk (Hrsg.), Verunsicherte Gesellschaft – Überforderter Staat, 2013, S. 109 (115 f.); *ders*., Öffentliches Fachgespräch des Ausschusses Digitale Agenda des Deutschen Bundestages zum Thema IT-Sicherheit, A-Drs. 18(24)10, S. 3.

anderen Bereichen gesucht, die ebenfalls durch Komplexität gekennzeichnet sind. Wegen der Ähnlichkeit von Schadprogrammen mit pathogenen Infektionen werden etwa terminologische Anleihen bei der Epidemiologie genommen. So ist in der IT-Sicherheit von Viren, Würmern oder Infektionen die Rede.[8]

Dies zeigt, dass die Komplexität der technischen Basis und die Faktenkomplexität zugleich zu einer „hohen epistemischen Komplexität" führen.[9] Verschiedene Sichtweisen, Konzeptionierungen, Kategorisierungen, Differenzierungen, Klassifizierung und Kontextualisierungen mit Bezug auf technisch immer anspruchsvollere Netze, Systeme und Programme führen bei den Akteuren unweigerlich zu einer komplexeren Betrachtung der Probleme in der Internetsicherheit. Sie ist zwar auch erforderlich, um unzulässige oder unzuverlässige Simplifizierungen zu vermeiden. Allerdings führt sie auch dazu, dass selbst die Experten das Feld kaum mehr überblicken, Probleme erkennen, Schwierigkeiten priorisieren oder Verwundbarkeiten determinieren können.[10]

Da die Komplexität des Internets für menschliche Beobachter kaum mehr zu durchdringen ist, stellt sich die Netz- und Informationssicherheit für die Akteure als kognitive und epistemische Unsicherheit und damit als Herausforderung dar.[11]

Organisationen verfolgen zur Mitigation von Gefahren für die Sicherheit grundsätzlich einen reduktionistischen Ansatz. Anders als es ein holistischer Ansatz erfordern würde, konzentrieren sich Unternehmen daher auf die IT-Sicherheit ihrer eigenen Systeme mit einem starken Fokus auf Kausalität. Somit gehören Schutzschichten wie Firewalls, Intrusion Detection Systems oder Anti-Viren-Programme zu verbreiteten Maßnahmen zur Abwehr von Gefahren für die IT-Sicherheit. Ein etablierter Ansatz im Risikomanagement ist außerdem das automatisierte Testen und Validieren der Systeme.[12] Problematisch an for-

---

[8] Vgl. *Armstrong/Mayo/Siebenlist*, Complexity Science Challenges in Cybersecurity, 2009, S. 4; *Eckert*, IT-Sicherheit, 2000, S. 58 ff., 68 ff.

[9] *Gaycken*, Cybersicherheit in der Wissensgesellschaft, in: Daase/Engbert/Junk (Hrsg.), Verunsicherte Gesellschaft – Überforderter Staat, 2013, S. 109 (117).

[10] *Gaycken*, Cybersicherheit in der Wissensgesellschaft, in: *Daase/Engbert/Junk* (Hrsg.), Verunsicherte Gesellschaft – Überforderter Staat, 2013, S. 109 (120).

[11] Der Begriff „kognitiv" wird für Vorgänge intellektueller Art verwendet, die sich innerhalb des Menschen abspielen, vgl. *Eberle*, Organisation der automatisierten Datenverarbeitung in der öffentlichen Verwaltung, 1976, S. 39, Fn. 31; *Dörner*, Die Logik des Misslingens – Strategisches Denken in komplexen Situationen, 11. Aufl. 2012, S. 61 f., *von Foerster*, The Curious Behavior of Complex Systems, in: Linstone/Simmonds (Hrsg.), Futures Research: New Directions, 1977, S. 104 (106 ff.), die veranschaulichen, dass Komplexität vor allem eine subjektive Größe ist, was heißt, dass die Wahrnehmung, ob eine Situation komplex ist oder nicht, von der jeweiligen Person abhängt. Kognitive Kompetenz kann aber in Erweiterung der rein anthropozentrischen Perspektive auch in Operationsformen und Organisationen manifestiert sein. Dazu unten unter § 3 B.

[12] Etwa durch Penetrationstests, siehe *Eckert*, IT-Sicherheit, 2014, S. 210.

malen Verfahren ist jedoch, dass selbst dann, wenn Problemstellungen in der Informatik in Logik, Mathematik und Algorithmen ausgedrückt werden können, nicht sichergestellt ist, dass sie vollständig konsistent oder in endlicher Zeit entscheidbar sind.[13] Hinzu kommt das Problem der Informationsasymmetrien. Das adäquate Erkennen von Risiken und Gefahren für die Netz- und Informationssicherheit ist für kleine Einheiten wie Unternehmen sehr kostenintensiv. Infolge fehlender Investitionsanreize und Moral Hazard können epistemische Unsicherheiten das Niveau der Netz- und Informationssicherheit stagnieren oder sogar sinken lassen.[14]

Bei allgemeinerer Betrachtung wird deutlich, dass das Wissensproblem in der Cybersicherheit *pars pro toto* für die Wissensprobleme der vernetzten Informations- und Wissensgesellschaft steht.[15] Bei diesen Gesellschaftsbeschreibungen handelt es sich um Bedeutungsträger, die den Komplexitätszuwachs einer Gesellschaft zusammenfassen.[16] Es sind die „funktionsspezifischen Operationsweisen" der gesellschaftlichen Bereiche, in denen Wissen wissenschaftlich organisiert und zum zentralen Faktor wird, die für moderne Gesellschaften diese übergreifenden Beschreibungen rechtfertigen.[17] Die Karriere des Internets hat die allgemeine Paradigmenverschiebung, die zu einer Neuordnung in eine Informations- und Wissensverteilung führte, mitverursacht.[18] Charakteristisch für die Wissensgesellschaft ist, dass wegen der Spezialisierung und Ausdifferenzierung der gesellschaftlichen Bereiche kein relevanter Akteur allein über

---

[13] Zu diesem fundamentalen Problem *Sassaman/Patterson/Bratus/Shubina*, The Halting Problems of Network Stack Insecurity, login Vol. 36 (No. 6), 2011, 22 (22 f.). Ob sich das Problem zukünftig durch künstliche Intelligenz und Quantencomputing lösen lässt, sei hier dahingestellt.

[14] Moral Hazard bezeichnet im Zusammenhang mit Internetsicherheit das Phänomen, dass sich private Betreiber von Netz- und Informationssystemen sich einer kostenintensiven Verantwortung für Sicherheit entziehen würden, weil sie auf eine staatliche Intervention im Falle von Sicherheitsvorfällen spekulierten. Dazu *Irion*, The Governance of Network and Information Security in the European Union, in: Krüger/Nickolay/Gaycken (Hrsg.), The Secure Information Society, 2013, S. 5 ff.; *Andersson/Malm*, Public-Private Partnership and the Challenge of Critical Infrastructure Protection, in: Dunn/Mauer (Hrsg.), International CIIP Handbook 2006, Vol. II, 2006, S. 139 (143); *Hämmerli/Renda*, Protecting Critical Infrastructure in the EU, 2010, S. 49 f.; vgl. *Bauer/van Eeten*, Telecommunications Policy 33 (2009), 706 (710 f.).

[15] Vgl. zur wissenssoziologischen Perspektive auch *Werle/Schimank* (Hrsg.), Gesellschaftliche Komplexität und kollektive Handlungsfähigkeit, 2000, S. 12; *Roßnagel/Wedde/Hammer/Pordesch*, Die Verletzlichkeit der ‚Informationsgesellschaft', 2. Aufl. 1989, S. 28, 42, 46 ff.

[16] Vgl. *Vesting*, Zwischen Gewährleistungsstaat und Minimalstaat. Zu den veränderten Bedingungen der Bewältigung öffentlicher Aufgaben in der „Informations- und Wissensgesellschaft", in: Hoffmann-Riem/Schmidt-Aßmann (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, 2015, S. 101 (107 ff.).

[17] So *Weingart/Carrier/Krohn* (Hrsg.), Nachrichten aus der Wissensgesellschaft, 2007, S. 38.

[18] Vgl. *Hoeren*, NJW 1998, 2849 (2854).

entscheidungsrelevantes Wissen verfügt. Das handlungs- und entscheidungsrelevante Wissen ist stattdessen gesamtgesellschaftlich und in den Teilbereichen dezentral vorhanden, d. h., eine zentrale Stelle, welche die Informationen aggregiert vorrätig hält, existiert grundsätzlich nicht, auch nicht in den gesellschaftlichen Subbereichen.

Aus der Dezentralisierung des Wissens folgt, dass das entscheidungsrelevante Wissen für die Bewältigung öffentlicher Aufgaben problemorientiert zusammengetragen werden muss.[19] Gleiches gilt für den Bereich der Internetsicherheit. Kollektiv besteht maßgebliches Wissen über den Zustand der Systeme. Vor allem nach der Privatisierung und Deregulierung der IKT-Infrastruktur ist das Wissen jedoch gesellschaftsweit verstreut.[20] So sind etwa Informationen über kritische IT-Schwachstellen und Sicherheitslücken, sofern überhaupt bekannt, auf verschiedene Unternehmen, Personen oder Behörden verteilt und nur fragmentiert vorhanden.

Komplexität hat als Problembegriff zwar Entlastungspotenzial. Doch sind komplexe Systeme nicht vorschnell mit komplizierten Systemen gleichzusetzen. Komplexität darf nicht zum Deckmantel für Resignation werden, indem mit der Unterstellung von gesellschaftlicher Selbstorganisation das Fehlen von Gestaltungsversuchen von vorneherein zu entschuldigen.[21] Wird die Gewährleistung der Internetsicherheit als Wissensproblem aufgefasst,[22] so stellt sich vor allem für den Staat als wissensbasierte Organisation[23] die Frage, wie das Recht mit diesem Problem umgeht. Unter der Prämisse, dass Rechtswissenschaft „nicht allein oder vorrangig als normtextorientierte Interpretationswissenschaft verstanden, sondern […] als problemlösungsorientierte Handlungs- und Entscheidungswissenschaft konzipiert werden [muss]“,[24] ist danach zu fragen, welche rechtlichen Instrumente dazu beitragen können, Probleme zu lösen.

---

[19] Vgl. *Wollenschläger*, Wissensgenerierung im Verfahren, 2009, S. 34 ff.; *Ladeur*, Postmoderne Rechtstheorie: Selbstreferenz – Selbstorganisation – Prozeduralisierung, 2. Aufl. 1995, S. 209 f.

[20] Siehe dazu die als Bangemann-Bericht bekannt gewordenen Empfehlungen vom 26.05. 1994 an den Europäischen Rat von Korfu „Europa und die globale Informationsgesellschaft“, 1994.

[21] Zum zeithistorischen Wandel des Begriffs Komplexität weg von einem, der dafür stand, Phänomene in ihrer Ganzheit zu erfassen, hin zu einem Problembegriff *Leendertz*, Das Komplexitätssyndrom. Gesellschaftliche Komplexität als intellektuelle und politische Herausforderung in den 1970er Jahren, MPIfG Discussion Paper 15/07.

[22] Im Kontext der Energieregulierung *Herzmann*, Konsultationen – Eine Untersuchung von Prozessen, kooperativer Maßstabskonkretisierung in der Energieregulierung, 2010, S. 33 ff.

[23] *Voßkuhle*, Das Konzept des rationalen Staates, in: Schuppert/Voßkuhle (Hrsg.), Governance von und durch Wissen, 2008, S. 13 (16); vgl. *Schulz*, Rewi 3 (2012), 330 (330).

[24] *Hoffmann-Riem*, Regulierungswissen in der Regulierung, in: Bora/Henkel/Reinhard, Wissensregulierung und Regulierungswissen, 2014, S. 135 (138).

Die vorliegende Arbeit nimmt das geschilderten Wissensproblem zum Anlass zu untersuchen, wie das Recht zur Lösung des Problems der Internetsicherheit beitragen kann. Die These lautet, dass das Informationsverwaltungsrecht mit seiner epistemischen Funktion zur Bewältigung des Wissensproblems einen Beitrag zur Gewährleistung der Sicherheit von Netz- und Informationssystemen in der Europäischen Union zu leisten vermag. Im Nachfolgenden wird untersucht, mit welchen informationsverwaltungsrechtlichen Instrumenten zur Initiierung, Strukturierung und Organisation von Informationen und Wissen dieser Beitrag zur Internetsicherheit geleistet werden könnte.

B. Aufbau der Untersuchung

In einem ersten Schritt werden Internetsicherheit und Informationsverwaltungsrecht einander zugeordnet (§ 2). Dabei wird der Untersuchungsgegenstand, die Gewährleistung der Internetsicherheit in Europa, zunächst begrifflich gefasst und losgelöst vom rechtlichen Kontext in seinen technischen Eigenschaften betrachtet. Doch ohne Theorie bleiben die Fakten ohne Aussagekraft. Nach der Betrachtung der technischen Dimension werden daher die extrajuristische Dimension des Wissensproblems und die epistemische Funktion des Informationsverwaltungsrechts entfaltet, um herauszuarbeiten, wie Recht als Steuerungsfaktor – Steuerung verstanden als indirekter Einfluss hinsichtlich eines Ziels und nicht etwa im Sinne der Beherrschung eines Zustands oder einer linearen Einwirkung – im Kontext des Internets Wirkung in der Sicherheitsgewährleistung entfalten kann. Zur weiteren Bestimmung des Beitrags des Informationsverwaltungsrecht unterscheidet die Untersuchung, dem Informationszyklus der administrativen Informationsverarbeitung folgend, Generierung, Transfer und Distribution sicherheitsrelevanter Informationen durch die informationsverarbeitende Administrative.

Die Generierung von Informationen über die Internetsicherheit ist grundlegend für die Erkenntnisgewinnung durch die Verwaltung (§ 3). Durch die Bestimmung der Reichweite der verfassungsrechtlichen Pflicht zur Informationsgenerierung und des die Akteure bestimmenden Organisationsrechts sowie die Betrachtung der rechtlichen Regelungen zur Generierung von sicherheitsbezogenen Informationen kann nachvollzogen werden, ob und welche Informationen bei den jeweiligen privaten Betreibern und Anbietern erhoben werden können. Diese Untersuchung lässt Aussagen darüber zu, in welchem Ausmaß das Wissensproblem durch Recht berücksichtigt und abgebildet wird und inwieweit dies noch eingefordert werden muss. Die Bewertung der Wirksamkeit der informationsverwaltungsrechtlichen Instrumente hängt auch davon ab, inwieweit das

Recht Grenzen kalkulierten Nichtwissens setzt. Besondere Grenzen werden hinsichtlich des Selbstbelastungsschutzes, des Datenschutzes und des Schutzes unternehmensbezogener Daten identifiziert.

Nach der Betrachtung der Generierung von Informationen wendet sich der Blick auf den Transfer von Informationen, d. h. auf die Weitergabe von Informationen im Rahmen der europäischen Kooperation im Bereich der Netz- und Informationssicherheit (§ 4). Dabei zeigt sich, dass die Union auch und gerade in sicherheitsbezogenen Politikbereichen auf Informationskooperation angewiesen ist, um handlungs- und entscheidungsrelevantes Wissen zu generieren und so Kompetenz- und Vollzugsdefizite im Bereich der Netz- und Informationssicherheit auszugleichen. Die Richtlinie (EU) 2016/1148 zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie) bezweckt, einen Rahmen für die Zusammenarbeit auf europäischer Ebene zu schaffen, und steht daher im Zentrum der Untersuchung des grenzüberschreitenden Informationstransfers. Besondere Begrenzungen für den Informationsfluss können neben dem Schutz von personenbezogenen und unternehmensbezogenen Daten aus dem Organisationsrecht folgen.

Die Generierung und der Transfer von Informationen dienen den nationalen und europäischen Informationsbedürfnissen der Verwaltung. Da vor allem Unternehmen und Bürgerinnen und Bürger als Hersteller, Anwender und Nutzer von Produkten und Systemen im Bereich der IT-Sicherheit auf eine funktionierende Internetinfrastruktur angewiesen sind, stellt sich die Frage, wie die durch die Verwaltung erhobenen Informationen und wie das so geschaffene Wissen weitergehend zur Sicherheitsgewährleistung genutzt werden kann. Da die Verfolgung von Individualinteressen durch unterschiedliche Eigenrationalitäten, Verhaltensmuster und Erfahrungsbestände eine entscheidende Schubkraft zur Verwirklichung von Gemeinwohl ist, wird schließlich untersucht, ob und wie die gesammelten Informationen durch Distribution, d. h. durch rechtliche Informationsbeziehungen der Verwaltung zu Privaten, in der Gewährleistung der Internetsicherheit fruchtbar gemacht werden können (§ 5). Zugrunde gelegt wird dabei die Annahme, dass das Informationshandeln des Staates nicht nur dem demokratischen Partizipationsgedanken verpflichtet ist, sondern darüber hinaus auch den gewandelten kognitiven Bedingungen der Gesellschaft.

Wegen der technischen Konvergenz und der mitunter einheitlichen Gefahren für die Netz- und Informationssicherheit können bestimmte Regelungsmaterien nicht immer auseinandergehalten werden. So kann die zivile Sicherheit nicht als streng von der militärischen Sicherheit des Internets getrennt erfasst werden. Die Untersuchung beschränkt sich indes auf die Aspekte der zivilen Sicherheit, zumal in der europäischen NIS-Kooperation ein Informationsaustausch mit militärischen Stellen nicht ausdrücklich vorgesehen ist. Sicherheit in der Informa-

tionstechnik wird zudem zu wichtigen Teilen präventiv durch das Polizeirecht und repressiv durch das Strafrecht und Strafverfolgungsrecht verfolgt. Diese Materien sind zum einen schon vielfach untersucht worden und zum anderen würden die legislativen Entwicklungen hier eigene monografische Behandlungen rechtfertigen.[25] Gegenstand der Arbeit ist daher der sich auf europäischer Ebene entwickelnde Bereich der Netz- und Informationssicherheit außerhalb der Abwehr polizeirechtlicher Gefahren und der Strafverfolgung.[26] Soweit informationsrechtliche Schnittstellen hinsichtlich der Datenflüsse der NIS-Zusammenarbeit zu Stellen relevant werden, die Daten zu Zwecken der Polizei- und Strafverfolgung verarbeiten, werden diese Rechtsbereiche in die Untersuchung mit einbezogen.

---

[25] Vgl. *Saloven*/*Grant*/*Hanel*/*Makai*/*Hansen*/*Belevicius*/*Pohnitzer*, Study on the status of information exchange amongst law enforcement authorities in the context of existing EU instruments, 2010, S. 84 f.

[26] Die Cybersicherheitsstrategie der Europäischen Union, JOIN(2013) 1 final, S. 20, teilt das „Thema der Cybersicherheit" in drei zentrale Bereiche auf, für die unterschiedliche Rechtsrahmen gelten. Neben der Netz- und Informationssicherheit sind dies die Strafverfolgung und die Verteidigung. Im Sinne dieser Strategie konzentriert sich die Arbeit auf Rechtsfragen des erstgenannten Bereichs.

§ 2 Internetsicherheit und Informationsverwaltungsrecht

Die Untersuchung des Beitrags des Informationsverwaltungsrechts zur Internetsicherheit in Europa erfordert wegen der begrifflichen Unschärfe eine eingrenzende Bestimmung des Begriffs der Internetsicherheit (A.). Eine kurze Skizzierung der Funktionsweise des Internets und der tatsächlichen wie rechtlichen Grenzen seiner Regulierbarkeit (B.) sollen zu der Frage leiten, wie Informationsverwaltungsrecht zur Lösung des Wissensproblems und damit zur Gewährleistung der Internetsicherheit in Europa beitragen kann (C.).

A. Schutzzielbezogene Eingrenzung der Internetsicherheit auf Netz- und Informationssicherheit

Der Begriff der Internetsicherheit ist aufgrund seiner verschiedenen Verwendungsmöglichkeiten unscharf. Gemeint sein kann die Sicherheit des Internets (Internet als Schutzobjekt), die Sicherheit im Internet (Internet als Medium zur Übertragung rechtswidriger Inhalte) oder die Sicherheit vor dem Internet (Internet als Angriffsmittel).[1] Der im Kontext von Internet und Sicherheit verwendete

[1] Grundsätzlich können je nach Typ des Angriffs auf eine NIS-Infrastruktur und der Angreifer die Begriffe Cyberkriminalität, Cyberspionage, Cybersabotage oder Cyberkrieg abgegrenzt werden. Dabei geht es um Verstöße gegen Vermögensrechte im weiten Sinne, um Einbrüche in fremde Datenbanken staatlicher oder nicht staatlicher Unternehmen und um staatliche Versuche, Interessen internetbasiert durchzusetzen, *Bendiek*, Europäische Cybersicherheitspolitik, 2012, S. 7. Unter den Bedrohungen mit geringem bis mittlerem Schadenspotenzial werden weiter Formen des Cyberaktivismus und Cybervandalismus diskutiert, *Chiesa/Ducci/Ciappi*, Profiling Hackers, 2009; *Dunn Cavelty*, Cyber(Un)Sicherheit: Grundlagen, Trends und Herausforderungen, in: Schieren (Hrsg.), Neue Medien, alte Fragen? Das Internet in der Politik, 2012, S. 66 ff. So bezieht sich Cyberkriminalität eher auf Verstöße gegen Eigentums- und Vermögensrechte von Privaten, während Cyberspionage Einbrüche in Datenbanken von staatlichen und nicht staatlichen Unternehmen durch fremde Staaten beschreibt. Unter Cyberwar kann der Versuch eines Staates verstanden werden, einen anderen Staat nachhaltig zu schädigen, vgl. *Robinson/Disley/Potoglou/Reding/Culley/Penny/Botterman/Carpenter/Blackman/Millard*, Feasibility Study for a European Cybercrime Centre,

Begriff der Cybersicherheit ist nicht wesentlich schärfer. Er steht eher in einem sicherheitspolitischen Zusammenhang und verweist auf die Gesamtheit der Politiken, Organisationen und Verfahren, die auf die Gewährleistung der Sicherheitseigenschaften von Informations- und Telekommunikationsinfrastrukturen gerichtet sind.[2] Im europäischen Primärrecht findet sich lediglich der denkbar weite kompetenzrechtliche Begriff der Computerkriminalität in Art. 83 Abs. 1 UAbs. 2 AEUV aus dem Politikbereich des Raums der Freiheit, der Sicherheit und des Rechts (Art. 67 ff. AEUV). Dort umfasst der Kriminalitätsbereich das Internet sowohl als Angriffsobjekt als auch als Tatmittel, d. h., auch inhaltsbezogene Straftaten wie Aussagedelikte oder Straftaten gegen das geistige Eigentum, die mittels Computersystemen begangen werden, sind erfasst.[3] In Ermangelung eines im europäischen Primärrecht verankerten Begriffs der Internetsicherheit ist es für die weitere Operationalisierung des Begriffs erforderlich, eine schutzzielbezogene Eingrenzung vorzunehmen.

Als Ansatzpunkt für die schutzzielbezogene Eingrenzung kann der Begriff der IT-Sicherheit herangezogen werden. Zwar besteht ein abgeschlossenes Rechtsgebiet der IT-Sicherheit nicht und der Bereich zeichnet sich durch verstreute Einzelregelungen aus.[4] Eine Definition der IT-Sicherheit findet sich jedoch im BSIG, dessen § 2 Abs. 2 lautet: „Sicherheit in der Informationstechnik […] bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen 1. in informationstechnischen Systemen, Komponenten oder Prozessen oder 2. bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen." IT-Sicherheit bezieht sich damit auf die in der Vorschrift genannten Schutzziele, also die Verfügbarkeit, Unversehrtheit im Sinne von Integrität und Vertraulichkeit von Informationen, die elektronisch gespeichert sind oder derart verarbeitet werden.[5] Diese Schutzziele wer-

---

2012, S. 17–55. Neben Vermögenswerten kann auch die staatliche Sicherheit ein gefährdetes Rechtsgut sein. Es lassen sich für die NIS neben anthropogenen Gefahren auch naturgegebene Gefahrenquellen anführen, *Saurugg*, Die Netzwerkgesellschaft und Krisenmanagement 2.0, 2012, S. 74.

[2] ITU, Definition of cybersecurity, ITU-T X.1205, abrufbar unter: http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.

[3] *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), AEUV/EUV, 57. Aufl. 2015, Art. 83 AEUV, Rn. 62; siehe auch das Übereinkommen des Europarates über Computerkriminalität vom 23.11.2011 (*Cybercrime Convention*), BGBl. 2008 II S. 1242, 1243, 2010 II S. 218, einschließlich des Zusatzprotokolls vom 28. Januar 2003 betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art, BGBl. 2011 II S. 290, 291, 843.

[4] Vgl. *Schmidl*, NJW 2010, 476 (477); *Spindler*, MMR 2008, 7 (8 ff.).

[5] *Heckmann*, MMR 2006, 280 (281).

den allerdings durch das BSIG selbst nicht näher bestimmt. Der Bedeutungsgehalt der Schutzziele wird aus der Informatik abgeleitet. Die Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen und sie schützt (zudem) davor, dass ausschließlich Befugten Informationen in zulässiger Weise zugänglich sind.[6] Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und Informationen und der korrekten Funktionsweise von Systemen und schützt vor unerlaubter Veränderung derselben. Verfügbarkeit meint, dass Dienstleistungen, Funktionen eines IT-Systems und IT-Anwendungen oder IT-Netze oder Informationen von den Anwendern stets wie vorgesehen genutzt werden können. Informationssicherheit umfasst die Maßnahmen und das Management zur Gewährleistung dieser Ziele.[7]

Die europäische Entsprechung des Begriffs der IT-Sicherheit ist die Netz- und Informationssicherheit (NIS). Deren Definition ergibt sich aus einer Richtlinie, die von der Kommission 2013 als Kernelement der EU-Cybersicherheitsstrategie[8] vorgeschlagen wurde. Die Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in Europa (NIS-RL) macht in Art. 1 Abs. 1 die Netz- und Informationssicherheit zum Gegenstand der rechtlichen Maßnahme. NIS bezeichnet nach der Begriffsbestimmung in Art. 3 Abs. 2 NIS-RL die „Fähigkeit von Netzen und Informationssystemen, bei einem bestimmten Vertrauensniveau Störungen und böswillige Angriffe abzuwehren, die die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit gespeicherter oder übermittelter Daten oder entsprechender Dienste beeinträchtigen, die über dieses Netz und Informationssystem angeboten werden beziehungsweise zugänglich sind".[9] Die NIS-RL geht über die Aufzählung der Schutzziele in § 2 Abs. 2 BSIG hinaus. Die Authentizität von Informationen soll sicherstellen, dass sie von der angegebenen Quelle erstellt wurde, wobei sie sich sowohl auf Personenidentitäten als auch auf IT-Komponenten oder Anwendungen bezieht.[10] Unter Netzen und Informationssystemen sind

---

[6] Zu diesen Definitionen das Glossar des IT-Grundschutz-Katalogs des BSI, abrufbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html.

[7] Vgl. auch *Schmidl*, IT-Recht von A–Z, 2014, S. 149 f.; *Conrad*, in: Auer-Reinsdorff/dies., IT- und Datenschutzrecht, 2. Aufl. 2016, § 33 Rn. 16 ff.; vgl. auch *Schmidl*, IT-Recht von A–Z, 2014, S. 149 f.

[8] JOIN(2013), 1 final.

[9] Vgl. die Definition der internationalen Fernmeldeunion (ITU): „Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets", abrufbar unter: http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.

[10] Zu dieser Definition das Glossar des IT-Grundschutz-Katalogs des BSI, abrufbar unter:

nach der Begriffsbestimmung in Art. 3 Abs. 1 a) bis c) NIS-RL zum einen elektronische Kommunikationsnetze im Sinne der RL 2002/21/EG zu verstehen, zum anderen Computerdaten automatisch verarbeitende (miteinander verbundene oder zusammenhängende) Vorrichtungen und zuletzt Computerdaten, die zum Zwecke des Betriebs, der Nutzung, des Schutzes und der Pflege gespeichert, verarbeitet, abgerufen oder übertragen werden.

Das sekundärrechtliche Begriffsverständnis der Netz- und Informationssicherheit ist sehr weit. Es stellt aber einen spezifischen Bezug zum Funktionieren der Netze und Informationssysteme her. Abgegrenzt werden können so inhaltsbezogene rechtswidrige Handlungen, auch wenn sie im umfassenderen Cybersicherheitsdiskurs eine Rolle spielen. Einbezogen werden können über den Begriff der Netz- und Informationssicherheit auch Gefahren, die ihre Ursache nicht in einem kriminellen Verhalten haben. Netz- und Informationssicherheit bzw. IT-Sicherheit gehen nicht zuletzt über den Begriff des Datenschutzes hinaus.[11] Datenschutz ist nur insofern ein Teilaspekt der Netz- und Informationssicherheit, als auch nicht personenbezogene Daten einbezogen werden.[12]

Internetsicherheit soll im Folgenden als Netz- und Informationssicherheit verstanden werden. Demnach zielt Internetsicherheit darauf, die Verfügbarkeit von Diensten und Daten zu gewährleisten, die Störung und das unerlaubte Abhören des Kommunikationsverkehrs zu verhindern, die Vollständigkeit und Richtigkeit von übermittelten, erhaltenen und gespeicherten Daten zu bestätigen, die Vertraulichkeit der Daten sicherzustellen, Informationssysteme gegen unerlaubten Zugriff zu schützen, Informationssysteme vor Angriffen unter Verwendung von Schadprogrammen zu schützen oder die zuverlässige Authentifizierung sicherzustellen.

---

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html;zu den über § 2 BSIG hinausgehenden Schutzinteressen *Heckmann*, MMR 2006, 280 ff.

[11] *Forgó*, Grundzüge des Informationssicherheitsrechts, in: Grützmacher/Conrad (Hrsg.), Recht der Daten und Datenbanken im Unternehmen, 2014, § 64, Rn. 4; vgl. *Feiler*, Information Security Law in the EU and the U.S., 2011, S. 14 f.

[12] Vgl. *von Lewinski*, Die Matrix des Datenschutzes, 2014, S. 4 f.; *Feiler*, Information Security Law in the EU and the U.S., 2011, S. 20. Siehe auch die Schutzziele in Art. 32 Abs. 1 b) und c) DS-GVO.

B. Infrastrukturbedingte Sicherheitsprobleme und Regulierbarkeit des Internets

Um die Schnittstelle von Technik und (Informationsverwaltungs-)Recht herzustellen, sind die relevanten Eigenschaften des Internets zu skizzieren.[13] Dazu ist auf die grundlegende Infrastruktur und auf spezifische Sicherheitsprobleme des Internet einzugehen (I.). Eine Regulierung, auch zur Gewährleistung der Sicherheit, ist hinsichtlich der Risiken und Gefahren und aufgrund der technischen Eigenschaften des Internets begrenzt, aber nicht ausgeschlossen (II.).

I. Infrastruktur des Internets

Die strukturellen Eigenschaften des Internets von heute sind Folge spezifisch historisch-kontingenter Ausgangsbedingungen. In Folge des Sputnikschocks und des „Wettlaufs ins All" wurde in den Vereinigten Staaten von Amerika die Advanced Research Project Agency (ARPA) gegründet, um wissenschaftliche Forschungseinrichtungen zu koordinieren. Ein Vorläufer des modernen Internets, das ARPANET, entstand 1969, als die erste Verbindung eines Rechners der University of California und der ARPA hergestellt wurde. Zum Zwecke einheitlicher Kommunikationsstandards entwickelte die später umbenannte Defense Advanced Research Project Agency (DARPA) die Protokollsuite TCP/IP. Die Migration des ARPANET auf TCP/IP galt zum 01.01.1983 als abgeschlossen und kann als die Geburtsstunde des Internets gewertet werden kann. Die von der (D)ARPA entwickelten TCP/IP-Protokolle und andere Paketvermittlungsdienste bilden noch heute das Rückgrat des Internets.[14] Der Verweis auf die Protokolle, d. h. verschiedene Kommunikationsregeln zur Datenübertragung, weist bereits auf den Tatbestand, dass das Internet nicht als die Summe der Elemente der physikalischen Infrastruktur verstanden werden kann. Zum Verständnis des Internets gehören auch die logischen Verknüpfungen.[15] Nicht nur die physische Infrastruktur in Gestalt von Hardware, sondern auch (techno-)logische Internetdienste und Protokolle bilden das Internet. Dieses Strukturverständnis vom Internet lässt sich in einem Modell abbilden, in dem die Vorgänge der Datenübertragung und Verarbeitung verschiedenen, aufeinander aufbauenden Schichten (*layer*) zugeordnet werden, die eine je unterschiedliche Funktion erfüllen.[16] Die bekanntesten Schichtenmodelle sind das ISO/OSI-Referenz-

[13] ENISA, Understanding the importance of the Internet Infrastructure in Europe, 2013, S. 29.

[14] *Internet Society*, Brief History of the Internet, 2012, abrufbar unter: www.internetsociety.org/brief-history-internet.

[15] Vgl. *Koenig*/*Loetz*/*Neumann*, Telekommunikationsrecht, 2004, S. 34.

[16] *Kurose*/*Ross*, Computer Networking: A Top-Down Approach, 6. Aufl. 2013, S. 47 ff.;

modell und das TCP/IP-Modell.[17] Alle Modelle haben gemeinsam, dass systembedingte Sicherheitslücken und Schwachstellen in unterschiedlicher Weise auf diesen Ebenen auftreten können.[18] In der gröbsten Differenzierung lässt sich zwischen der physikalischen Infrastrukturebene (1.) und der logischen Strukturebene (2.) unterscheiden.

1. Physikalische Infrastruktur

In der physikalischen Schicht (*physical layer*) bzw. Verbindungsschicht werden elektrische Spannungszustände als kleinste Informationseinheiten (*bits*) übertragen, um Verbindungen zwischen Rechnern aufzubauen. Verschiedene Übertragungsmedien mit unterschiedlichen Spezifikationen kommen für die Transmission in Betracht. Es lassen sich grob leitungsgebundene (z. B. Kabel- oder Glasfasernetze) und drahtlose Netze (z. B. Mobilfunk- oder Satellitennetze) differenzieren.[19] Aus der Telefonie sind die Netzarten Zugangs- und Teilnehmernetze bekannt.[20] Das Internet stellt keine originäre Netzart dar, sondern ist ein Netzwerk von Netzen.[21]

Ein Telekommunikationsnetz oder eine Telekommunikationsinfrastruktur wird in der Nachrichtentechnik als die Gesamtheit von Netzknoten und Netzkanten verstanden, die eine Verbindung der Endpunkte, etwa zum Zwecke des Informationsaustausches, ermöglichen.[22] Es wäre unzweckmäßig, die Teilnehmer des Netzes untereinander unmittelbar zu verbinden. Sinnvoller ist es, die Teilnehmer über Vermittlungsstellen, also Netzknoten, zu verbinden. Dies geschieht mittels geeigneter Steuerungsprotokolle, die die Verbindungswege schalten. In einem weltweiten Netzwerk kommunizieren Rechner mit Hilfe standardisierter Protokolle miteinander. Eine stetig wachsende Anzahl voneinander unabhängiger Netzwerke, sog. autonomer Systeme (AS), die sich selbst aus Teilnetzen zusammensetzen und über Router miteinander verbunden sind, bilden das Internet. Verbindendes Element der das Internet bildenden AS ist die gemeinsam verwendete „Sprache", das TCP/IP-Protokoll. Die autonomen Systeme selbst wiederum werden aus verschiedenen Teilnetzen zusammengesetzt, die

---

Kühling/*Schall*/*Biendl*, Telekommunikationsrecht, 2014, S. 53 ff. Es gibt verschiedene solcher Schichtenmodelle. Für die Untersuchung genügt eine Orientierung am sog. OSI-Modell (Open Systems Interconnection).

[17] *Koenig*/*Braun,* K&R-Beilage 2/2002, 1 (16).

[18] *Eckert*, IT-Sicherheit: Konzepte – Verfahren – Protokolle, 2000, S. 93, 95.

[19] *Kühling*/*Schall*/*Biendl*, Telekommunikationsrecht, 2014, S. 55.

[20] Vgl. *Klußmann*, Lexikon der Kommunikations- und Informationstechnik, 2003, S. 956.

[21] Vgl. dazu *Klußmann*, Lexikon der Kommunikations- und Informationstechnik, 2003, S. 494.

[22] Vgl. *Jung*/*Warnecke*, Handbuch für die Telekommunikation, 2014, Einl. 4-3.

über Router verbunden sind. Alle unterstehen aber einer einzigen administrativen Instanz. Betreiber autonomer Systeme sind Internetdienstanbieter (Internet Service Provider), Webhoster, größere Unternehmen und öffentliche Internetaustauschpunkte. Koordinationsstelle der AS-Netze ist die zentrale Internet Assigned Numbers Authority (IANA). Sie zeichnet dafür verantwortlich, die konkrete Administration an die jeweiligen Regional Internet Registries (RIR) zu delegieren. Für Europa ist dies das Reseaux IP Européens (RIPE). Topologisch hat das Internet eine dezentrale Architektur ohne eine zentrale Verbindungsstelle. Mit der eigenen Terminologie des Internets werden größere Verbindungen als *backbones* bezeichnet und größere Knotenpunkte als *peering-points*. Einer der größten Internetknotenpunkte ist der DE-CIX in Frankfurt am Main.

2. Logische Infrastruktur

Die logische bzw. technologische Infrastruktur setzt auf die technische Infrastruktur auf und stellt weitere Verbindungs- und Funktionselemente zur Verfügung. Die in der Informatik so genannten Protokolle stellen die Regeln bereit, nach denen Informationssysteme in Netzwerken kommunizieren und Daten austauschen. Auf der Internetschicht regelt das wichtige Basisprotokoll im TCP/IP-Modell, das Internet Protocol (IP), die Datenübertragung. Es stellt sicher, dass Datenpakete vom Quellhost zum Zielhost übertragen werden. Die Funktionsfähigkeit des Internets hängt darüber hinaus von anderen Protokollen wie dem File Transfer Protocol (ftp), dem Hypertext Transfer Protocol (http) oder dem Simple Mail Transfer Protocol (smtp) ab. Schwachstellen in diesen Protokollen können dazu führen, dass ein schädlicher Code übertragen wird. Zum Teil sind bereits Protokollerweiterungen vorhanden, die einen Beitrag zur Gewährleistung der Sicherheit leisten. Für das Internet Protocol der Version 6 (IPv6), das Nachfolgeprotokoll des IPv4, gibt es mit IPsec eine Protokollsuite, die zur Gewährleistung der Schutzziele Vertraulichkeit, Authentizität und Integrität beiträgt und etwa IP-Spoofing, also das Versenden von IP-Paketen mit gefälschter Absender-IP-Adresse, verhindern soll. Ein ähnliches Beispiel ist HTTPS, dass das Hypertext-Übertragungsmodell schützen soll. Allerdings hat der sog. Heartbleed-Bug, eine für das nahezu gesamte Internet kritische Sicherheitslücke, gezeigt, dass auch Erweiterungen von Verschlüsselungsprotokollen schwerwiegende Programmierfehler aufweisen können.[23]

---

[23] Der Heartbleed-Bug war ein Fehler im OpenSSL (Secure Sockets Layer), einer freien Software, die die Transportschicht verschlüsseln sollte. Durch den Programmierfehler konnten verschlüsselte Datentransporte eingesehen und so private Daten von Clients und Servern ausgelesen werden.

Für den Adressraum im Internet ist das Domain Name System (DNS) wichtig. Dieses Domainnamensystem ist eine verteilte Datenbank, die den numerischen IP-Adressen Zeichenketten zuordnet und die Adressen nutzerfreundlich auflöst. Als essenzielle Komponente der Internetinfrastruktur wird das DNS vorrangig zur Ausnutzung von Sicherheitslücken herangezogen. Bei der Entwicklung des DNS wurde die Sicherheit kaum berücksichtigt. Besonders anfällig ist es daher für Man-in-the-Middle-Angriffe und für Cache Poisoning. Bei diesen Bedrohungen werden gefälschte Daten verwendet, um Internetverkehr auf ungewünschte Adressen umzuleiten. Auf diese Weise können etwa Kreditkartendaten extrahiert oder Benutzerkennwörter gestohlen werden, Angreifer können sich in die Voice-over-IP-Kommunikation (VoIP) einschalten und schädliche Software installieren. Da einzelne DNS-Nameserver für die Auflösung des Namens für Tausende Benutzer fungieren können, können die Folgen eines Angriffs auf diese Server sehr weitreichend sein.

Die Sicherheitslücken und Schwachstellen in der Infrastruktur sowie den Diensten und Anwendungen des Internet sind systembedingt. Daneben können Gefahren für die Sicherheit durch die Interaktionen der internen Computerprogramme und externen Anwendungen auftreten, d. h. dann, wenn das Programm (Software) auf einem Client, der an das Internet angeschlossen ist, mit einem externen Dienst interagiert. So kann etwa ein Browser, der als Software auf dem Client die Nutzung der Plattform „www“ erlaubt, externe Dienste wie http, ftp oder das E-Mail-Protokoll smtp in Anspruch nehmen. Akteure der Nutzung können Hersteller von IT-Produkten, Anbieter von Diensten oder Nutzer von Programmen sein. Gefahren für die Netz- und Informationssicherheit können dabei vorsätzlich verursacht oder auch auf sonstige Mängel und Fehlverhalten zurückzuführen sein. Die Schwachstellen machen die Netze und Systeme zu einem Angriffsziel vorsätzlich schädigender Handlungen, die auf die Störung oder den Ausfall des Betriebs der Systeme gerichtet sind. Die Zunahme von Tragweite, Häufigkeit und Auswirkungen von Sicherheitsvorfällen, die eine erhebliche Bedrohung für den störungsfreien Betrieb von Netz- und Informationssystemen darstellen, war ein zentraler Grund für den Erlass der NIS-Richtlinie.[24]

II. Regulierbarkeit des Internets

Das Internet hat eine mit dem Buchdruck vergleichbare emanzipatorische Wirkung auf die Gesellschaft. Nicht ohne Grund sind dem Internet ein anarchischer Zug und ein egalitärer Kern zugeschrieben worden.[25] Die Natur des Internets

[24] Erwägungsgrund 1 der NIS-RL.

[25] *Engel*, Der egalitäre Kern des Internet. Eine vernachlässigte Herausforderung für Steue-

mit seiner – subjektiv – fehlenden topografischen Lokalität und der dadurch bewirkte virtualisierte Raumeindruck lassen es plausibel erscheinen, den Raum zunächst als Cyberspace mit weitestgehend begrenzter Staatlichkeit zu begreifen, da Staat herkömmlich als Territorialverband begriffen wurde.[26] *Lawrence Lessig* erweckte mit seinem durch ihn verbreiteten prominenten Postulat *Code is law* den Eindruck, eine rechtliche Regulierung sei wegen der technischen Funktionsweise des Internets nicht möglich. Vielmehr seien Code bzw. Software und Hardware „cyberspace's law".[27] Die immer noch bemühte Parole, „das Internet" oder der „Cyberspace" sei ein rechtsfreier Raum,[28] ist rechtlich betrachtet jedoch nicht mehr haltbar. Sie verkennt die das Internet beeinflussenden Regeln und Regelungen und die Entwicklung der Rechtsprechung.

Das Internet ist kein rechtsfreier Raum und im Grundsatz regulierbar.[29] Zwar stößt das Paradigma staatlichen Rechts für die Regulierung dieser prinzipiell globalen Infrastruktur an kaum überwindbare Grenzen.[30] Klassische Unterscheidungen wie Völker- und nationales Recht, Norm und Vertrag, öffentliches und Privatrecht sind wenig dazu geeignet, den Charakter dieses Ordnungsrahmens treffend zu beschreiben. Das Internet wird aber in einem Ordnungsrahmen verwaltet, der als Internet Governance oder als spezifisches Regelungsarrangement beschrieben werden kann.[31]

---

rungstheorie und Steuerungspraxis, in: Ladeur (Hrsg.), Innovationsoffene Regulierung des Internet, 2003, S. 25 (25 ff.); vgl. *Mayer-Schönberger*, Journal of Law Technology and Policy I (2001), 1 (12); aus wissenschaftshistorischer Sicht und zur Entwicklungslinie der Counterculture zur Cyberculture *Turner*, From counterculture to cyberculture. Stewart Brand, the Whole Earth Network, and the rise of digital utopianism, 2008, passim.

[26] *Hobe*, Cyberspace – der virtuelle Raum, in: Isensee/Kirchhof (Hrsg.), HbStR XI, 3. Aufl. 2009, § 231 Rn. 10.

[27] *Lessig*, Code and Other Laws of Cyberspace, 1999, S. 6.

[28] *Barlow*, A Declaration of the Independence of Cyberspace, 08.02.1996, abrufbar unter: https://www.eff.org/cyberspace-independence. Der Beginn lautet: „Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear." Vgl. *Schmidt/Cohen*, The New Digital Age, 2013, S. 3.

[29] Für eine völkerrechtliche Perspektive siehe Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN-Dok. A/68/98*, 24.06.2013, Abs. 19 ff.

[30] Vgl. *Pernice*, Die Verfassung der Internetgesellschaft, in: Blankenagel (Hrsg.), Den Verfassungsstaat nachdenken, 2014, S. 171 ff.

[31] Dazu *Hofmann*, Internet Governance, in: Schuppert (Hrsg.), Governance-Forschung –

Die mit der Entwicklung des Internet geführte Debatte um die Regulierung und Regulierbarkeit, die sowohl Fragen der technischen Infrastruktur, den Zugang zum Internet als auch das Verhalten im Internet betrifft, differenzierte sich entsprechend der internetspezifischen Handlungen und Vorgänge.[32] Auffassungen vom Internet als anarchischen Raum konnten spätestens mit Beginn von Rechtsprechungen, die das Verhalten „im" Internet betreffen, nicht mehr beibehalten werden.[33] Auch solche Auffassungen, nach denen das Internet nur einer Selbstregulierung durch neuartiges Recht, das auf einem „market for law" entstehe, zugänglich sei, weil das Internet die Bedeutung geografischer Orte und der Territorialität aufhebe, sind schon deshalb nicht aufrechtzuerhalten, weil eine staatliche Intervention in die Selbstregulierung sich nicht verhindern lässt und die Funktion staatlicher Gerichte als letzter Weg für Rechtsstreitigkeiten nicht aufgehoben ist.[34] Ferner ist die These, das Internet sei etwas fernab jeglicher herkömmlicher politischer Grenzen, technisch nicht haltbar.[35] Die international verbreitete und territorial differenzierte Praxis der Internetzensur, die Tendenzen der Fragmentierung oder „Balkanisierung" des Internets[36] und die Überwachung im und durch das Internet haben nach der anfänglichen Euphorie zur Ernüchterung geführt. Sie zeigen auf, welche Einflussnahmen auf das Internet staatlicherseits möglich sind.[37] Das Urheberrecht ist ein weiteres Beispiel für staatliche Handlungsmöglichkeiten. Die Durchsetzbarkeit des Rechts stößt mit der Digitalisierung zwar an weitere Grenzen. Aufgrund einer zunehmenden Be-

---

Vergewisserung über Stand und Entwicklungslinien, 2005, S. 277 ff.; *Viellechner*, Transnationalisierung des Rechts, 2013, S. 147 ff.

[32] *Viellechner*, Transnationalisierung des Rechts, 2013, S. 110.

[33] Etwa AG München, NJW 1998, S. 2386 ff. – CompuServe I. In dem Fall wurde der Geschäftsführer der deutschen Tochtergesellschaft eines Internetanbieters mit Sitz in den Vereinigten Staaten von Amerika wegen öffentlicher Zugänglichmachung von Daten mit pornografischem Inhalt für strafbar gemäß §§ 184 Abs. 3 Nr. 2, 11 Abs. 3, 13, 14 Abs. 1 Nr. 1, 25 Abs. 2 StGB befunden.

[34] *Viellechner*, Transnationalisierung des Rechts, 2013, S. 114.

[35] Exemplarisch für technisch mögliche Nationalisierungen des Internets im Sinne einer nationalen Einwirkung auf Teile des Internets waren zuletzt etwa die 2011 von Ägypten und Libyen im Zusammenhang mit den Aufständen beobachtbare Abschaltung von Teilnetzen des Internets (autonomer Systeme) und die Manipulation der Routing-Einträge des Border Gateway Protocol (BGP) bei den Internetdienstanbietern. Siehe dazu *Dainotti/Squarcella/Aben/Claffy/Chiesa/Russo/Pescapè*, IEEE/ACM TON 2014, S. 1964 ff.

[36] *Hill*, Internet Fragmentation, Harvard Belfer Center for Science and International Affairs Working Paper, 2012.

[37] Vgl. *Wählisch/Schmist/de Brün/Häberlen*, Exposing a Nation-Centric View on the German Internet – A Change in Perspective on AS-level, in: Taft/Ricciato (Hrsg.), Proc. of the 13th PAM, 2012, S. 200 ff.

reitschaft zur internationalen Kooperation schaffen Nationalstaaten Regelungen, die Abhilfe bei den Vollzugsdefiziten zu schaffen versuchen.[38]

Die anfänglichen Missverständnisse über das sind ist nicht nur im Verständnis der Natur und Architektur des Internets begründet. Dass das internationale Recht als geeignete Arena für eine Regelung des Internets in Betracht kommt, wurde anfangs schlicht nicht berücksichtigt.[39] Fragen der Regulierung des Internets und der Verwaltung der Kernressourcen wurden jedoch bereits auf den von der Internationalen Fernmeldeunion (Internet Telecommunications Union – ITU) ausgerichteten Weltgipfeln zur Informationsgesellschaft 2003 und 2005 auf internationaler Ebene behandelt.[40] Bestrebungen, das Internet in den Regelungsbereich der ITU mit einzubeziehen und von den seit 1998 bestehenden International Telecommunications Regulations (ITRs) zu erfassen und damit ein anderes Regulierungsmodell zu etablieren, sind indes zuletzt 2012 nicht erfolgreich gewesen.[41]

Richtig ist hingegen, dass eine Internetregulierung nicht ausschließlich durch staatliches Recht stattfinden kann. Dies gilt insbesondere für die technische Regulierung, die für die hier relevante sicherheitsrechtliche Betrachtung maßgeblich ist. Zum einen stößt in territorialer Hinsicht die Regulierung *de jure* an Jurisdiktionsgrenzen. Eine staatliche Regulierung mit extraterritorialem Geltungsanspruch wäre mangels Durchsetzbarkeit und angesichts etwaigig auftretender Regelungswidersprüche unwirksam, eine internationale Kooperation in diesem Bereich dürfte mit erheblichen Schwierigkeiten verbunden sein. Zum anderen stieße die Rechtsexpansion einzelner oder mehrerer Staaten im Kontext des Internet nicht zuletzt in demokratietheoretischer Hinsicht auf Legitimationsschwierigkeiten. Überdies sind wesentliche „Bestandteile" des Internets *de facto* nicht

---

[38] Exemplarisch hier die sog. Internetverträge der Weltorganisation für geistiges Eigentum (World Intellectual Property Organization – WIPO). Der WIPO-Urheberrechtsvertrag (WIPO Copyright Treaty) und der WIPO Performances and Phonogram Treaty verpflichten die 156 WIPO-Mitgliedstaaten zu urheberrechtlichen Maßnahmen zum Schutze von Urhebern sowie zu Maßnahmen, um dem Umgehen von Kopierschutztechnik (DRM) mit rechtlichen Vorkehrungen entgegenzuwirken; vgl. auch *Dreier*, GRUR 1997, 859 ff.; allgemein und sehr informiert über das Urheberrecht als Teil der Internetregulierung *Peukert*, GRUR-Beilage 2014, 77 ff.

[39] *Mayer*, Europäisches Internetverwaltungsrecht, in: Terhechte (Hrsg.), Verwaltungsrecht in der Europäischen Union, 2011, § 25 Rn. 4 Fn. 8, mit dem Argument, *Lessig* habe in Code and Other Laws of Cyberspace, 1999, seine Argumentation diesbezüglich nicht konsequent zu Ende verfolgt.

[40] *Kleinwächter*, Internet Governance – die Kontroverse des WSIS. Eine globale Ressource im Spannungsfeld nationaler Interessen, Medienheft Dossier 24, 2005, S. 29 (29 ff.), online abrufbar; vgl. *Fischer,* www.InfrastrukturInternet-Cyberterror.Netzwerk, 2007, S. 44 f.

[41] Vgl. World Conference on International Telecommunications (WCIT-12), abrufbar unter: http://www.itu.int/en/wcit-12/Pages/default.aspx; *Spies*, MMR-Aktuell 2012, 339462.

durch staatliches Recht determiniert oder sie sind Produkte von Organisationen, die nicht staatlich organisiert werden. Als Beispiel mag das Arrangement zur Vergabe von Domains im Internet dienen.[42] Für die Verwaltung des globalen Adressierungsraums für das Internet ist unter anderem die Internet Assigned Numbers Authority (IANA), eine Abteilung der Corporation for Assigned Names and Numbers (ICANN), verantwortlich, die über ein Netzwerk von Verträgen Domains im Internet vergibt und bei der es sich um eine nach kalifornischem Gesellschaftsrecht verfasste gemeinnützige Körperschaft handelt.[43] Die ICANN hat eine Regulierungsmacht, die nicht auf einem staatlichen Gewaltmonopol beruht, sondern auf der Kontrolle einer technischen Infrastruktur, der sog. A-Root-Server, die ihrerseits an den groben Konsens (*rough consensus*) der Administratoren und Eigentümer der Netze rückgekoppelt ist.[44] Die ICANN übernimmt auch sicherheitsbezogene Aufgaben. Die Verwaltung etwa des internetsicherheitsrelevanten DNSSEC-Schlüssels gehört zum Aufgabenbereich der ICANN im Rahmen der IANA-Funktion.[45] Als weiteres Beispiel können die Internetprotokolle herangezogen werden. Die verbreitetsten Protokolle, die das Internet verwendet, sind offene, d. h. nicht proprietäre, Protokollsuiten. Deren Dokumentationen werden in technischen Berichten spezifiziert und im Verfahren des sog. Requests for Comments (RFC) von der Internet Engineering Task Force (IETF) verabschiedet und veröffentlicht.[46] Bei der IETF handelt es sich um einen formlosen Zusammenschluss von Freiwilligen wie Netzwerkingenieuren, Netzbetreibern, Herstellern, Anwendern, für die keine Mitgliedschaftsvoraussetzung besteht und deren Entscheidungen über Internetstandards im *rough consensus* gefunden werden.[47] Die Protokollsuite IPSec ist eine der Erweiterungen, die von der IETF in einer Reihe von RFCs offiziell standardisiert und dokumentiert werden.[48]

Das Internet stellt sich demnach nicht als singuläre Technologie dar, die rechtlich durch zielgerichtete und lineare Einwirkung beherrscht werden kann. Das Internet setzt sich aus vielen Netzen und Systemen in unterschiedlichen

---

[42] *Viellechner*, Transnationalisierung des Rechts, 2013, S. 127 ff.; zur Funktion siehe § 2 B. I.

[43] Siehe zur Entstehungsgeschichte *Hutter*, Global Regulation of the Internet Domain Name System: Five Lessons from the ICANN Case, in: Ladeur (Hrsg.), Innovationsoffene Regulierung des Internets – Neues Recht für Kommunikationsnetzwerke, 2003, S. 39 ff.

[44] Zur weiteren Funktionsweise *Weber*, Internet-Governance, in: Hoeren/Sieber/Holznagel (Hrsg.), Handbuch Multimedia-Recht, 42. Aufl. 2015, Teil 2, Rn. 10.

[45] ICANN, DNSSEC, abrufbar unter: https://www.icann.org/resources/pages/dnssec-qaa-2014-01-29-en.

[46] *Kurose*/*Ross*, Computer Networking: A Top-Down Approach, 6. Aufl. 2013, S. 5.

[47] *Clark*, A Cloudy Crystal Ball – Vision of the Future, in: Davies et al. (Hrsg.), Proceedings of the Twenty-Fourth Internet Engineering Task Force, 1992, S. 539 (543).

[48] Vgl. IETF, RFC 6071, abrufbar unter: https://tools.ietf.org/html/rfc6071.

Jurisdiktionen zusammen. Verschiedene Akteure entscheiden über die Rahmenbedingungen und kritischen Komponenten des Internets, die jeweils die Sicherheit beeinflussen.[49] Die Entwicklung normativ verbindlicher Standards und Prinzipien über ein „Völkerrechts des Netzes" wird zwar bereits progressiv vorgedacht, der Wandel wird indes naturgemäß wohl noch einige Zeit in Anspruch nehmen.[50]

C. Sicherheitsgewährleistung durch Informationsverwaltungsrecht

Eine direkte Steuerung der Sicherheitseigenschaften des Internets als prinzipiell globale Infrastruktur durch das Recht ist, wie aufgezeigt, derzeit wegen des fehlenden regulierenden Zugriffs und mangels einer zentralen Stelle nur schwer vorstellbar. Werden die Gewährleistung der Sicherheit von Netzen und Informationssystemen aus der Wissensperspektive betrachtet und die Sicherheitsgewährleistung als Wissensproblem begriffen, so stellt sich die Frage, ob und wie das Recht einen Beitrag für den Umgang mit den Bedingungen disparaten Wissens und der epistemischen Unsicherheit leisten kann.

Hier setzt das Informationsverwaltungsrecht an. In seiner Gesamtheit als das Recht des Umgangs mit Informationen durch die Verwaltung betrachtet, vermag das Informationsverwaltungsrecht zur Sicherheitsgewährleistung beizutragen, indem es in der Verwaltung den Prozess der Produktion und der Verteilung von spezifischen Informationen und spezifischem Wissen über die Internetsicherheit anleitet und so strukturell die Prävention und Detektion von und Reaktion auf Sicherheitsprobleme fördert. Dabei ist die Vorstellung, das Wissensproblem mit einem allwissenden Staat anzugehen, schon im Ansatz absurd.[51] Es ist bereits ausgeschlossen, dass ein Staat allein alle Sicherheitsprobleme und Schwach-

---

[49] In tatsächlicher Hinsicht ist auf die Abhängigkeit der meisten Staaten von kommerzieller Hard- und Software und damit auch von deren Sicherheit hinzuweisen. Nach *Dickow*/*Bashir*, Sicherheit im Cyberspace, APuZ 43–45/2016, S. 15 (16) sei nationale technologische Souveränität in der Informationstechnik schon deshalb eine Illusion, weil die Produktions- und Lieferketten globalisiert sind. Für die meisten Staaten würde souveräne Informationstechnik wirtschaftlich auch keinen Sinn ergeben, da die heimischen Märkte zu klein für die nötigen Investitionen in Forschung, Entwicklung und Produktion seien.

[50] Zu den Elementen einer Verfassung des Internets *Pernice*, „Völkerrecht des Netzes" – Konstitutionelle Elemente eines globalen Rechtsrahmens für das Internet, in: Biaggini/Diggelmann/Kaufmann (Hrsg.), Polis und Kosmopolis, FS Thürer, 2015, S. 576 (580 ff.); zur „aktuellen psychopolitischen Weltlage" *Sloterdijk*, Zorn und Zeit, 4. Aufl. 2016, S. 282 ff.

[51] Siehe *Lepsius*, Steuerungsdiskussion, Systemtheorie und Parlamentarismuskritik, 1999, S. 17; zur These, dass das Wissen einer Gesellschaft verteilt ist und warum es besser genutzt

stellen im Internet erfassen kann. Aufgrund seiner epistemischen Funktion ist dagegen das Informationsverwaltungsrecht geeignet, den rechtlichen Umgang mit dem Wissensproblem in der Sicherheitsgewährleistung zu organisieren (I.). Es stellt mit den Kategorien Generierung, Transfer und Distribution einen rechtlichen Ordnungsrahmen für die Informationsverarbeitung und das Informationshandeln durch die Verwaltung bereit. Diese Kategorien können herangezogen werden, um den Beitrag des Informationsverwaltungsrechts zur Gewährleistung der Internetsicherheit zu untersuchen (II.). Erforderlich ist für die anschließende Untersuchung eine Erhellung der Begriffe Daten, Information, Wissen und Kommunikation (III.).

I. Epistemische Funktion des Informationsverwaltungsrechts

Während im Privatrecht den kontrahierenden Parteien die Verteilung und der Austausch von Informationen obliegt und sich daher im Zivilrecht tendenziell nur die Privatautonomie begrenzende und den strukturell unterlegenen Vertragspartnern schützende informationsbezogene Regeln finden, um Informationsasymmetrien zu nivellieren (etwa § 119 oder § 123 BGB, Verbraucherschutzvorschriften und Aufklärungspflichten im Wertpapierhandel),[52] muss sich im öffentlichen Recht in den geregelten Sachbereichen je eine Informationsordnung etablieren, die Informationsdefizite und -asymmetrien für das politische und administrative System auszugleichen bezweckt.[53] Der Umgang mit Informationen und Wissen wird daher zu den größten Herausforderungen des Rechts im Allgemeinen und der Neuen Verwaltungsrechtswissenschaft im Besonderen gezählt.[54] Diese Herausforderung besteht insbesondere dort, wo der Staat das für ihn erforderliche Wissen nicht selbst generieren kann, wie dies bei privaten Diensten und privatisierter Infrastruktur der Fall ist. Insofern ist es Aufgabe des Regulierungsrechts als Privatisierungsfolgenrecht, die „veränderten Wissensverhältnisse" rechtlich einzufassen.[55]

---

werden kann, wenn es dezentral zur Planung verwendet wird, *Hayek*, The Use of Knowledge in Society, American Economic Review Vol. 35 (1945), S. 519 ff.

[52] *Fleischer*, Informationsasymmetrie im Vertragsrecht, 2001; vgl. *Wielsch*, Zugangsregeln – die Rechtsverfassung der Wissensteilung, 2008, S. 29.

[53] *Trute*, Wissen – Einleitende Bemerkung, in: Röhl (Hrsg.), Wissen – Zur kognitiven Dimension des Rechts, Die Verwaltung, Beiheft 9, 2010, S. 11 (23).

[54] *Hoffmann-Riem*, Eigenständigkeit der Verwaltung, in: ders./Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band I, 2. Aufl. 2012, § 10, Rn. 131; *Trute*, Wissen – Einleitende Bemerkung, in: Röhl (Hrsg.), Wissen – Zur kognitiven Dimension des Rechts, Die Verwaltung, Beiheft 9, 2010, S. 11 (22).

[55] *Wollenschläger*, Wissensgenerierung im Verfahren, 2009, S. 119; *Augsberg*, Informationsverwaltungsrecht, 2014, S. 119; *Herzmann*, Konsultationen, 2010, S. 35 ff.; allgemein

Gleichwohl sind im gesamten öffentlichen Recht Regelungen vorzufinden, die bestimmen, welcher Informationen und Daten der Staat bedarf, damit er die ihm übertragenen Aufgaben erfüllen kann, da staatliches Handeln stets Informationen und Wissen voraussetzt.

Im Informationsrecht als dem Rechtsgebiet, welches Informationen zum Gegenstand hat, sind erste informationsrechtliche Leitvorstellungen und Systematisierungen entwickelt worden.[56] Das Informationsrecht hat seine Wurzeln zwar im Datenschutzrecht, geht indes über dieses hinaus. Es ist insofern rechtsgebietsübergreifend und kein erweiterter Datenschutz.[57] Mit den spezifisch öffentlich-rechtlichen Gegenständen befasst sich das Informationsverwaltungsrecht. Damit ist „die Gesamtheit jener öffentlich-rechtlichen Normen gemeint, die sich auf den staatlichen Umgang mit Informationen und Kommunikationshandeln beziehen und die das Informationsverhalten der Behörden untereinander sowie gegenüber dem Bürger regeln".[58] Es bezeichnet die „rechtliche Anleitung einer angemessenen Informationsverarbeitung der Administrative, die zur rechtsinternen Wissenskonstruktion beiträgt […]".[59] Insoweit erfüllen rechtliche Mechanismen, etwa im Verfahrens-[60] oder durch Organisationsrecht,[61] eine „vielfach latent bereits vorhandene epistemische Funktion".[62]

Dem Informationsverwaltungsrecht als reflexivem Recht geht es insoweit „weniger um die Herausarbeitung eines gänzlich neuartigen Phänomens als um die Einübung einer gegenüber der Tradition gewandelten Perspektive, um auf diese Weise eine Seite der verwaltungsrechtlichen Untersuchungsgegenstände in den Blick zu bekommen, die in der traditionellen Fokussierung nicht gänzlich fehlt, aber abgeschottet geblieben ist."[63] *Hoffmann-Riem* formulierte in diesem Sinne den Imperativ informationsverarbeitenden und informierenden Verwal-

---

Stohrer, Informationspflichten Privater gegenüber dem Staat in Zeiten von Privatisierung, Liberalisierung und Deregulierung, 2007, passim.

[56] Vgl. *Kloepfer*, Informationsrecht, 2002, S. V: „Das Informationsrecht ist das spezifisch informationsbezogene Recht der Informationsgesellschaft".

[57] *Albers*, Rechtstheorie 33 (2002), 61 (66); *Schmidt-Aßmann*, Das allgemeine Verwaltungsrecht als Ordnungsidee, 2. Aufl. 2006, 6. Kap. Rn. 5.

[58] *Pitschas*, Allgemeines Verwaltungsrecht als Teil der öffentlichen Informationsordnung, in: Hoffmann-Riem et al. (Hrsg.), Reform des allgemeinen Verwaltungsrechts. Grundfragen, 1993, S. 219 (242).

[59] *Augsberg*, Informationsverwaltungsrecht, 2014, S. 34.

[60] *Wollenschläger,* Wissensgenerierung im Verfahren, 2009, passim.

[61] *Kluth*, Die Strukturierung von Wissensgenerierung durch das Verwaltungsorganisationsrecht, in: Spiecker gen. Döhmann/Collin (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, 2008, S. 73 ff., passim; *Schmidt-Aßmann*, Verwaltungsorganisationsrecht als Steuerungsressource, 1997.

[62] *Augsberg*, Informationsverwaltungsrecht, 2014, S. 34.

[63] *Augsberg*, Informationsverwaltungsrecht, 2014, S. 34.

tungshandelns: „Der Rechtswissenschaft ist aufgegeben, an Ordnungsmustern zu arbeiten, die die Generierung und den Transfer von Wissen ermöglichen und die Verarbeitung von Information und Wissen und die dafür erforderlichen kommunikativen Akte der Informationsverarbeitung in der und durch die Verwaltung erleichtern (informationsverarbeitendes Verwaltungshandeln). Zugleich muss sie die Weitergabe von Informationen, etwa ihren Einsatz als Steuerungsmittel, erfassen (informierendes Verwaltungshandeln), [sic] sowie die Regelungen verfeinern, die den Informationszugang der Bürger sichern."[64]

Indem das Informationsverwaltungsrecht auf die Wissensgenerierung und -verteilung von Akteuren Bezug nimmt, Kontexte beeinflusst, auf Relevanzen Einfluss nimmt, Rechte und Informationspflichten festlegt sowie die Reichweite des Daten- und Geheimnisschutzes mitbestimmt,[65] bietet es sich als Schlüssel für die Lösung des Wissensproblems bei der Gewährleistung der Internetsicherheit an. Es geht mithin um die Untersuchung des relevanten Teils des Informationsverwaltungsrechts des europäisch geprägten Rechts der Internetsicherheit hinsichtlich der Leitfrage, in welchem Umfang er die Lösung des Wissensproblems fördert und welche Potenziale einer gezielteren Anwendung oder Gestaltung zur Sicherheitsgewährleistung das Informationsverwaltungsrecht bietet.

II. Generierung, Transfer und Distribution von Wissen und sicherheitsrelevanten Informationen

Herauszuarbeiten ist also, ob und wie sicherheitsrelevante Informationen und Wissen generiert, transferiert und distribuiert werden können. Die zugrundliegenden sicherheitsspezifischen Relevanzkriterien lassen sich vorab am Informationsbedarf der Sicherheitsverwaltung und der Anwender skizzieren.[66]

Das Risikomanagement der zuständigen Behörden setzt zunächst voraus, dass Bedrohungslagen im Bereich der Netz- und Informationssicherheit von Internetinfrastrukturen erkannt werden.[67] Erforderlich ist also die Erhebung von Informationen über Probleme und Vorfälle, um überhaupt die Reaktions- und Abwehrbereitschaft bewerten zu können.[68] Darüber hinaus sind Wissen und Informationen erforderlich, um Sicherheitsprobleme und Schwachstellen zu er-

---

[64] *Hoffmann-Riem*, Eigenständigkeit der Verwaltung, in: ders./Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band I, 2. Aufl. 2012, § 10, Rn. 131.

[65] *Trute*, Wissen – Einleitende Bemerkung, in: Hans-Christian Röhl (Hrsg.), Wissen – Zur kognitiven Dimension des Rechts, Die Verwaltung, Beiheft 9, 2010, S. 11 (22).

[66] Siehe zu den informationsverwaltungsrechtlichen Funktionen von Generierung, Transfer und Distribution im Einzelnen § 3 A., § 4 A., § 5 A.

[67] Zu den Aufgaben der Informations- und Wissensakteure § 3 B.

[68] Vgl. Erwägungsgrund 23 ENISA VO 526/2013.

kennen und zu interpretieren. Die Sicherheitsprobleme müssen über ihr Erkennen hinaus analysiert und gelöst werden. Es müssen Ableitungen gefolgert, Folgewirkungen antizipiert, Pläne entworfen und am Ende Entscheidungen getroffen werden. Das Handeln und Treffen von Entscheidungen oder Prognosen auf Grundlage von Wissen setzt eine jeweils von den Eigenschaften des jeweiligen Gegenstands abhängige administrative Intelligenztechnik voraus, um Informationen zu komplexeren Wissensebenen zu verdichten. Dynamischer Wissensbedarf besteht demnach ferner über Technologien des Internets und seiner Applikationen, über Abwehr- und Schutztechnologien sowie über die Bedingungen der Resilienz der Netze und Informationssysteme. In kooperativen Ansätzen zur Sicherheitsgewährleistung ist der Informationsfluss zwischen den Akteuren von eminenter Bedeutung.

Anhand des rechtlichen Instruments der Meldepflicht lässt sich die sicherheitsspezifische Bedeutung der Generierung, des Transfers und der Distribution exemplifizieren. Bestimmte Unternehmen haben bei Vorliegen spezifischer Voraussetzungen IT-Sicherheitsvorfälle zu melden.[69] Die unmittelbaren Funktionen der Meldepflicht sind auf der Ebene der Erkennungs- (*awareness*) und Reaktionsfähigkeit (*incident response*) zu verorten.[70] Zum einen können sich die Behörden über die Meldeinformationen überhaupt erst ein Bild über die Sicherheitslage verschaffen.[71] Unter Sicherheitslage wird gemeinhin die Gesamtschau der Bedrohungen und der Einschränkungen der Sicherheit verstanden. Zum anderen soll der Inhalt der Meldung den Behörden die Möglichkeit geben, auf konkrete Sicherheitsvorfälle zu reagieren, indem sie Gegenmaßnahmen treffen und angemessene Prioritäten setzen (*risk mitigation*).[72] Im IT-Bereich ist die Sammlung von Informationen über Sicherheitsvorfälle über Meldepflichten und deren Auswertung eine wichtige Methode für die Identifikation von Schwachstellen. Informationen aus Meldungen sind mithin erforderlich, um Angriffsszenarien zu antizipieren. Ein wirklicher Mehrwert entsteht, wenn ausgehend von einem akkurateren Lagebild Planungen unmittelbar verbessert und Strategien entworfen und umgesetzt werden können. Erst im Bewusstsein von Schwachstellen und den Auswirkungen von Angriffen können Alternativpläne vorbereitet und das Handeln angepasst werden.[73] Die aus den Meldungen ge-

---

[69] Siehe § 3 D I. 2.

[70] Dazu *Feiler*, Information Security Law in the EU and the U.S., 2011, S. 490 mit Verweis auf die Federal Communications Commission (FCC) 57 Fed. Reg. 7, 883, 7, 884 vom 05.03. 1992; *Heinickel*/*Feiler*, CR 2014, 708 (710).

[71] *Lurz*/*Scheben*/*Dolle*, BB 2015, 2755 (2757).

[72] COM(2013) 48 final, S. 3; BT-Drs. 18/4096, S. 47.

[73] Vgl. *Gercke*, CR 2014, 344 (348) in Bezug auf Lagebilder im Rahmen des Red-Teaming-Ansatzes.

wonnenen Erkenntnisse können zudem bei der Erstellung der Sicherheitsanforderungen an die Unternehmen eingebracht werden (vgl. § 109 Abs. 6 TKG).[74] Die auf Grundlage der Meldungen ermittelten präventiven Schutzmaßnahmen und Erkenntnisse können außerdem anderen Behörden, Betreibern oder auch anderen Anwendern von IT rechtzeitig zur Verfügung gestellt werden (*information sharing*), damit sie sich rechtzeitig schützen können. Der Ansatz des frühzeitigen Erkennens von Cyberangriffen sowie der proaktive Umgang mit Bedrohungen unterscheiden sich dabei nicht wesentlich von den *intelligence*-getriebenen Methoden anderer Analysezentren oder privater Sicherheitsdienstleister.[75] Zuletzt kann mit gemeldeten Informationen der Zweck verfolgt werden, Transparenz herzustellen (*transparency*). Die Marktgegenseite kann über Sicherheitsrisiken informiert werden. Durch den so stattfindenden indirekten Risikotransfer können Nutzer und Anwender Entscheidungen auf besserer Informationsgrundlage treffen.[76] Das bei den Sicherheitsbehörden geschaffene entscheidungsrelevante Wissen kann demnach auch bei Herstellern, Nutzern, Anwendern, Betreibern und Anbietern sicherheitsbezogener Leistungen nutzbar gemacht werden.

III. Daten, Information, Wissen und Kommunikation

Die bereits eingeführten Begriffe Information und Wissen sind für die weitere Untersuchung zu klären und in Verhältnis zu den anderen Grundbegriffen Daten und Kommunikation zu setzen.

Der Begriff Information lässt sich nur schwer definieren.[77] Nach einer üblichen Einstiegsdefinition kann Information verstanden werden als ein Unterschied, der einen Unterschied macht (differenztheoretischer Informationsbe-

---

[74] Der Wortlaut der neuen Fassung der Norm hat eine normative Stärkung der Belange der Informationssicherheit und des Datenschutzes erfahren. Mit der Einbeziehung dieser Behörden („Einvernehmen" statt „Benehmen") werden die fachliche Expertise des BSI und des BfDI stärker eingebunden. Das Zustandekommen und der Inhalt sind demnach vom Einverständnis der Behörden abhängig, die jeweils die Expertise aus den Meldepflichten gewinnen.

[75] In den Vereinigten Staaten von Amerika ist die Einrichtung des sog. Cyber Threat Intelligence Integration Center (CTIIC) im Wege eines Presidential Memorandum – Establishment of the Cyber Threat Intelligence Integration Center vom 25.02.2015 vorgegeben worden. Für ein privates Sicherheitsunternehmen *Palantir*, Palantir Cyber – An End-to-End Cyber Intelligence Platform for Analysis & Knowledge Management, 2013, S. 3 f., online abrufbar.

[76] Dazu unter § 5 A. II.

[77] Vgl. *Hoeren*, Tractatus germanico-informaticus – Some Fragmentary Ideas on DRM and information law, in: Lodder/Meijboom/Osterbaan (Hrsg.), IT Law – The Global Future, 2006, S. 149 (155); vgl. DIN 44 300 (1988).

griff).[78] Gemeint ist damit, dass Informationen durch Selektivität und Selektionsleistungen gekennzeichnet sind.[79] Information ist kein Bestandteil der materiellen Welt. Damit eine Information existiert, muss es jemanden geben, der sie aufnehmen und verstehen kann.[80] Der Begriff der Information kann für die Zwecke dieser Arbeit funktional verwendet werden. Informationen können demnach als Wissen und kognitive Zustände beeinflussende Signale verstanden werden, die Handlungen und Entscheidungen beeinflussen können.[81]

Daten sind Zeichen oder Symbole, die einer Interpretation nicht zugänglich sind. Mit Datem sind also strikt formalisierte Werte gemeint, die in schematischen Abläufen beliebig reproduziert werden können. In Zahlen, Sprache, Text oder Bilder codiert, sind Daten vor allem von Maschinen (Computern) lesbar.[82] Sie lassen sich infolge ihrer Vergegenständlichung eigenständig speichern und erfassen.[83] Es ist gerade die Nichtinterpretierbarkeit von Daten, die den Unterschied zu Informationen markiert.[84] Häufig werden die Begriffe Information und Daten synonym verwendet.[85] Gesetzesbestimmungen wie die in Art. 4 Abs. 1 DS-GVO, nach dem „personenbezogene Daten" alle Informationen be-

---

[78] *Bateson*, Geist und Natur, 4. Aufl., 1995, S. 123. *Bateson* verdeutlicht diesen Informationsbegriff so: „Man kann einem Hund einen Tritt geben, dass der Hund wegfliegt, oder man kann ihm einen Tritt geben, dass er wegrennt. Im ersten Fall gibt man die Energie, die den Hund bewegt, im zweiten Fall leistet der Hund seine Bewegung selbst, das heisst, man hat ihm nur Information gegeben, die bewirkt, dass er seine eigene Energie verwendet. Im ersten Fall muss der Hund nichts verstehen, im zweiten Fall muss er verstehen, was ich meine. Er muss also nicht nur seine eigene Energie aufwenden, sondern auch noch interpretieren, wie er das tun soll."

[79] *Albers*, Rechtstheorie 33 (2002), 61 (68).

[80] Beispiel: Dass *Hamlet* als Information existiert, ist nicht an die Anzahl der materiellen Träger, also der gedruckten oder digitalen Texte gebunden. Vgl. *Lem*, Summa technologiae, 6. Aufl. 2003, S. 224.

[81] Ähnlich *von Bogdandy*, Die Informationsbeziehungen im europäischen Verwaltungsverbund, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band II, 2. Aufl. 2012, § 25 Rn. 3; für Informationsbegriffe, die nicht auf einen konkreten menschlichen Verstand angewiesen sind, siehe *Zech*, Information als Schutzgegenstand, 2012, S. 13 ff.

[82] *Vesting*, Die Bedeutung von Information und Kommunikation für die verwaltungsrechtliche Systembildung, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band II, 2. Aufl. 2012, § 20 Rn. 11.

[83] *Albers*, Umgang mit personenbezogenen Informationen und Daten, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band II, 2. Aufl. 2012, § 22 Rn. 11.

[84] Vgl. *Hoffmann-Riem*, Verwaltungsrecht in der Informationsgesellschaft – Einleitende Problemskizze, in: ders./Schmidt-Aßmann (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, 2000, S. 12; BVerfGE 65, 1 (49).

[85] Insofern irritiert auch die Begriffsbestimmung des § 2 Abs. 2 IFG mit der Formulierung „Daten oder sonstige Informationen".

zeichnen, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen, sind nicht Ausdruck einer reflektierten Regelungsentscheidung und spiegeln ein Verständnis aus Zeiten der Großrechenanlagen wider.[86]

Wissen kann als Bestand von Erkenntnissen begriffen werden. Den Begriff definierte bereits *Platon*, demzufolge Wissen eine wahre und begründete Überzeugung ist.[87] Hier kann aber vorliegend keine universal gültige Definition von Wissen in Anspruch genommen werden; vielmehr kommt es auf den zweckdienlichen Gebrauch der Bestimmung an. Wissen ist Faktor und Produkt eines (Erfahrungs-)Kontextes und führt über die Summe aller Informationen hinaus.[88] Wissen besteht auch in kognitiven Erwartungen, die Informationen den Überraschungseffekt nehmen. Wissen ist zudem relativ zeitbeständig und durch eine prinzipielle Lernfähigkeit und -bereitschaft geprägt bzw. Bedingung für dieselbe.[89] Wissen stellt mithin einen dynamischen Prozess dar, in dem durch Lernvorgänge neue oder revidierte Wissensbestände entstehen können.[90] Demzufolge ist Wissen als Bestand von Informationen zu verstehen, der eine organisierte oder systematisierte Form aufweist. Informationen gehen in Wissen über, sie werden zu Wissen „veredelt".[91] Schon jetzt sei angedeutet, dass der Erwerb von Wissen ein zentrales Ziel der mit Netz- und Informationssicherheit befassten Behörden und Agenturen ist.[92]

---

[86] *Albers*, Umgang mit personenbezogenen Informationen und Daten, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band II, 2. Aufl. 2012, § 22 Rn. 9.

[87] Diese Begriffsbestimmung geht auf den Dialog Theaitetos (Θεαίτητος) zurück, der Fragen der Erkenntnistheorie behandelt. Vgl. *Baumann*, Erkenntnistheorie, 3. Aufl. 2015, S. 33 ff.

[88] Vgl. *Spiecker gen. Döhmann*, Rewi 2010, 247 (253 f.).

[89] Vgl. *Luhmann*, Die Wissenschaft der Gesellschaft, 2005, S. 137 ff.; *Albers*, Die Komplexität verfassungsrechtlicher Vorgaben für das Wissen der Verwaltung, in: Collin/Spiecker gen. Döhmann (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, 2008, S. 50 (54 f.).

[90] *Willke*, Einführung in das systemische Wissensmanagement, 3. Aufl. 2011, S. 11.

[91] Vgl. *Wollenschläger*, Wissensgenerierung im Verfahren, 2009, S. 30; *Hoffmann-Riem*, Wissen als Risiko – Unwissen als Chance, in: Augsberg (Hrsg.), Ungewissheit als Chance, 2009, S. 17 (23).

[92] Nach Art. 2 Abs. 1 VO (EU) Nr. 526/2013 entwickelt und pflegt die ENISA „ein hohes Niveau an Sachkenntnis". Ihre Aufgabe ist nach Art. 3 Abs. 1 b) i) der Aufbau von Fähigkeiten in diesem Bereich, indem sie „das erforderliche Wissen zur Verfügung stellt […]". Zur Aufgabe des BSI gehört es nach § 3 Abs. 1 Nr. 2 BSIG, Informationen zu sammeln und auszuwerten, die die „gewonnenen Erkenntnisse" bereitstellen. Für die Bundesnetzagentur drückt sich der Wissensbedarf in § 125 TKG aus, der statuiert, dass die Behörde zur Vorbereitung ihrer Entscheidung oder zur Begutachtung von Fragen wissenschaftliche Kommissionen einsetzen kann, deren Mitglieder über besondere „Erfahrungen und über ausgewiesene wissenschaftliche Kenntnisse verfügen" müssen.

Kommunikation als gemeinschaftsbezogenes (*com-municatio*) Verständigungshandeln bezeichnet im verwaltungsrechtlichen Kontext einen Transfer selegierter Informationen. Gelungene Kommunikation setzt das Verständnis des Empfängers der vom Sender mitgeteilten Information voraus.[93] Da Verwaltung rechts- und folglich sprachgebunden ist, kann sie von vorneherein als Kommunikationssystem verstanden werden, sodass jede verwaltungsbezogene Handlung, d. h. auch die Rezeption und Produktion von Recht, immer eine solche der Verarbeitung von Information und Wissen ist.[94]

[93] *Vesting*, Die Bedeutung von Information und Kommunikation für die verwaltungsrechtliche Systembildung, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band II, 2. Aufl. 2012, § 20 Rn. 30.

[94] So *Vesting*, Die Bedeutung von Information und Kommunikation für die verwaltungsrechtliche Systembildung, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band II, 2. Aufl. 2012, § 20 Rn. 30 mit Verweis auf *Luhmann*, Organisation und Entscheidung, 2000, S. 57.

§ 3 Generierung von Informationen über die Netz- und Informationssicherheit

Die Generierung von Informationen über die Sicherheit von Netzen und Informationssystemen dient der Erfüllung verfassungsrechtlicher Pflichten zur Produktion sicherheitsrelevanter Informationen (A.). Wahrgenommen werden diese Pflichten durch administrative Wissensakteure auf europäischer und deutscher Ebene, zu denen nicht nur die Sicherheitsbehörden zu zählen sind, sondern auch Datenschutzbehörden und Computer-Notfallteams (B). Die Quellen für die Generierung von Informationen im Bereich der Informationstechnik und Telekommunikation ergeben sich aus dem die Netz- und Informationssicherheit betreffenden Unionsrecht und den entsprechenden Einordnungen im nationalen Recht. Diese Quellen sind insbesondere Betreiber kritischer Infrastrukturen, Telekommunikationsnetzbetreiber und -diensteanbieter, Digitale Dienste und Telemedien sowie Verantwortliche im Sinne des Datenschutzrechts (C.). Die Unternehmen haben Informationen entweder von sich aus beizubringen oder sie werden über Informationsbefugnisse erhoben. Die Übernahme verwaltungsexternen Wissens im Wege der Kooperation mit Privaten ist ein wichtiges Instrument der staatlichen Wissensgenerierung (D.). Grenzen der Informations- und damit Wissensgenerierung folgen aus dem Datenschutz (E.) und dem Schutz unternehmensbezogener Daten (F.).

A. Funktion der Informationsgenerierung für die Sicherheitsgewährleistung

Die Netz- und Informationssicherheit stellt keine exklusive Staatsaufgabe dar. Ein staatliches Monopol für Internetinfrastrukturen ist rechtlich nicht verankert. Vornehmlich tragen Private zur Gewährleistung der Internetsicherheit bei. Verfassungsrechtliche Pflichten zur Informationsgenerierung durch den Staat und die Europäische Union zur Sicherheitsgewährleistung folgen jedoch aus Schutzpflichten zur Informationsgewinnung (I.) und aus der Gewährleistungsverantwortung für Internetinfrastrukturen (II.).

I. Schutzpflicht zur Informationsgewinnung

Mit der Konstitutionalisierung der Rechtsordnung sind aus den Grundrechten zur ursprünglichen subjektiv-rechtlichen Abwehrfunktion weitere Dimensionen hinzugekommen. Neben der Ausstrahlungswirkung, den Organisationsprinzipien, Leistungsansprüchen in Privatrechtsverhältnissen, Teilhaberechten und Verfahrensgarantien werden den Grundrechten auch Schutzpflichten entnommen. Grundrechtliche Schutzpflichten zielen auf den Schutz vor Privaten. Die Grundrechte entfalten in mehrpoligen Konstellationen eine Horizontalwirkung. Grundrechte sind nach der Rechtsprechung des Bundesverfassungsgerichts nicht nur Abwehrrechte, sondern auch objektive Prinzipien, die den staatlichen Organen gebieten, sich schützend vor die grundrechtlichen Schutzgüter zu stellen.[1] Je gewichtiger der Schutzgegenstand, desto leichter fällt die Herleitung von Schutzpflichten.

Im Unionsrecht hat der Europäische Gerichtshof Schutzpflichten für die Grundrechte bislang nicht anerkannt. Das Konzept der Schutzpflichten ist dem Gericht aber nicht fremd, da Art. 52 Abs. 3 GRCh den Gerichtshof dazu verpflichtet, zur Auslegung der Grundrechte die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte zu den entsprechenden EMRK-Grundrechten heranzuziehen. Ein Herleitungs- und Rechtsquellenproblem zur Begründung von unionrechtlichen Grundrechten besteht daher grundsätzlich nicht.[2]

Für den Bereich des Internets ergibt sich eine mehrpolige Grundrechtskonstellation. Die Betreiber von Internetinfrastrukturen und -diensten sind überwiegend Private, die durch ihre Tätigkeit direkten oder indirekten Einfluss auf die Grundrechte Dritter nehmen. Der Staat hat im Ergebnis die grundrechtlichen Interessen sowohl der Nutzer als auch der Betreiber zu schützen. Aktiviert wird diese Schutzpflicht jedoch erst, wenn eine Gefährdungslage besteht, aus der Handlungspflichten abgeleitet werden können. Gefährdungen bestehen für verschiedene Grundrechte, welche sich in ihrer digitalen Dimension online realisieren.[3] Zunehmend wird das Internet als größeres Ganzes verstanden, wodurch es als solches zum Schutzgegenstand aufgewertet wird. Das Bundesverfassungsgericht hat anerkannt, dass zum Gehalt des Grundrechts auf Gewährleistung des menschenwürdigen Existenzminimums gehört, die Nutzung von Informations- und Kommunikationstechnologien zu ermöglichen. Das Sozialstaatsgebot halte den Gesetzgeber an, die soziale Wirklichkeit zeit- und realitätsgerecht zu erfassen.[4] Auf einer Linie mit der bisherigen Rechtsprechung des

---

[1] BVerfGE 39, 1 (42); BVerfGE 85, 191 (212).

[2] Dazu *Leuschner*, EuR 2016, 431 (445).

[3] *Luch/Schulz*, MMR 2013, 88 (88).

[4] BVerfGE 125, 175 (222 ff.).

Bundesgerichtshofs zum Nutzungsausfallschaden, nach der eine Entschädigung nur gefordert werden kann, wenn es sich bei einem entzogenen Gegenstand um ein „Wirtschaftsgut von zentraler Bedeutung für die eigene Lebensführung" handelt, erkannte das Gericht die „zentrale Bedeutung" des Internets an und erweiterte die Kategorie des normativen Schadens dahin gehend, dass in der fehlenden Nutzungsmöglichkeit eines Internetanschlusses ein konkreter Vermögensschaden gesehen werden kann.[5]

Doch eine Schutzpflicht kann erst dann greifen, wenn Gefahren erkannt werden. Da ein Großteil der Internetinfrastrukturen von Privaten betrieben wird, ist für die öffentlichen Stellen eine Gefährdungslage nicht ohne Weiteres erkennbar. Die Aktivierung einer etwaigig bestehenden Schutzpflicht setzt also voraus, dass die epistemische Lücke geschlossen und dem Mangel an Eigeninformationen abgeholfen wird.[6] Insoweit folgt aus der Schutzpflicht, dass eine Informationsbasis aufzubauen ist, die es erlaubt, sie auch wahrnehmen zu können. Dieses Gebot der Risikovorsorge ist den Schutzpflichten insbesondere im Bereich der Technik und der damit verbundenen Gefahren und Risiken entnommen worden.[7] Der Begriff Vorsorge meint die zeitliche Vorverlegung hoheitlichen Handelns, bei der „der Staat sein eigenes Unwissen reflektiert und sich und/oder Private dazu verpflichtet, die eigenen Mittel der Wissensgewinnung permanent zu aktualisieren".[8]

Eine andere Frage ist, wie die aus der Schutzpflicht abgeleitete Risikovorsorge erfüllt werden kann. Es besteht ein Kontinuum mit denkbaren Handlungsformen und Kriterien. In Bezug auf eine unsichere Informationsbasis reicht dieses von der bloßen Schaffung eines rechtlichen Rahmens für die freiwillige Informationsweitergabe bis hin zu klassischen finalen Informationsbefugnissen.[9] Der Ableitung konkreter Handlungspflichten ist indes Sache des Gesetzgebers, dem die Einschätzungs-, Beurteilungs- und Gestaltungsprärogative zusteht und dem ein Prognosespielraum zukommt.[10] Die Lehre vom Vorbehalt des Gesetzes gilt auch für die Erfüllung grundrechtlicher Schutzpflichten.[11] Für die Verwaltung bedarf es daher auf der Anwendungsebene einer gesetzlichen Grundlage

---

[5] BGHZ 196, 101.

[6] *Möllers/Pflug*, Verfassungsrechtliche Rahmenbedingungen des Schutzes kritischer IT-Infrastrukturen, in: Kloepfer (Hrsg.), Schutz kritischer Infrastrukturen, 2010, S. 47 (59).

[7] *Kugelmann*, Polizei- und Ordnungsrecht, 2. Aufl. 2012, S. 31 Rn. 33: „Risikovorsorge kann durch grundrechtliche Schutzpflichten geboten sein." Kritisch *Lepsius*, Risikosteuerung im Verwaltungsrecht, in: VVDStRL 63 (2004), S. 264 (301 ff.).

[8] *Möllers*, Der vermisste Leviathan, 2008, S. 85.

[9] Im Zusammenhang mit dem Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme *Hoffmann-Riem*, JZ 2008, 1009 (1011).

[10] Dazu BVerfGE 53, 257 (293).

[11] *Wahl*/*Masing*, JZ 1990, 553 (555).

für die Informationsbefugnisse, zumal sich eine Ausübung solcher Befugnisse für die Betreiber von Infrastrukturen als Grundrechtseingriff auswirkt.[12]

Zu bedenken ist, dass ein Mehr an Informationen nicht nur zu Sicherheitsgewinnen führt, sondern auch neue Gefährdungslagen mit sich bringt, da zum Schutz von Grundrechten wiederum die Grundrechte Dritter beschränkt werden. Festzuhalten ist aber, dass für eine das Untermaßverbot beachtenden Anwendung dieser Schutzpflichtenkonzeption zumindest ein rechtlicher Rahmen gefordert werden kann, der dem grundrechtsverpflichteten Staat ein Instrumentarium zur Wissensgenerierung bereitstellt. Da der Staat mit seinen Gewalten als Akteursmehrheit begriffen werden muss,[13] hat dieser Rechtsrahmen eine jeweils unterschiedliche Aufgabe zu erfüllen. Der Gesetzgebung müssen Informationen zur Verfügung gestellt werden, die sie benötigt, um ihrer Pflicht zur Beobachtung der tatsächlichen Verhältnisse nachzukommen.[14] Die Informationsbasis bildet die Voraussetzung dafür, Schutzpflichten wahrnehmen zu können. Die juristischen Entscheidungen im Bereich der Exekutive und Administrative sind informationsverarbeitende Prozesse und ebenso auf eine Informationsbasis angewiesen, um Sachverhalte akkurat zu erfassen und ihrer Pflicht zu fehlerfreien Ermessensentscheidungen zu entsprechen.

II. Gewährleistungsverantwortung

Auf hoher Abstraktionsstufe angesiedelt ist die Idee und Konzeption der Gewährleistungsverantwortung, die beschreibt, dass der Staat bzw. eine Rechtsgemeinschaft wie die Europäische Union nach der Öffnung zur pluralen Verwirklichung der Daseinsvorsorge ein „besonders verpflichteter Akteur" bleibe.[15] Dabei handelt es sich um eine Deutungsfolie für weitere, teleologische Wertungen aus der staatstheoretischen Diskussion, in der Staatlichkeit vor dem Hintergrund verschiedener „Paradigmen von Regulierung" verhandelt wird. Zwei zentrale Ansätze sind hier im Rahmen der Privatisierungsdebatte die Privatisierungsfolgenverantwortung und in Fortsetzung sozialstaatlicher Konzeption die Idee der Vorsorge.[16] Nach der Privatisierung setzte sich die Erkenntnis durch,

[12] *Sonntag*, IT-Sicherheit kritischer Infrastrukturen, 2002, S. 115.

[13] *Spiecker gen. Döhmann*, Rechtswissenschaft 2010, 247 (264, Fn. 77); zu den einzelnen verwaltungsrechtlichen Informationsgewinnungsakteuren *Groß*, Ressortforschung, Agenturen und Beiräte – zur notwendigen Pluralität der staatlichen Wissensinfrastruktur, in: Röhl (Hrsg.), Wissen – Zur kognitiven Dimension des Rechts, Die Verwaltung, Beiheft 9, 2010, S. 135 (138 ff.).

[14] Zum Beispiel BVerfGE 88, 203 (263); *Trute*, Wissenschaft und Technik, in: Isensee/Kirchhof (Hrsg.), HbStR, Band IV, 3. Aufl. 2006, § 88 Rn. 38.

[15] *Franzius*, Gewährleistung im Recht, 2009, S. 121.

[16] *Möllers*, Der vermisste Leviathan, 2008, S. 81 ff. (82).

dass dem Staat eine Rückfallposition zukommen muss, wenn der durch die Liberalisierung geschaffene Markt seiner Aufgabe nicht gerecht wird. Das Regulierungsverwaltungsrecht und der Wettbewerb stünden nicht in einem Widerspruch, sondern in einem Verhältnis der Ermöglichung.[17]

1. Europäische Dimension

Sowohl die europarechtlichen Privatisierungs- und Liberalisierungsverpflichtungen als auch die bestehenden Regulierungen[18] machen deutlich, dass die europäischen Verträge keinen (interventionistischen) Wohlfahrtsstaat bilden. Gleichwohl ist der Union die Daseinsvorsorge nicht fremd. Nur die Realisierung erfolgt in Ermangelung von Benennungen im EUV und AEUV zu Fragen der Netz- und Informationsinfrastruktur durch eine Fülle sekundärrechtlicher Vorgaben, die dann aber immer eher als konkrete politische Einigungen und Kompromisse zu verstehen sind denn als funktional verfassungsrechtliche Strukturvorgaben mit dem Ziel, die endogenen gesellschaftlichen Potenziale für die Verfolgung öffentlicher Zwecke nutzbar zu machen.[19]

Dass das Gemeinwohl nicht nur eine ridiküle Schimäre, sondern auch ein dogmatischer Rechtsbegriff und ein Tatbestandsmerkmal in der europäischen Rechtsordnung ist, beweist Art. 52 Abs. 1 S. 2 GRCh. Grundrechtseinschränkungen dürfen nur vorgenommen werden, wenn sie „dem Gemeinwohl dienenden Zielsetzungen […] entsprechen".[20] Eine positivrechtliche Anerkennung eines Unionsgemeinwohls als Zweck findet sich in Art. 17 Abs. 1 S. 1 EUV. Die Kommission ist Förderin und Hüterin der „allgemeinen Interessen der Union und ergreift Initiativen zu diesem Zweck". In wirtschaftlicher Hinsicht erkennt das Unionsrecht in Art. 106 Abs. 2 AEUV Grenzen der Anwendung der Verträge für Unternehmen an, die mit „Dienstleistungen von allgemeinem wirtschaftlichem Interesse" betraut sind.[21] Im Beihilferecht wird ebenfalls die Vorstellung eines höheren Unionsinteresses deutlich. Art. 107 Abs. 3 lit. b und c AEUV ma-

---

[17] *Möllers*, Der vermisste Leviathan, 2008, S. 83.

[18] *Fehling*, AöR 121 (1996), 60 (66).

[19] Vgl. zu diesem Gedanken *Voßkuhle*, Beteiligung Privater an der Erfüllung öffentlicher Aufgaben und staatliche Verantwortung, in: VVDStRL 62 (2003), S. 266 (307).

[20] In der französischen und englischen Sprachfassung „des objectifs d'intérêt général reconnues par l'Union" bzw. „objectives of general interest recognised by the Union". Vgl. auch Art. 17 Abs. 1 S. 2 GRCh, wonach Enteignungen nur „aus Gründen des öffentlichen Interesses" erfolgen dürfen. Zu den „zwingenden Gründen des Gemeinwohls" als ungeschriebenem Rechtfertigungsgrund im Rahmen der Grundfreiheiten EuGH, Rs. 120/78, Rn. 8 – Cassis de Dijon.

[21] Die Kommission definiert die Dienstleistungen als marktbezogene Tätigkeiten, „die im Interesse der Allgemeinheit erbracht und daher von den Mitgliedstaaten mit besonderen Gemeinwohlverpflichtungen verbunden werden". Siehe Mitteilung der Kommission zu den

chen Ausnahmen vom Beihilfeverbot zur Förderung des „gemeinsamen europäische[n] Interesses". Dem Gemeinwohl ist nach Art. 309 AEUV schließlich auch die Europäische Investitionsbank verpflichtet.[22] Art. 14 AEUV lässt sich entnehmen, dass der Union und den Mitgliedstaaten eine geteilte Verantwortung für die im Europarecht so genannten Dienste von allgemeinem wirtschaftlichem Interesse zugewiesen ist.[23] Somit können den europäischen Instrumenten der (Gewährleistungs-)Verantwortung die allgemeinen Wettbewerbsregeln und die auf den Kompetenzgrundlagen ergangenen sekundärrechtlichen Maßnahmen zur Liberalisierung, Regulierung und Harmonisierung zugeordnet werden. Das Protokoll Nr. 26 zählt die „Sicherheit" dieser Dienste ausdrücklich zu den gemeinsamen Werten der Union.[24]

Auf der europäischen Grundrechtsebene geht eine gewisse Ausstrahlung von Art. 36 GRCh aus, der den Zugang zu Dienstleistungen von allgemeinem wirtschaftlichem Interesse anerkennt und achtet. Aus dem allgemeinen Recht auf „gute Verwaltung", der sich auch aus Art. 41 GRCh ergibt, wird eine weitere unionsrechtlich normierte Verankerung der „kognitiven Grundlagen des Staatshandelns" abgeleitet.[25]

Auf sekundärrechtlicher Ebene im Bereich der Telekommunikation wie der Netz- und Informationssicherheit werden die verfolgten öffentlichen Interessen zum Teil reflektiert.

Die telekommunikationsrechtliche Rahmen-RL 2002/21/EG, die allgemeine materiell-rechtliche und prozedurale Bestimmungen enthält, setzt voraus, dass durch die Vorgaben öffentliche Interessen verfolgt werden, indem eine Telekommunikationsordnung erschaffen wird, die eine flächendeckende Versorgung sicherstellt.[26] Als politisches Ziel und regulatorischen Grundsatz in Art. 8 Abs. 4 lit. f Rahmen-RL fördern die nationalen Regulierungsbehörden die Interessen der Unionsbürger, indem sie sicherstellen, dass die Integrität und Sicherheit der öffentlichen Kommunikationsnetze gewährleistet sind. Neben dem Telekommunikationsrecht steht die NIS-RL als Ganze für eine dem europäischen Inter-

---

Leistungen der Daseinsvorsorge in Europa („Daseinsvorsorgemitteilung"), ABl. EU 2001 C 17/4, Rn. 14.

[22] *Jardet*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Europäisches Unionsrecht, Band 4, 7. Aufl. 2015, AEUV, Art. 309, Rn. 4.

[23] *Franzius*, Gewährleistung im Recht, 2009, S. 549; *Dörr*, Die Anforderungen an ein zukunftsfähiges Infrastrukturrecht, in: VVDStRL 73 (2013), S. 323 (335 f.); vgl. BVerfGE 123, 267 (294).

[24] Vgl. Art. 1 und 2 des „Protokolls (Nr. 26) über Dienste von allgemeinem Interesse", ABl. EU 2012 C 326/308.

[25] *Augsberg*, Informationsverwaltungsrecht, 2014, S. 42 (Fn. 12).

[26] *Kühling*, Europäisches Telekommunikationsverwaltungsrecht, in: Terhechte (Hrsg.), Verwaltungsrecht der Europäischen Union, 2011, § 24 Rn. 28, 70.

esse dienende Wissensgenerierung. Die durch sie geschaffenen Informationskooperationsstrukturen dienen der Erkennungs- und Reaktionsfähigkeit hinsichtlich der Gefahren für die Netz- und Informationssicherheit auf EU-Ebene.[27]

Damit lässt sich festhalten, dass im Europarecht die Verantwortung für hochrangige, allgemeine Interessen als solche anerkannt ist, die Gewährleistung indes nur schwach durch originäre, primärrechtliche Leistungspflichten determiniert wird. Die Sicherheit der Netz- und Informationsinfrastruktur ist als Bedingung der Möglichkeit der Unionspolitiken vorausgesetzt und die Verantwortung dafür wird durch das Sekundärrecht der Internetsicherheit ausgeformt.[28]

2. Grundgesetz

Dem Grundgesetz lassen sich im Vergleich zum Unionsrecht konkretere, an den Staat gerichtete Aufträge zur Gewährleistung der Internetsicherheit entnehmen. Informationspflichten für den Staat ergeben sich zum einen daraus, dass wesentliche Internetinfrastruktur ein grundrechtliches Schutzgut sind (a), und zum anderen aus der in Art. 87f GG zum Ausdruck kommenden Gewährleistungsverantwortung für Telekommunikationsdienstleistungen (b).

a) Internetinfrastruktur als grundrechtliches Schutzgut

Das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Das Bundesverfassungsgericht hat dieses Grundrecht als besondere Ausprägung des allgemeinen Persönlichkeitsrechts erkannt.[29] „Insbesondere das Internet als komplexer Verbund von Rechnernetzen“ und „komplexe informationstechnische Systeme“ begründeten für den Einzelnen neben neuen Möglichkeiten neue Gefährdungen.[30] Die Gesamtbetrachtung der Entscheidung des Bundesverfassungsgerichts ergibt, dass das Grundrecht primär den Einzelnen vor dem staatlichen Zugriff auf Systeme wie Personalcomputer schützt.[31] Eine technische Vernetzung setzt der grund-

---

[27] Vgl. zum Bedarf Mitteilung der Kommission zum Schutz kritischer Informationsinfrastrukturen (CIIP) v. März 2011, KOM(2010), 245 und Schlussfolgerungen des Rates vom 31.05.2010 zur Mitteilung „Eine digitale Agenda für Europa“ (101310/10).

[28] Vgl. auch Kommission, Wachstum, Wettbewerbsfähigkeit, Beschäftigung – Herausforderungen der Gegenwart und Wege ins 21. Jahrhundert – Weißbuch (1993), KOM(93) 700, Dezember 1993, S. 82, die eine transeuropäische Telekommunikation als konstitutive Voraussetzung für einen gemeinsamen Informationsraum ansieht.

[29] BVerfGE 120, 274 (303); zur Kritik an der Konzeption dieses Grundrechts *Hornung*, CR 2008, 299 (301 f.).

[30] BVerfGE 120, 274 (304).

[31] Vgl. BVerfGE 120, 274 (314).

rechtliche Schutz der Integrität und Vertraulichkeit informationstechnischer Systeme nicht voraus.[32] Anders als der Name des Grundrechts vermuten lässt, der immerhin mit der Integrität und Vertraulichkeit zwei der Schutzziele der Netz- und Informationssicherheit beinhaltet, kann aus ihm keine normative Aussage darüber abgeleitet werden, ob über die abwehrrechtliche Schutzdimension hinaus aus der Gewährleistung auch eine grundrechtliche Schutzpflicht für Internetinfrastrukturen folgt und eine Pflicht besteht, über die Sicherheitslage staatlicherseits Informationen zu erheben.

Das Internet als zusammenhängende, vernetzte Infrastruktur erscheint als Ganzes zu wenig konturiert, als dass es als ein einen normativen Zweck erfüllendes Schutzgut bezeichnet werden könnte. Gefragt ist also nach einem normativ greifbaren Verständnis von Infrastruktur.

Nach einer funktionalen Definition kann eine Infrastruktur verstanden werden als „Gesamtheit aller Mittel […], die der Überwindung von Entfernungen dienen und dadurch die Integration eines Raumes bewirken. Aus ihrer Basisfunktion für die Herstellung sozialer, wirtschaftlicher und politischer Einheit folgt, dass sie notwendig darauf angelegt ist, allen Interessierten zugänglich und deshalb flächendeckend ausgelegt zu sein. Dies erfordert regelmäßig vernetzte Strukturen, ohne die raumüberwindenden Vorgänge von verschiedenen Punkten zu einer Mehrzahl anderer Punkte nicht denkbar sind“.[33] Für das Internet kann diese Definition zumindest insofern herangezogen werden, als sie sich auf netzgebundene und nicht auf stationäre Infrastrukturen bezieht. Das Bundesverfassungsgericht hat in der betreffenden Entscheidung solche Infrastrukturen als grundrechtliches Schutzgut anerkannt, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen gefährdet, zu denen auch die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen gehöre.[34] Daraus ergibt sich das Erfordernis spezifischer Relevanzkriterien, die vernetzte oder vernetzende Infrastrukturen erfüllen müssen, um als grundrechtliches Schutzgut in Betracht zu kommen, welches verfassungsrechtliche Pflichten zur Wissensgewinnung aktiviert.

Wenn die dem Internet zugrundliegende Kommunikations- und Informationstechnologie nicht pauschal als „wesentlich“ eingestuft werden soll, bedarf es einer Prüfung, die diejenigen Bestandteile von informationstechnischen Infrastrukturen als „kritisch“ und damit als schutzbedürftig ermittelt, die für andere, gesellschaftlich relevante Infrastrukturen, die auf die Vernetzung mit dem Internet angewiesen sind, zwingend erforderlich sind.[35]

---

[32] BVerfGE 120, 274 (314).

[33] *Hermes*, Staatliche Infrastrukturverantwortung, 1998, S. 329.

[34] BVerfGE 120, 274 (328).

[35] Vgl. *Feiler*, Information Security Law in the EU and the U.S., 2011, S. 28; *Sonntag*,

Ermitteln lässt sich die Kritikalität einer IT-Infrastruktur mit einer „dreifachen Relevanzprüfung".[36] Erstens muss die Informations- und Telekommunikationstechnologie zu einem Infrastrukturbereich gehören, der selbst als „kritisch" einzustufen ist und einem betreffenden Sektor angehört, zweitens muss die Technologie systemrelevante Teile dieser Infrastruktur betreffen und drittens muss der fragliche Teil des Systems als kritisch klassifiziert werden können.

Mit der Novellierung des BSIG durch das IT-Sicherheitsgesetz wurde auf einfachgesetzlicher Ebene der Begriff der kritischen Infrastrukturen erstmals durch eine Legaldefinition verrechtlicht. Eine Verordnung auf Grundlage des Gesetzes bestimmt erstmals, welche Dienstleistungen in den vom Gesetz benannten Sektoren, denen die Infrastrukturen zuzuordnen sind, wegen ihrer Bedeutung kritisch sind und welche für die Erbringung der Dienstleistungen erforderlichen Anlagen wegen ihres als bedeutend anzusehenden Versorgungsgrades aus gesamtgesellschaftlicher Sicht als kritische Infrastrukturen gelten.[37]

Mit der Bestimmung kritischer Internetinfrastrukturen wie Internet Exchange Points, Domain-Name-System-Diensteanbieter und Transport-Layer-Security-Name-Registries in der Verordnung sind konkrete Infrastrukturelemente benannt, aus deren Bedeutung für das Funktionieren des Gemeinwesens die öffentliche Aufgabe erwächst, die Sicherheit dieser Elemente zu gewährleisten. Die Informationserhebung ist die notwendige Voraussetzung zur Sicherheitsgewährleistung.

b) Gewährleistungsverantwortung aus Art. 87f GG

Art. 87f GG gibt dem Bund auf, im Bereich der Telekommunikation flächendeckend angemessene und ausreichende Dienstleistungen zu gewährleisten. Der Artikel manifestiert verfassungsrechtlich die Reduzierung der ursprünglichen Erfüllungsverantwortung auf eine gewährleistende Garantie- und Regulierungsfunktion des Staates und ist, auch mit Blick auf Art. 14 AEUV, somit Ausdruck der Gewährleistungsverantwortung des Bundes.[38] Den Abs. 1 und 2 des Art. 87f GG liegt der Grundsatz der Trennung von privatwirtschaftlich erbrachten Dienstleistungen und der vom Bund wahrzunehmenden Hoheitsaufgaben zugrunde. Dem Bund ist es durch das verfassungsrechtliche Gebot der Privati-

---

IT-Sicherheit kritischer Infrastrukturen, 2005, S. 29 ff.; *Möllers*/*Pflug*, Verfassungsrechtliche Rahmenbedingungen des Schutzes kritischer IT-Infrastrukturen, in: Kloepfer (Hrsg.), Schutz kritischer Infrastrukturen, S. 47 (51).

[36] *Schulz*/*Tischer*, ZG 2013, 339 (351).

[37] Siehe § 3 C. II. 2.

[38] *Dörr*, Die Anforderungen an ein zukunftsfähiges Infrastrukturrecht, in: VVDStRL 73 (2013), S. 323 (337 ff.); *Freund*, NVwZ 2003, 408 (409); grundlegend *Eifert*, Grundversorgung mit Telekommunikationsleistungen im Gewährleistungsstaat, 1998, S. 18 ff.

sierung des Art. 87f Abs. 2 S. 1 GG versagt, Telekommunikationsdienstleistungen selbst zu erbringen. Mit der Zuordnung der Verwaltungskompetenz zum Bund geht ein Privatisierungsverbot für den Kernbereich der Hoheitsaufgaben einher.[39] Die Hoheitsaufgaben im Bereich der Telekommunikation werden gem. Art. 87f Abs. 2 S. 2 GG in bundeseigener Verwaltung durchgeführt.

Unter Telekommunikation kann in Fortentwicklung des Begriffs des Fernmeldewesens die körperlose Übermittlung von Informationen jeden Inhalts in der Weise verstanden werden, dass sie am Empfangsort wiedererzeugt werden.[40] Nach Sinn und Zweck der Vorschrift sind auch die Errichtung des Telekommunikationsnetzes und die Bereitstellung von Endgeräten erfasst.[41] Der Kompetenztitel des Art. 73 Abs. 1 Nr. 7 Alt. 2 GG umfasst die „Regelung der technischen Seite der Errichtung einer Telekommunikationsinfrastruktur und der Informationsübermittlung mit Hilfe von Telekommunikationsanlagen"; *ex negativo* nicht erfasst sind hingegen „Regelungen, die auf die übermittelten Inhalte oder die Art der Nutzung der Telekommunikation gerichtet sind".[42]

Ein unmittelbarer sicherheitsspezifischer Regelungsgehalt lässt sich dem Wortlaut von Art. 87f GG nicht entnehmen. Bei Entstehung der Norm hatte der Gesetzgeber in erster Linie das Risiko vor Augen, Telekommunikationsunternehmen könnten aus ökonomischen Gründen insbesondere strukturschwache Gebiete nicht mit Telekommunikation zu angemessenen Preisen versorgen. Nicht ausgeschlossen ist es aber, auch weitere Gesichtspunkte hinsichtlich der Frage angemessener Dienstleistungen zu berücksichtigen. So können auch der Schutz und die IT-Sicherheit von Infrastrukturen zur Infrastrukturgewährleistungspflicht gezählt werden. Zu einer angemessenen Telekommunikationsversorgung gehört auch der Schutz vor der Beeinträchtigung der Kommunikation.[43] Die angemessene Absicherung der kritischen, also systemrelevanten Elemente der Infrastruktur ist erforderlich, da sonst die staatliche Verantwortung nur rudimentär erfüllt wäre. IT-Sicherheit ist insofern Element des Grundversorgungsauftrags und der (E-)Daseinsvorsorge.[44]

Da verfassungsrechtlich eine Eigenerbringung ausgeschlossen ist, kann die Gewährleistungsverantwortung durchaus auch Formen der Erfüllungsverant-

---

[39] *Gröpl*, in: Gröpl/Windhorst/von Coelln (Hrsg.), Studienkommentar GG, 2. Aufl. 2015, Art. 87f, Rn. 7.

[40] BVerfGE 46, S. 120 (143).

[41] BT-Drs. 12/7269, S. 5; *Sommer*, Staatliche Gewährleistung im Verkehrs-, Post und Telekommunikationsbereich, 2000, S. 93.

[42] BVerfGE 125, 260 (314).

[43] *Hoffmann-Riem*, Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses, 2014, S. 17.

[44] *König/Popescu-Zeletin/Schliesky* (Hrsg.), IT und Internet als kritische Infrastruktur, 2014, S. 23.

wortung einschließen, sodass private Betreiber und Anbieter legitim zu Sicherheitsmaßnahmen verpflichtet werden können.[45] Der gebundene Gesetzgeber und die gebundene Exekutive haben für die Bestimmung des Sicherheitsniveaus eine beträchtliche Einschätzungsprärogative.[46] Durch die alleinige Berechtigung der Privaten für die Erbringung der Leistung nach eigener Handlungslogik verbleibt der öffentlichen Hand jedoch ein dauerhafter Steuerungs- und Sicherungsauftrag, der sich zumindest darauf verdichtet, einen Rahmen organisatorisch-institutioneller Art bereitzustellen, um zum einen eine kontinuierliche Beobachtung zu gewährleisten und zum anderen die Fähigkeit sicherzustellen, bei Fehlentwicklungen gesetzlich korrigierend einzugreifen.[47]

Als einfachgesetzlicher Steuerungsimpuls ist § 2 TKG anzusehen, der das in § 1 TKG angelegte Programm auffächert und die Art und Weise der Zielerreichung der telekommunikationsrechtlichen Regulierung vorgibt. Ziel der Regulierung ist gemäß § 2 Abs. 2 Nr. 9 TKG die Wahrung der Interessen der öffentlichen Sicherheit. Dass die Sicherheit als Regulierungsziel aufgelistet ist, wird zwar zum Teil als „systematisch verfehlt" angesehen.[48] Mit Blick auf das Gebot, die Regulierung als hoheitliche Aufgabe wahrzunehmen, und vor dem Hintergrund der vom Telekommunikationsbereich ausgehenden und denselben bedrohenden Gefahren und Risiken ist es aber nur folgerichtig, die Sicherheit als Regulierungsziel anzusehen und regulatorisch zu gewährleisten.[49]

Damit stellt sich die Frage, ob die öffentliche Verantwortung für Netz- und Informationssicherheit auch die von den Infrastrukturnetzen zu trennenden transportierten Dienste umfasst. Dies betrifft die Trennung des Telekommunikations- vom Telemedienrecht.[50] Da der Begriff der Telekommunikation in Art. 87f GG weiter gefasst ist als der dem TKG zugrundeliegende, könnte die These lauten, dass sich die Verantwortung insoweit auf die für Telemedienangebote in Anspruch genommenen technischen Einrichtungen bezieht, als diese nicht den Inhalt der Kommunikation oder die wirtschaftsbezogenen Anforderungen betrifft.[51] Gegen diesen Ansatz spricht, dass die Defizite in der Vertraulichkeit von Telemediendiensten (z. B. E-Mail) bei den Verbrauchern als bekannt vorausgesetzt werden können und deren Entscheidungen für einen Dienst

[45] Vgl. auch *Luch*/*Schulz*, Das Recht auf Internet als Grundlage der Online-Grundrechte, 2013, S. 69 ff.

[46] *Pieroth*, in: Jarass/Pieroth, Grundgesetz, Art. 87f, Rn. 86.

[47] Vgl. BVerfGE 93, 37 (74); *Sonntag*, IT-Sicherheit kritischer Infrastrukturen, 2005, S. 131 f.

[48] *Manssen*, Telekommunikations- und Multimediarecht, 36. Aufl. 2015, § 1 Rn. 10; *Säcker*, in: ders. (Hrsg.), TKG, 3. Aufl. 2013, § 2 Rn. 15.

[49] *Cornils*, in: Geppert/Schütz (Hrsg.), BeckTKG, 4. Aufl. 2013, § 2 Rn. 1.

[50] Siehe § 3 C. 2.

[51] Vgl. *Hoeren*, NJW 2007, 801 (802).

im Zweifelsfall als Grundrechtsverzicht zu werten ist, der den Staat aus der Verantwortung nimmt. Sachgemäß scheint hier indes, dass sich die verfassungsrechtliche Verantwortung aufgrund der „Schlüsselrolle von Telemedien im Cyberraum" auf die kritischen Teile bezieht.[52] Ohnehin legt § 13 Abs. 7 TMG ein weites Verständnis von der Reichweite der Verantwortung nahe. Der gebotene Schutz technischer Einrichtungen ist dort weit zu verstehen und erstreckt sich über die gesamte genutzte Hardware, Software und Systemumgebung.[53] Die verfassungsrechtlich verankerte Gewährleistungsverantwortung umfasst demnach internetbezogene Telekommunikationsinfrastrukturen einschließlich kritischer Telemedieninfrastrukturen.

B. Informations- und Wissensakteure

Ob und in welchem Ausmaß der Wissensbedarf auf institutioneller Ebene gedeckt werden kann und ob die erforderliche kognitive Infrastruktur für die mit NIS befassten Behörden besteht, ist an den organisationsrechtlichen Vorgaben zu bemessen. Bei der Ermittlung des Informationsbedarfs kann das Organisationsrecht der Verwaltungen herangezogen werden.[54] Die organisationsrechtliche Perspektive erlaubt es, sich von der anthropozentrischen Perspektive zu lösen und so der Bedeutung des organisationalen Wissens Rechnung zu tragen.[55] Darunter ist das Wissen zu verstehen, „das nicht in den Köpfen der Menschen gespeichert ist, sondern in den Operationsformen, Artefakten und sonstigen Verkörperungen von Problemlösungskompetenz eines sozialen Systems".[56] Wissen ist demnach nicht lediglich als die kognitive Kompetenz von Individuen

---

[52] Vgl. BT-Drucks. 18/4096, 2.

[53] *Gerlach*, CR 2015, S. 581 (582).

[54] Vgl. zur Erweiterung der Überlegungen über das Verfahren mit organisationsrechtlichen Arrangements *Willke*, Einführung in das systemische Wissensmanagement, 3. Aufl. 2011, S. 27; *Collin/Spiecker gen. Döhmann*, Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts – ein Problemaufriss, in: ders./dies. (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, 2008, S. 3 (17); zur Rolle von Unionsagenturen im europäischen Wissensmanagement *Kaiser*, Wissensmanagement im Mehrebenensystem, in: Gunnar Folke Schuppert/Andreas Voßkuhle (Hrsg.), Governance von und durch Wissen, 2008, S. 217 (230); zur gesamtheitlichen Betrachtung der Rechtsdimensionen *Möllers*, Materielles Recht – Verfahrensrecht – Organisationsrecht, in: Trute/Groß/Röhl/ders. (Hrsg.), Allgemeines Verwaltungsrecht – zur Tragfähigkeit eines Konzepts, 2008, S. 489 (489 ff.).

[55] Vgl. *Gärditz*, Hochschulorganisation und verwaltungsrechtliche Systembildung, 2009, S. 90 f.

[56] *Willke*, Dystopia: Studien zur Krisis des Wissens in der modernen Gesellschaft, 2002, S. 130.

zu begreifen, sondern unter Abstraktion der Zurechnung ausschließlich auf individuelles Bewusstsein auch als organisationales Wissen.[57] Der Gedanke der Wissenszurechnung an sich ist auch dem positiven Verwaltungsrecht keinesfalls fremd. Der § 48 Abs. 4 VwVfG ermöglicht der Verwaltung die Aufhebung eines rechtswidrigen Verwaltungsaktes, wenn „die Behörde von Tatsachen Kenntnis" erhält, welche die Rücknahme rechtfertigen. Die Norm begründet zwar nicht wie der im Zivilrecht analog angewendete § 166 Abs. 1 BGB die Wissenszurechnung zwischen Personen, setzt eine solche aber voraus.[58] Einer Wissenszurechnung lässt sich wohl kaum in praktischer Hinsicht entgegenhalten, dass einzelne Amtswalter keine reale Möglichkeit des Informations- und Wissensaustausches hätten. Die Wissenszurechnung darf zwar insgesamt nicht zu einer Fiktion werden, die juristische Personen weit über jede menschliche Fähigkeit hinaus belastet.[59] Technisch ist aber heutzutage jederzeit und prinzipiell von allen Orten ein intrabehördlicher Informationsaustausch durch elektronische Kommunikation möglich und Wissen beschaffbar.[60]

Maßgeblich für die materiell-rechtliche Programmierung der Wissensproduktion sind vor den verfahrensrechtlichen Informationsbefugnissen, die noch untersucht werden, die Aufgaben- und Befugnisnormen.[61] Betrachtet werden daher im Folgenden solche europäischen (I.) und nationalen (II.) Behörden, die einen spezifischen Bezug zur Gewährleistung der Sicherheit von Netzen und Informationssystemen aufweisen. Polizei- und Strafverfolgungsbehörden werden daher nur behandelt, insoweit sie Akteure im NIS-Kooperationsnetz im Sinne des Art. 11 der NIS-RL sind. Die Computer Security Incident Response Teams sind als besondere Informations- und Wissensakteure in die Untersuchung mit einzubeziehen (III.).

Inwieweit die NIS-Akteure effektive wissensbasierte Organisationen bilden, ist noch nicht durch das Bestehen entsprechenden Organisationrechts determiniert. Die jeweilige Stärke der Rolle als Informations- und Wissensakteur ist durch spezifische Informationsbeziehungen bedingt, die sich aus Kompetenzzuweisungen, der föderalen Struktur, der Unterscheidung von innerer und äußerer Sicherheit und der etwaigen Trennung von Polizei- und Verfassungsschutzbehörden bzw. vom Bundesnachrichtendienst einerseits sowie der Tren-

---

[57] *Augsberg*, Informationsverwaltungsrecht, S. 35; *Luhmann*, Die Wissenschaft der Gesellschaft, 1990, S. 11.

[58] Vgl. *Henning*, Wissenszurechnung im Verwaltungsrecht, 2003, S. 59 ff.

[59] Vgl. der Einwand in BGHZ 132, 30 (38).

[60] *Aden*, Wissenszurechnung in der Körperschaft, NJW 1999, 3098 (3099).

[61] *Kluth*, Die Strukturierung von Wissensgenerierung durch das Verwaltungsorganisationsrecht, in: Spiecker gen. Döhmann/Collin (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, 2008, S. 73 (79 ff.).

nung der zivilen Sicherheitsbehörden von militärischen Einrichtungen andererseits ergeben.[62] Dies ist eine Frage des im weiteren Verlauf untersuchten interbehördlichen Transfers von Informationen.[63]

I. Europäische Institutionen

3. Europäische Agentur für Netz- und Informationssicherheit

Die wichtigste zivile Sicherheitsbehörde auf europäischer Ebene im Bereich der NIS ist die Europäische Agentur für Netz- und Informationssicherheit (ENISA). Sie wurde im Jahr 2004 errichtet, um zur Gewährleistung der Netz- und Informationssicherheit innerhalb der Union beizutragen.[64] Dem allgemeinen Trend im europäischen Verwaltungsrecht entsprechend wurde die bevorzugte Organisationsform der Agentur gewählt.[65] Im Jahr 2013 wurde die Rechtsgrundlage der ENISA neu gefasst.[66] Sie zielt darauf ab, die Agentur zu „stärken", um auf die Entwicklung der Technik, des Marktes und des sozioökonomischen Umfelds mit den damit einhergehenden Herausforderungen zu reagieren.[67]

Das Aufgabenprofil der ENISA ist vielfältig. Sie soll zur Gewährleistung einer hohen und effektiven Netz- und Informationssicherheit innerhalb der Union beitragen und eine Kultur der Netz- und Informationssicherheit mitentwickeln.[68] Zu den Zielen der ENISA gehört zuvörderst die Entwicklung und die Pflege von einem „hohen Niveau an Sachkenntnis" (Art. 2 Abs. 1 ENISA-VO). Der Aufbau von Wissen ist nicht Selbstzweck, sondern das angesammelte Wissen soll den Mitgliedstaaten auf deren Ersuchen hin und den Organen der Union zur Verfügung gestellt werden (Art. 3 Abs. 1 lit. b i) bzw. Art. 3 Abs. 3 lit. f iii) ENI-

---

[62] Dazu *Kutscha*, Innere Sicherheit und Verfassung, in: Roggan/Kutscha (Hrsg.), Handbuch zum Recht der Inneren Sicherheit, 2. Aufl. 2006, S. 24 (85).

[63] Siehe § 4.

[64] Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit (ABl. L 77 vom 13.3.2004, S. 1). Das Mandat wurde durch die Verordnung (EG) Nr. 1007/2008 vom 24. September 2008 und durch die Verordnung (EG) Nr. 580/2011 des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EG) Nr. 460/2004 jeweils verlängert.

[65] Vgl. *Majone*, The New European Agencies: Regulation by Information, Journal of European Public Policy 1997, 262 (262 ff.).

[66] Verordnung (EU) Nr. 526/2013 des Europäischen Parlaments und des Rates vom 21. Mai 2013 über die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) und zur Aufhebung der Verordnung (EG) Nr. 460/2004 (ABl. L 165/42 vom 18.06.2013). Im Folgenden: ENISA-VO.

[67] ENISA-VO, Erwägungsgrund 11.

[68] ENISA-VO, Erwägungsgrund 9.

SA-VO). Die Unterstützung kann auch die Formulierung von Rechtsakten umfassen (vgl. Art. 3 Abs. 1 lit. a ENISA-VO).[69]

4. EU-Intelligence and Situation Centre

Das EU-Intelligence and Situation Centre (EU INTCEN) ist eine 2003 inoffiziell gegründete nachrichtendienstliche Organisation der EU im Rahmen des Europäischen Auswärtigen Dienstes (EAD) im Sinne von Art. 27 EUV. Die Aufgaben von INTCEN sind unklar. Es wird davon ausgegangen, dass INTCEN nicht selbst Informationen generieren und erforschen kann. Es fungiert jedenfalls als europäische Plattform und Tauschzentrale für geheimdienstliche und nachrichtendienstliche Informationen.[70] Das beim Rat angesiedelte EU INTCEN ist weder dem Europäischen Parlament noch den nationalen Parlamenten rechenschaftspflichtig. Die Informationskooperation basiert auf strikter Freiwilligkeit.

II. Nationale Behörden

1. Nationale Behörden für Netz- und Informationssicherheit

Die Mitgliedstaaten haben nach Art. 6 der NIS-RL eine zuständige nationale Behörde für die Netz- und Informationssicherheit einzurichten. Es können mehrere Behörden zuständig sein, doch nur eine Behörde hat als zentrale Anlaufstelle zu fungieren. Die zentralen deutschen NIS-Behörden sind das Bundesamt für Sicherheit in der Informationstechnik (a) und die Bundesnetzagentur (b). Insoweit der Datenschutz die Datensicherheit umfasst, sind auch die Datenschutzbehörden dem Bereich der Netz- und Informationssicherheit zuzuordnen (c).

a) Bundesamt für Sicherheit in der Informationstechnik

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist in Deutschland die zentrale zivile und defensive Sicherheitsbehörde im Bereich der Sicherheit der Informationstechnik. Das Amt ist aus der Zentralstelle für Chiffrierwesen, einem Teil des Bundesnachrichtendienstes, hervorgegangen.[71] Organisationsrechtlich ist das BSI eine Bundesoberbehörde, die dem BMI untersteht (§ 1 S. 1 und 3 BSIG) und damit nicht unabhängig, sondern in Zweifelsfällen

---

[69] Vgl. auch Erwägungsgrund 68 NIS-RL. Kritisch zur Rolle von dezentralen Agenturen in der Unionsrechtssetzung *Weiß*, EuR 2016, 631 (636).

[70] *Bergmann*, in: Handlexikon der Europäischen Union, 5. Aufl. 2015, Eintrag INTCEN.

[71] Bundesamt für Sicherheit in der Informationstechnik, Historie, 2015, abrufbar unter: https://www.bsi.bund.de/DE/DasBSI/Historie/historie_node.html.

weisungsgebunden handelt.[72] Es ist nach § 1 S. 2 zuständig für die Informationssicherheit auf nationaler Ebene.

Das BSI fördert die Sicherheit in der Informationstechnik (§ 3 Abs. 1 S. 1 BSIG), worunter die Einhaltung bestimmter IT-Sicherheitsstandards zu verstehen ist.[73] Die Informationstechnologie entwickelt sich rasant weiter und bringt Verwundbarkeiten und Angriffsvektoren mit sich. Im Recht, namentlich in Art. 91c Abs. 1 GG, findet diese Dynamik Berücksichtigung. Dort wird der Begriff des „informationstechnischen Systems" verwendet. Der Terminus erfasst sämtliche „technische Mittel zur Verarbeitung und Übertragung von Informationen".[74] Damit soll der Begriff bewusst für zukünftige, noch unbekannte Weiterentwicklungen der Informationstechnologie offengehalten werden.[75] Informationen zu sammeln und Wissen über Internetsicherheit zu generieren dient der Erfüllung sicherheitstechnischer Bedürfnisse. Dem breit gefächerten Aufgabenspektrum (§ 3 Abs. 1 S. 2 Nr. 1–15 BSIG) lassen sich wesentliche informationsrechtliche Zuweisungen entnehmen, die hier interessierende kognitive Funktionen einnehmen.

Das BSI nimmt im Bereich NIS eine hervorzuhebende Intelligence-Funktion (*cyber intelligence*) ein. Wesentliche Bedeutung für die kognitive Organisationsstruktur des BSI ist gemäß § 3 Abs. 1 Nr. 2 BSIG die Aufgabe der Sammlung und Auswertung von Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen und der Zurverfügungstellung der gewonnenen Erkenntnisse für andere Stellen. Die Kenntnis über Sicherheitsschwachstellen und Bedrohungen ist unabdingbar, weil sich ein großer Teil der Gefährdungen schon durch einfache (administrative) Maßnahmen sowie durch den Einsatz verfügbarer Softwareprodukte vermeiden oder begrenzen lässt.[76] Zudem ist das BSI als zentrale Meldestelle bestimmt, sowohl nach § 4 Abs. 1 BSIG für die Sicherheit der Informationstechnik beim Bund als auch nach § 3 Abs. 1 S. 3 Nr. 17 in Verbindung mit § 8b Abs. 1 BSIG für Betreiber kritischer Infrastrukturen. Das Amt ist auch mit der Fortschreibung eines möglichst lückenlosen und systematischen Lagebildes beauftragt, dessen es bedarf, um eine Übersicht über den Status quo in der Netz- und Informationssicherheit auf nationaler Ebene zu erlangen.

Im Zusammenhang mit der Informationstechnik in diesen kritischen Infrastrukturen übernimmt das Bundesamt erweiterte Aufgaben nach § 8b Abs. 2

---

[72] Zur Frage der organisationsrechtlichen Unabhängigkeit unter § 4 F. III.

[73] Siehe oben § 2 A. zum Begriff der IT-Sicherheit.

[74] BT-Drs. 16/12410, S. 8; gleich ist die Begriffsbestimmung von „Informationstechnik" in § 2 Abs. 1 BSIG.

[75] Vgl. *Suerbaum*, in: Hillgruber/Epping (Hrsg.), BeckOK GG, 27. Ed. 2015, Art. 91c GG Rn. 9 f.

[76] *Eckert*, IT-Sicherheit, 2000, S. 95.

Nr. 1 bis 4 BSIG. Es sammelt für die Gefahrenabwehr wesentliche Informationen, wie zu Sicherheitslücken, Schadprogrammen, zu erfolgten und versuchten Angriffen und der beobachteten Vorgehensweise, und wertet diese Informationen aus. Es hat ferner die Informationen hinsichtlich ihrer potenziellen Auswirkungen auf die Verfügbarkeit der kritischen Infrastrukturen zu analysieren. Dafür arbeitet die Behörde mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und den zuständigen Aufsichtsbehörden zusammen. Das Lagebild bezüglich der IT-Sicherheit hat das BSI kontinuierlich zu aktualisieren.

Die Erforderlichkeit der Expertisegewinnung macht § 3 Abs. 1 S. 2 Nr. 14 BSIG deutlich. Danach ist Aufgabe des BSI auch die „Beratung und Warnung" des Bundes, der Länder und von Privaten (Hersteller, Vertreiber und Anwender) in Fragen der Sicherheit in der Informationstechnik. Die Beratungsfunktion des BSI hinsichtlich kritischer Infrastrukturen wurde mit der Novellierung des BSIG durch das IT-Sicherheitsgesetz gestärkt. Nach § 3 Abs. 3 BSIG kann das BSI die Betreiber auf deren Ersuchen beraten und unterstützen.

b) Bundesnetzagentur

Die Bundesnetzagentur wurde ursprünglich als Regulierungsbehörde für Telekommunikation und Post auf Grundlage des Art. 87f Abs. 2 S. 2 GG errichtet. Um später eine sektorübergreifende Regulierungsbehörde zu schaffen und den Zuständigkeitserweiterungen Rechnung zu tragen, wurde die Behörde anschließend in Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen umbenannt.[77] Die zentrale Aufgabenzuweisungsnorm für die Bundesnetzagentur ist § 116 TKG.[78] Danach nimmt sie die ihr nach dem TKG zugewiesenen Aufgaben und Befugnisse wahr. Der Agentur fällt insofern die Aufgabe zu, die für die jeweiligen Sektoren formulierten Regulierungsziele umzusetzen. Für den Bereich des Telekommunikationssektors sind das die Ziele des § 2 Abs. 1 und Abs. 2 TKG, zu denen „die Wahrung der Interessen der öffentlichen Sicherheit" gehört (§ 2 Abs. 2 Nr. 9 TKG).[79] Das Aufgabenprofil der Bundesnetzagentur enthält daher nicht nur marktregulatorische Elemente. Die

---

[77] *Berliner*, Informationsbefugnisse der Bundesnetzagentur im Telekommunikationsrecht, 2012, S. 21 f.

[78] Nach § 2 Abs. 1 Nr. 2, Abs. 2 BNAG ist die Bundesnetzagentur u. a. auf dem Gebiet der Telekommunikation tätig und nimmt im Rahmen dieser Tätigkeiten die Verwaltungsaufgaben des Bundes wahr, die ihr durch oder aufgrund eines Gesetzes zugewiesen sind.

[79] Die Abteilung Informationstechnik und Sicherheit ist mit 172 Mitarbeitern (Stand 13.01.2015) nicht unbedeutend. Vgl. Antwort der Bundesnetzagentur vom 13.01.2015 auf Anfrage nach § 1 IFG, abrufbar unter: https://fragdenstaat.de/a/7947.

Behörde ist vielmehr auch mit ordnungsrechtlichen Befugnissen ausgestattet, was sie zu einer besonderen Aufsichtsbehörde macht.[80]

c) Datenschutzbehörden

Die Aufsichtsbehörden für den Datenschutz sind nicht nur wichtige Wissensakteure für den Datenschutz im herkömmlichen Begriffsverständnis, also für den Schutz von Rechtspositionen von Personen, sondern auch für die ursprüngliche Wortbedeutung, d. h. für den Schutz von Daten im Sinne der Informationssicherheit. Die materiell-rechtlichen Pflichten aus § 9 BDSG samt den zugehörigen Anlagen, Art. 17 RL 95/46/EG sowie Art. 32 DS-GVO, gemäß derer die Verarbeiter personenbezogener Daten geeignete technische und organisatorische Maßnahmen zu treffen haben, um ein dem Risiko angemessenes Schutzniveau der Datensicherheit zu gewährleisten, machen Datensicherheit zu einem Kernanliegen des Datenschutzes. Im Vorfeld ihrer Tätigkeiten trifft die Datenschutzbehörden eine Beobachtungspflicht. Um die neuesten Risiken und Schutzmaßnahmen zu kennen, „muss" die Aufsichtsbehörde nach Art. 57 Abs. 1 lit. i) DS-GVO „maßgebliche Entwicklungen verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken". Die Expertisefunktion zeigt sich außerdem an den institutionellen Aufgaben der Aufsichtsbehörden. Die Aufsichtsbehörden haben „zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen", an die mitgliedstaatlichen Gewalten oder die Öffentlichkeit von sich aus oder auf Anfrage Stellungnahmen zu richten (Art. 58 Abs. 3 lit. b DS-GVO).

2. Nachrichtendienstliche Einrichtungen

Die Nachrichtendienste sind keine NIS-Behörden im Sinne von Art. 8 NIS-RL. Gleichwohl tragen der Bundesnachrichtendienst (a) und das Bundesamt für Verfassungsschutz (b) zur Informations- und Erkenntnisgewinnung der NIS-Behörden bei.

a) Bundesnachrichtendienst

Die Aufgabe des Bundesnachrichtendienstes (BND) besteht nach § 1 Abs. 2 BNDG darin, mittels Informationen Erkenntnisse über das Ausland zu gewinnen, die von außen- und sicherheitspolitischer Relevanz für Deutschland sind. Dem BND kommt für die Zukunft eine Schlüsselrolle in der nationalen Cyber-

[80] Vgl. *Ruffert*, Regulierung im System des Verwaltungsrechts, AöR 124 (1999), 237 (247 f.).

sicherheit und damit der Außen- und Sicherheitspolitik zu.[81] Die besondere Rolle des Bundesnachrichtendienstes ergibt sich zum einen aus der Befugnis und zum anderen aus den technischen Möglichkeiten zur strategischen Erfassung internationaler Datenverkehre.

Aus der Organisation und den gesetzlichen Ausprägungen des Trennungsgebots in § 1 S. 2 und § 2 Abs. 3 BNDG ergibt sich, dass der BND nicht mit polizeilichen Befugnissen ausgestattet sein darf. Der BND ist als *Nachrichten*dienst auf Informationsrechte beschränkt, die sich in der Informationsübermittlung an Dritte oder in Berichtspflichten erschöpfen. Über weitergehende operative Befugnissen oder Zwangsbefugnissen verfügt der BND nicht, was ihn von *Geheim*diensten unterscheidet.[82]

Das Aufgabenfeld des BND resultiert zunächst aus dem Aufklärungsauftrag bezüglich Tatsachen, die „von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland" sind. Allerdings sind aufgrund der Regelungstechnik des BNDG, die sich durch eine auf Geheimhaltungsinteressen zurückgehende Kürze und ein geringes Maß an Normbestimmtheit und -klarheit auszeichnet, die Aufgaben und Befugnisse nicht eindeutig bestimmt.[83] Aus § 1 Abs. 2 BNDG folgt insoweit nur ein Aufgabenprofil, welches sich maßgeblich über den Auslandsbezug definiert („über das Ausland"). Dieser Auslandsbezug bestimmt sich nicht so sehr nach dem Ort der Informationsgewinnung, sondern vielmehr nach dem Inhalt der zu gewinnenden Erkenntnis.[84] Das Aufgabenprofil wird durch die nähere Bestimmung des Aufklärungsauftrags geprägt, der sämtliche Aufgaben des Dienstes verbindet.

Das Aufgabenfeld des Dienstes ist hinsichtlich der Cyberabwehr erweitert worden.[85] Aufgrund des auslandsbezogenen Aufgabenprofils und infolge der technisch nur durch den BND generierbaren Erkenntnisse ist der Nachrichtendienst in die Lage versetzt worden, mit den zur Verfügung stehenden Kompetenzen und Mitteln Erkenntnisse über die Cyberbedrohungslage und -abwehr beizusteuern. Das schließt die Internetsicherheit ein.

b) Bundesamt für Verfassungsschutz

Das Bundesamt für Verfassungsschutz (BfV) hat den gesetzlichen Auftrag (§ 3 BVerfSchG), Informationen, Nachrichten und Unterlagen zu sammeln und aus-

---

[81] *Kullik*, Vernetzte (Un-)Sicherheit, 2014, S. 155.

[82] *Gusy,* in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, BNDG, § 1 Rn. 23.

[83] *Gusy*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, BNDG, Vorbemerkung Rn. 10.

[84] *Droste*, Handbuch des Verfassungsschutzrechts, 2007, S. 162 ff.

[85] Siehe § 3 D II. 3.

zuwerten. Der dem BMI unterstehende Inlandsgeheimdienst verfolgt primär nicht Straftaten, sondern hat einen Beobachtungsauftrag hinsichtlich verfassungsbezogener Bestrebungen. Mit der Neuausrichtung der Cybersicherheitsarchitektur durch die Digitale Agenda der Bundesregierung erfährt das BfV eine strategische und organisatorische Stärkung.[86]

Eine gesetzliche Umsetzung der Neuausrichtung ist der 2016 in Kraft getretene § 5 Abs. 4 BVerfSchG. Dem BfV kommt die Funktion einer Zentralstelle zu, welche die Landesbehörden für Verfassungsschutz unterstützt. Die Konkretisierung der allgemeinen Unterstützungsregelung des § 1 Abs. 3 BVerfSchG zielt darauf, „speziell im Bereich der Cyberabwehr wie auch im Bereich technischer Analysefähigkeit (durch Verbesserung der informationstechnischen Analysemittel)" Ressourcen bereitzustellen.[87] § 5 Abs. 4 BVerfSchG stellt keine abschließende Regelung dar („insbesondere"). Daneben übernimmt das BfV die zentrale Beobachtung technischer Entwicklungen sowohl für die eigene Nutzung als auch für die potenzielle Nutzung durch das nachrichtendienstliche Gegenüber.[88] In erster Linie soll das BfV die Gefährdungslage durch elektronische Angriffe analysieren und zuordnen.[89] Verschiedene Erkenntnisse werden zusammengeführt, neben solchen aus menschlichen Quellen auch solche aus Schadsoftware-Erkennungssystemen und Fernmeldeaufklärung.[90] Eine zentrale Rolle hat das BfV in der internetbasierten Spionageabwehr[91] und in der Analyse der Gefährdungen für kritische Infrastrukturen im Rahmen von § 8b Abs. 2 Nr. 4 BSIG zu erfüllen. Das BfV ist somit zuständig, wenn die Amtsführung der Verfassungsorgane durch Cyberangriffe beeinträchtigt wird (vgl. § 3 Abs. 1 Nr. 1 BVerfSchG). Richten sich etwaige Angriffe nicht gegen eine Einrichtung eines Verfassungsorgans, darf das BfV jedenfalls dann tätig werden, wenn sie von einer fremden Macht, also vor allem von einem Nachrichtendienst des Gegenübers, ausgehen (§ 3 Abs. 1 Nr. 2 BVerfSchG). Seine Aufgabe in der Internetsicherheit nimmt das Amt insbesondere durch das Mitwirken am Cyber-Abwehrzentrum wahr.[92]

---

[86] *Bundesregierung*, Digitale Agenda 2014–2017, 2014, S. 33.

[87] Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes, Bearbeitungsstand 20.04.2015, BT-Drs. 18/4653, S. 21.

[88] BT-Drs. 18/4653, S. 21.

[89] Kritisch und mit der Forderung, den Beobachtungsdruck zu reduzieren und thematisch auf Kernbereiche der Beobachtung extremistischer Phänomene zu reduzieren, *Kullik*, Vernetzte (Un-)Sicherheit, 2014, S. 149.

[90] *Maaßen*, PinG 2015, 137 (140).

[91] *Schönbohm*, Deutschlands Sicherheit: Cybercrime und Cyberwar, 2011, S. 112.

[92] Siehe § 3 B. II. 3.

3. Nationales Cyber-Abwehrzentrum

Als behördenübergreifende Einrichtung wurde 2011 als Teil der Cybersicherheitsstrategie der Bundesregierung die Errichtung des Nationalen Cyber-Abwehrzentrums (NCAZ) beschlossen.[93] Das NCAZ ist beim BSI angesiedelt, dessen Präsident auch der Vorsitzende des NCAZ ist.[94] Ziel der institutionalisierten Kooperation im NCAZ ist der zügige und unkomplizierte Informationsaustausch über Sicherheitslücken in Hard- und Software, abstrakte Angriffsformen und Täterbilder sowie sonstige Risiken und Gefahren für die Informations- und Kommunikationstechnologie.[95] Auf Grundlage des Kabinettsbeschlusses und von Kooperationsvereinbarungen arbeiten als Kernbehörden das BSI, das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und das BfV zusammen. Das Bundeskriminalamt, die Bundespolizei, das Zollkriminalamt, der Militärische Abschirmdienst, die Bundeswehr sowie die aufsichtführenden Stellen über die Betreiber der kritischen Infrastrukturen sind assoziiert und beteiligen sich durch Verbindungsbeamte. Die Beteiligten erfassen zum gemeinsamen Nutzen eine „nationale Cybersicherheitslage". Der Nationale Cybersicherheitsrat[96] wird anlassbezogen oder regelmäßig unterrichtet. Das NCAZ ist keine eigenständige Behörde, eine Rechtsgrundlage wird für entbehrlich gehalten. Ein Errichtungsgesetz sei ebenfalls nicht erforderlich, da die beteiligten Behörden unter strikter Wahrung ihrer Aufgaben und gesetzlichen Befugnisse zusammenarbeiten würden.[97] Eine dauerhaft analytische oder operative Zusammenarbeit finde nicht statt.[98]

Das NCAZ ist die erste Einrichtung, die bezweckt, alle Beteiligten über die Grenzen von Zuständigkeiten und Hierarchien hinweg zusammenzubringen und Informationen zumindest auf informeller Ebene punktuell zu fusionieren. Die Institution ist Ausdruck der Erkenntnis, dass die Grenze sicherheitsrelevanten Wissens nicht am Maßstab der Unterscheidung von ziviler und militärischer sowie polizeilicher und strafverfolgungsrechtlicher Sicherheit gezogen werden

---

[93] Das NCAZ ist nicht zu verwechseln mit dem Gemeinsamen Internet-Zentrum (GIZ), das 2007 eingerichtet wurde. Die Aufgaben des GIZ werden von den beteiligten Behörden festgelegt. Seit Aufnahme des Wirkbetriebs sind das die Sichtung, Auswertung und Analyse terroristischer Internetinhalte mit Deutschlandbezug. Siehe BT-Drs. 17/6596, S. 3.

[94] *Graulich*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, BKAG, § 2 Rn. 26.

[95] *Linke*, DÖV 2015, 128 (129).

[96] Der Nationale Cybersicherheitsrat ist ein strategisches Planungs- und Beratungsgremium der Bundesregierung, siehe Bundesministerium des Innern, Cyber-Sicherheitsstrategie für 2016, S. 45.

[97] BT-Drs. 17/5694, S. 2; *Graulich*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, BKAG, § 2 Rn. 26.

[98] BT-Drs. 17/5694, S. 3.

kann. Inwiefern das unterschiedliche Organisationsrecht der Beteiligten mit verschiedenartigen Aufgabenzuweisungen tatsächlich und rechtlich den Informationsfluss beeinflusst, ist eine Frage des Transfers sicherheitsrelevanter Informationen.[99]

III. Computer Security Incident Response Teams

Für die Netz- und Informationssicherheit bedeutende Einrichtungen sind die IT-Notfallteams, sog. Computer Security Incident Response Teams (CSIRTs) oder Computer Emergency Response Teams (CERTs).[100] Dabei handelt es sich um Notdienste, die auf Fachebene für die Bewältigung von Sicherheitsvorfällen und -risiken nach einem festgelegten Ablauf zuständig sind.[101] Die Zusammenarbeit von CSIRTs kann in vier Konstellationen erfolgen:[102] Kommunikation, d. h. die Kommunikation mit der Zielgruppe, Kooperation, also die Zusammenarbeit mit anderen CSIRTs zur Behandlung von Sicherheitsvorfällen, Koordination, d. h. die Abstimmung hinsichtlich des gemeinsamen Vorgehens, und Kommando, also die Leitung von Einsätzen gegen Cyberangriffe.

CSIRTs spielen eine wesentliche Rolle in der Gewährleistung der Sicherheit von Netzen und Informationssystemen,[103] sie sind aber wissenschaftlich bislang wenig behandelt und noch weniger in der Rechtswissenschaft rezipiert. Ursprünglich wurde die Aufgabe der CSIRTS bzw. CERTs in nichtstaatlicher Selbstorganisation vor allem im universitären und privaten Bereich wahrgenommen. In der jüngsten Vergangenheit ist jedoch eine Zunahme der staatlichen, d. h. öffentlich initiierten Stellen zu beobachten, was in einem unmittelbaren Zusammenhang mit der Tendenz steht, den Schutz kritischer Informationsinfrastrukturen als öffentliche Aufgabe anzusehen.[104]

Die Einrichtung von CSIRTs schreibt Art. 9 NIS-RL den Mitgliedstaaten vor. In Deutschland fungiert das beim BSI angesiedelte CERT-Bund als zentrale Anlaufstelle für präventive und reaktive Maßnahmen für NIS-Sicherheitsvorfälle auf nationaler Ebene.[105] Zu den Aufgaben gehören die Analyse, Reaktion,

---

[99] Siehe § 4 C. III.

[100] Eine andere früher gebräuchliche Bezeichnung ist Computer Security Incident Response Team (CSIRT); vgl. aber auch noch DS-GVO-E, Erwägung 39.

[101] IETF, RFC-2350, abrufbar unter: https://www.ietf.org/rfc/rfc2350.txt. Solche CERTs gibt es seit Langem in privaten Unternehmen, öffentlichen Einrichtungen, Forschungseinrichtungen und sonstigen Stellen, um auf konkrete Sicherheitsvorfälle reagieren zu können.

[102] Vgl. *Huber/Hellwig/Quirchmayr*, DuD 2016, 162 (163 f.).

[103] Bundesministerium des Innern, Cyber-Sicherheitsstrategie für 2016, S. 34.

[104] *Einzinger/Skopik/Fiedler*, DuD 2015, 723 (724); *Skierka/Morgus/Hohmann/Maurer*, CSIRT Basics for Policy-Makers, 2015, S. 8.

[105] BSI, RFC-2350, 3 Charter, abrufbar unter: https://www.bsi.bund.de/SharedDocs/

Unterstützung und Warnung im Zusammenhang mit Sicherheitsvorfällen.[106] Privatpersonen und kleine Unternehmen werden vom Bürger-CERT vorbeugend über Gefahren und Risiken informiert und gewarnt.[107] Eine Vielzahl von CERTs hat sich zu einem übergreifenden CERT-Verbund zusammengeschlossen, um Informationsaustausch zu ermöglichen und Synergien in gemeinsamen Projekten freizusetzen.[108] Auf europäischer Ebene besteht mit dem CERT-EU für die Organe, Einrichtungen und sonstigen Stellen der Europäischen Union ein eigenes IT-Notfallteam. Eine transeuropäische CERT-Kooperation stellt die European Government CERTs (EGC) Group dar, in der sich die nationalen CERTs von Mitgliedstaaten zur Problembehandlung in größer skalierten Netzwerken zusammengeschlossen haben.[109] Als Informations- und Wissensakteure kommt ihnen im Rahmen des europäischen Informationsaustausches eine wichtige Rolle zu.

C. Rahmen der Informationsgenerierung

Die Frage, welche privaten Betreiber von Internetinfrastrukturen und Anbieter von über das Internet vermittelten Diensten Quellen der öffentlichen Informationsgewinnung sein können, richtet sich nach dem für sie anwendbaren IT-Sicherheitsrecht. Die Sicherheit im und die Sicherheit des Internets mit den dazugehörigen Netzen wird durch ein ganzes Spektrum regulatorischer Vorgaben beeinflusst.[110] Zu untersuchen ist daher, welcher Rechtsrahmen für die Netz-

---

Downloads/EN/BSI/Kritis/rfc2350_CERT-Bund_txt.txt?__blob=publicationFile; Bundesministerium des Innern, Cyber-Sicherheitsstrategie für 2016, S. 34.

[106] BSI, RFC-2350, 4.1, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Kritis/rfc2350_CERT-Bund_txt.txt?__blob=publicationFile.

[107] Bürger-Cert, Über uns, abrufbar unter: https://www.buerger-cert.de/about.

[108] CERT-Verbund, Unser Ziel, abrufbar unter: https://www.cert-verbund.de/. Der IT-Planungsrat, der mit dem IT-Staatsvertrag zur Ausführung des Art. 91c GG 2010 als zentrales Gremium für die föderale Zusammenarbeit in der IT von Bund, Ländern und Kommunen errichtet wurde, hat eine Kooperationsgruppe damit beauftragt, mit dem Aufbau eines Verwaltungs-CERTS-Verbunds zu beginnen, *IT-Planungsrat*, Entscheidung 2011/33 – Kooperationsgruppe Leitlinie Informationssicherheit.

[109] European Government Certs group, Main, abrufbar unter: http://www.egc-group.org/index.html.

[110] *Spindler*, IT-Sicherheit und kritische Infrastrukturen, in: Kloepfer (Hrsg.), Schutz kritischer Infrastrukturen, 2010, S. 85 (88), der die Vielzahl der öffentlich-rechtlichen und zivilrechtlichen Vorschriften zusammengenommen darstellt als „System kommunizierender Röhren […], das sich gegenseitig beeinflussen und ergänzen kann"; vgl. *ders.*, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, Studie im Auftrag des BSI durchgeführt, 2007, online abrufbar; vgl. für die USA *Fischer*, Federal Laws Relating to Cyber-

und Informationssicherheit in der Union gilt (I.). Diesem lassen sich die materiell-rechtlichen Regelungen zur Gewährleistung der Sicherheit von Internetinfrastrukturen und -diensten und zugleich die einschlägigen informationsverwaltungsrechtlichen Vorschriften zur Informationsgenerierung entnehmen (II.).

I. Internetsicherheit im europäischen Primärrecht

Die Begriffe Internet, Internetsicherheit oder Netz- und Informationssicherheit finden sich in den europäischen Verträgen nicht. Der primärrechtliche Rahmen für das aktuelle und potenzielle Internetsicherheits- und Informationsverwaltungsrecht ergibt sich aus verschiedenen Kompetenzbereichen, insbesondere aus dem Politikbereich des Raums der Freiheit, der Sicherheit und des Rechts (1.), dem europäischen Infrastrukturrecht (2.), dem europäische Katastrophenschutzrecht (3.) und dem Statistikrecht (4.). Die wesentlichen bestehenden sekundärrechtlichen Vorgaben zur Netz- und Informationssicherheit sind indes auf die Kompetenz zur Binnenmarktharmonisierung gestützt. Ihnen sind die zentralen informationsverwaltungsrechtlichen Vorschriften zu entnehmen (5.).

1. Raum der Freiheit, der Sicherheit und des Rechts

Einen Raum der Freiheit, der Sicherheit und des Rechts (RFSR) zu bieten ist Ziel der Union, Art. 3 Abs. 2 EUV. Der RFSR erfasst die Sicherheit in der Union, die von der „nationalen Sicherheit" der Mitgliedstaaten im Sinne des Art. 4 Abs. 2 S. 3 EUV zu unterscheiden ist. Für diese behalten sich die Mitgliedstaaten die Letztverantwortung vor.[111] Die Zielvorstellung des RFSR wird durch die Bestimmungen in Art. 67 ff. AEUV näher ausgeführt. Die Union wird durch sie kompetenziell ausgestattet. Der Begriff der Sicherheit im Sinne von Art. 67 ff. AEUV bezieht sich auf die spezifischen Bedrohungen, die sich infolge der Entwicklung des Binnenmarktes ergeben.[112] Es geht insbesondere um die Prävention und Repression von Straftaten. Art. 83 Abs. 1 UAbs. 2 AEUV listet als besonderen Kriminalitätsbereich mit grenzüberschreitender Dimension die Computerkriminalität auf. Für diesen dürfen die Gesetzgeber strafrechtliche Mindestvorgaben festlegen. Art. 87 erlaubt der Union die Entwicklung der polizeilichen Zusammenarbeit. Gemäß Art. 87 Abs. 2 lit. a AEUV ist vor allem die informationelle Zusammenarbeit durch Einholen, Speichern, Verarbeiten, Ana-

---

security: Overview and Discussion of Proposed Revisions, Congressional Research Service, 2013, S. 2.

[111] *Streinz*, in: ders. (Hrsg.), EUV/AEUV, 2. Aufl. 2012, EUV, Art. 4 Rn. 17; vgl. auch Art. 276 AEUV.

[112] *Weiß*/*Satzger*, in: Streinz (Hrsg.), EUV/AEUV, 2. Aufl. 2012, AEUV, Art. 67 Rn. 29.

lysieren und Austauschen sachdienlicher Informationen erlaubt. Diese Zusammenarbeit ist „einer der zentralen Bereiche des entstehenden Informationsverwaltungsrechts im RFSR".[113] Art. 87 Abs. 2 lit. a AEUV gestattet allerdings nur die zwischenbehördliche informationelle Zusammenarbeit, sodass Maßnahmen zur primären Informationsbeschaffungspflicht von Privaten nicht auf diese Kompetenznorm gestützt werden können.[114] Aus systematischer Perspektive ergibt sich dies aus der Titelüberschrift von Kapitel 5 des AEUV („Polizeiliche Zusammenarbeit"). In den Art. 87 bis 89 AEUV findet sich zudem an keiner Stelle eine Regelung, die das unmittelbare Verhältnis der Union oder der Mitgliedstaaten zu Privaten regelt.

Eine bereits getroffene, auf den Kompetenznormen des RFSR beruhende und die Sicherheit der Infrastruktur des Internets betreffende Maßnahme stellt die RL 2013/40/EU über Angriffe auf Informationssysteme dar.[115] Die Richtlinie stützt sich auf Art. 83 Abs. 1 AEUV und hat die Festlegung strafrechtlicher Mindestvorgaben hinsichtlich der Straftaten und Strafen bei Angriffen auf Informationssysteme sowie die Verbesserung der Zusammenarbeit der Einrichtungen wie Eurojust, Europol und ENISA zum Gegenstand.[116] Informationsverwaltungsrechtliche Implikationen folgen aus Art. 13 RL 2013/40/EU. Der Artikel schafft hinsichtlich des Informationsaustausches über Straftaten eigenständige, vom NIS-Kooperationsrecht unabhängige Strukturen. Informationelle Verbindungsstrukturen zur hier relevanten NIS-Verwaltung bestehen jedoch auf Grundlage des NIS-Kooperationsrechts.[117] Im Übrigen ist nicht ausgeschlossen, dass sich Maßnahmen zur NIS-Informationszusammenarbeit auch auf Art. 87 Abs. 2 lit. a AEUV stützen können, da die genannten Informationsverarbeitungen nicht originär polizeiliche Informationen zum Gegenstand haben müssen.[118]

---

[113] *Röben*, in: Grabitz/Hilf/Nettesheim (Hrsg.), AEUV/EUV, 59. Aufl. 2016, Art. 87 AEUV Rn. 49.

[114] *Röben*, in: Grabitz/Hilf/Nettesheim (Hrsg.), AEUV/EUV, 59. Aufl. 2016, Art. 87 AEUV Rn. 21.

[115] Die Internetinfrastruktur wird auch durch Regelungen von Netzsperren getroffen. Diese betreffen aber nicht die Netz- und Informationssicherheit, sondern zielen auf die Bekämpfung bestimmter Inhalte und den Jugendschutz. Dazu *Mayer*, Europäisches Internetverwaltungsrecht, in: *Terhechte* (Hrsg.), Verwaltungsrecht in der Europäischen Union, 2011, § 25, Rn. 38.

[116] Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates (ABl. Nr. L 218 S. 8); siehe dazu *Reindl-Krauskopf*, ZaöRV 2014, 563 (563 ff.).

[117] Siehe § 4 B. II. 2. c) bb) (2).

[118] *Böse*, in: Schwarze/Becker/Hatje/Schoo (Hrsg.), EU-Kommentar, 3. Aufl. 2012, AEUV, Art. 87 Rn. 6; *Röben*, in: Grabitz/Hilf/Nettesheim (Hrsg.), AEUV/EUV, 59. Aufl. 2016, Art. 87 AEUV Rn. 21.

2. Schutz personenbezogener Daten

Korrespondierend zu dem in Art. 8 GRCh und Art. 16 Abs. 1 AEUV verankerten Recht auf Schutz der personenbezogenen Daten sind der Union in Art. 16 Abs. 2 AEUV und für die Gemeinsame Außen- und Sicherheitspolitik in Art. 39 EUV Rechtssetzungsbefugnisse übertragen. Für Regelungen zur Verarbeitung personenbezogener Daten durch Unionsstellen sowie durch die Mitgliedstaaten bei der Ausübung von Tätigkeiten im Anwendungsbereichs des Unionsrechts bedarf es daher keines Rückgriffs auf die Kompetenz zur Harmonisierung des Binnenmarktes. Maßnahmen der Datensicherheit, soweit sie auf den Schutz personenbezogener Daten zielen, können demnach auf primärrechtliche Kompetenzen gestützt werden.

3. Europäisches Infrastrukturrecht

Die Schaffung transeuropäischer Netze ist für die Union ein Mittel zum Zweck der Verwirklichung des Binnenmarktes und der Stärkung des wirtschaftlichen, sozialen und territorialen Zusammenhalts. Die Union trägt daher zum Auf- und Ausbau der Telekommunikationsinfrastruktur bei, Art. 170 Abs. 1 AEUV. In Art. 171 Abs. 1 S. 1 AEUV ist in drei Spiegelstrichen festgelegt, wie die Zwecke umzusetzen sind. Auf Art. 171 AEUV (Art. 151 EGV a. F.) stützt sich die Verordnung (EG) Nr. 733/2002 zur Einführung der Domäne oberster Stufe „.eu“,[119] die auf europäischer Ebene im Internetnamensrecht einen regulatorischen Rahmen für die Verwaltung der europäischen Top-Level-Domain schafft. Die Verordnung führt „.eu“ als länderspezifische Domäne oberster Stufe (ccTLD) in die Union ein. Die TLDs sind Bestandteil der Infrastruktur des Internets. Ein Bezug zur Sicherheit besteht insofern, als die TLDs für die weltweite Interoperabilität des World Wide Web (www), einer wichtigen Nutzung des Internets, von wesentlicher Bedeutung sind. Die Interoperabilität der „europäischen Netze“ soll gemäß der Verordnung gefördert werden. Zusätzliche Namensserver würden sich „positiv auf die Topologie und die technische Infrastruktur des Internets in der Gemeinschaft auswirken“.[120] Die Verordnung betrifft im Übrigen jedoch nur die Bedingungen der Benennung und der Arbeit des sog. Registers. Diese Organisation schließt mit der ICANN einen Vertrag über die Delegierung der ccTLD „.eu“, um deren ordnungsgemäße Einbindung in das DNS zu gewährleisten.[121]

---

[119] Art. 151 EGV a. F.

[120] Erwägungsgrund 5 Verordnung (EG) Nr. 733/2002.

[121] Da die Domainverordnung keine technischen Hindernisse beseitigt, war sie umstritten, *Koenig/Neumann*, EuZW 2002, 485 (488); ferner *Mayer*, Europäisches Internetverwaltungsrecht, in: Terhechte (Hrsg.), Verwaltungsrecht in der Europäischen Union, 2011, § 25, Rn. 41.

Im europäischen Infrastrukturrecht bestehen demnach Regelungszugriffe auf die Infrastruktur des Internets. Ableitungen für informationsverwaltungsrechtliche Regelungen ergeben sich aus ihnen nicht.

4. Europäisches Katastrophenschutzrecht

Dem europäischen Katastrophenschutzrecht wird in der Sicherheitsarchitektur die Rolle eines tragenden Elements zugewiesen.[122] Nach Art. 222 Abs. 1 S. 2 a) 1. Var. AEUV mobilisiert die Union alle ihr zur Verfügung stehenden Mittel, einschließlich der von den Mitgliedstaaten bereitgestellten militärischen Mittel, um terroristische Bedrohungen im Hoheitsgebiet von Mitgliedstaaten abzuwenden. Bei weiter Auslegung könnte die Vorschrift bei Angriffen auf Internetinfrastrukturen zur Anwendung kommen. Die Kommission und der Hohe Vertreter der EU für Außen- und Sicherheitspolitik haben gemeinsam den Vorschlag für einen Beschluss des Rates gemäß Art. 222 Abs. 3 S. 1 AEUV über die Anwendung der Solidaritätsklausel durch die Union vorgelegt.[123] Der Beschluss soll gemäß Art. 2 lit. b bei Terroranschlägen auf Infrastrukturen Anwendung finden. Das Parlament machte vorab in Erwägung der Beistandsklausel des Art. 42 Abs. 7 EUV in einer Entschließung die Auffassung deutlich, dass Cyberangriffe gegen kritische Infrastrukturen unter die Klausel fallen könnten.[124] Im Vergleich mit dem Vorgängerentwurf des Beschlusses sind aber kritische Infrastrukturen im eigentlichen Sinne nun nicht mehr erfasst.[125] Lediglich in den Erwägungen zum Beschluss über ein Katastrophenverfahren in der Union wird gefordert, dass Synergien mit dem Europäischen Programm zum Schutz kritischer Infrastrukturen (EPCIP) und dem Gemeinsamen Informationsraum (CISE) genutzt werden sollten.[126] Die Netz- und Informationssicherheit von Internetinfrastrukturen spielt daher mit der bestehenden Beschlusslage nach Art. 222 Abs. 3 AEUV keine hervorgehobene Rolle.[127]

---

[122] *Reichenbach/Göbel/Wolff/Stokar von Neuforn* (Hrsg.), Risiken und Herausforderungen für die öffentliche Sicherheit in Deutschland, 2. Aufl. 2011; vgl. *Trute*, Katastrophenschutzrecht – Besichtigung eines verdrängten Rechtsgebiets, KritV 2005, 342 (342 ff.).

[123] Beschluss des Rates vom 24. Juni 2014 über die Vorkehrungen für die Anwendung der Solidaritätsklausel durch die Union (2014/415/EU), ABl. Nr. L 192 S. 53, ber. ABl. Nr. L 221 S. 26 und ABl. Nr. L 275 S. 7.

[124] Entschließung des Europäischen Parlaments vom 22. November 2012 zu den EU-Klauseln über die gegenseitige Verteidigung und Solidarität: politische und operationelle Dimensionen, 2012/2223(INI), Rn. 13.

[125] JOIN (2012) 39 final.

[126] Beschluss Nr. 1313/2013/EU des Europäischen Parlaments und des Rates vom 17. Dezember 2013 über ein Katastrophenschutzverfahren der Union, Erwägung 6.

[127] Die EU-Cybersicherheitsstrategie weist lediglich darauf hin, dass ein besonders

Im Übrigen könnte die europäische Katastrophenschutzkompetenz, Art. 196 AEUV, als sektorenübergreifende Kompetenz für unterstützende, ergänzende, fördernde und Kohärenz schaffende Maßnahmen der Risikovorsorge der Mitgliedstaaten herangezogen werden.[128]

5. Europäisches Statistikrecht

Das europäische Statistikrecht ist ein von der Rechtswissenschaft unterschätzter, aber unter der Fragestellung, ob und wie Informationen zu einem bestimmten Regelungsgegenstand generiert werden, durchaus zu berücksichtigender Bereich.[129] Auf Grundlage von Art. 338 AEUV können Maßnahmen für die Erstellung von Statistiken beschlossen werden, wenn diese für die Durchführung der Tätigkeit der Union erforderlich sind. Von der Ermächtigung hat die Union vor dem Hintergrund der Finanzkrise mit dem Erlass eines sekundärrechtlichen Rahmens zur Harmonisierung der öffentlichen Rechnungslegung und zur besseren Überwachung der Erfüllung öffentlicher Rechenschaftspflichten Gebrauch gemacht.[130] Informationsrechtliche Regelungen, die etwa die Generierung statistischer Informationen über Angriffe auf Netze und Informationssysteme betreffen, finden sich allerdings nicht.[131] Sie dürften nach Art. 338 AEUV aber zulässig sein und wären in Erwägung zu ziehen, soweit nicht spezialisierte Stellen wie die ENISA derartige Erhebungen durchführen.

6. Gewährleistung der Netz- und Informationssicherheit als Angelegenheit des Binnenmarktes

In Ermangelung eines eigenen Politikbereichs im dritten Teil des AEUV sind die maßgeblichen Regelungen zur Gewährleistung der Sicherheit von Netzen und Informationssystemen auf die Kompetenz zur Harmonisierung des Binnenmarktes gestützt.

Das telekommunikationsrechtliche Sekundärrecht,[132] die NIS-RL, die VO (EU) Nr. 526/2013 über die ENISA sowie die Verordnung (EU) Nr. 910/2014

---

schwerer „Cybervorfall oder -angriff" dazu führen könnte, dass ein Mitgliedstaat die Solidaritätsklausel des Art. 222 AEUV geltend macht, JOIN(2013) 1 final, S. 22.

[128] Dazu *Altwicker*, in: Gusy/Kugelmann/Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, 2017, S. 153.

[129] Vgl. *Heußner*, Informationssysteme im Europäischen Verwaltungsverbund, 2007, S. 126 ff.

[130] Richtlinie 2011/85/EU des Rates vom 8. November 2011 über die Anforderungen an die haushaltspolitischen Rahmen der Mitgliedstaaten; siehe auch COM(2013) 114 final.

[131] Die Aufgabe der Erstellung von Statistiken kommt wohl der ENISA zu, VO (EU) Nr. 526/2013, Erwägung 24.

[132] Siehe zuletzt Richtlinie 2009/140/EG des Europäischen Parlaments und des Rates vom

über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt haben die EU-Gesetzgeber auf Art. 114 AEUV gestützt. Die Robustheit und Stabilität der Netze sei „insbesondere für das Funktionieren des Binnenmarkts […] von entscheidender Bedeutung".[133] Die aus den unterschiedlichen Kapazitäten, Strategien und Schutzniveaus resultierenden Disparitäten im Bereich der Netz- und Informationssicherheit in den Mitgliedstaaten rechtfertigten ein harmonisierendes Tätigwerden der Union.

Das Heranziehen von Art. 114 AEUV als Kompetenzgrundlage für Maßnahmen betreffend die Netz- und Informationssicherheit ist dennoch problembehaftet. Gegen die Errichtungs-Verordnung der ENISA[134] wurde mit der Auffassung geklagt, die Rechtsgrundlage sei nicht geeignet und daher sei die Verordnung für nichtig zu erklären. Der Europäische Gerichtshof erkannte Art. 114 AEUV (Art. 95 EGV a. F.) jedoch als ausreichende Rechtsgrundlage zur Errichtung der Agentur an.[135] Aufgrund der technischen Komplexität von Netzen und Informationssystemen, der Vielfalt der zusammengeschalteten Produkte und der Vielzahl eigenverantwortlicher privater und öffentlicher Akteure durfte der Gesetzgeber annehmen, dass das reibungslose Funktionieren des Binnenmarktes durch eine heterogene Umsetzung der technischen Vorschriften, die in den die Netz- und Informationssicherheit betreffenden Richtlinien enthalten sind, gefährdet werden könnte. Der Gesetzgeber dürfe daher die Schaffung einer (Unions-)Einrichtung für notwendig erachten, deren Aufgabe es ist, in Situationen, in denen der Erlass von nicht zwingenden Begleit- und Rahmenmaßnahmen zur Erleichterung der einheitlichen Durchführung und Anwendung auf Art. 114 AEUV gestützter Rechtsakte geeignet erscheint, zum Harmonisierungsprozess beizutragen. Das dafür zu erfüllende Kriterium, dass die übertragenen Aufgaben in einem engen Zusammenhang mit den anzugleichenden Vorschriften zu stehen haben, sei für die der ENISA übertragenen Aufgaben erfüllt.

Auch mit Blick auf die in Art. 4 Abs. 2 S. 2 EUV enthaltene Staatsfunktionengarantie kann sich demnach europäisches Internetsicherheitsrecht grundsätzlich auf die Kompetenz zur Binnenmarktharmonisierung stützten.

---

25. November 2009 zur Änderung der Richtlinie 2002/21/EG über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste, der Richtlinie 2002/19/EG über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung und der Richtlinie 2002/20/EG über die Genehmigung elektronischer Kommunikationsnetze und -dienste.

[133] Erwägungsgrund 1 NIS-RL; allgemein *Gercke*, CR 2016, 28 (28 f.).

[134] Verordnung (EG) Nr. 460/2004.

[135] EuGH, Urteil vom 02.05.2006 – C-217/04 Vereinigtes Königreich Großbritannien und Nordirland/Europäisches Parlament u. a., Rn. 44 ff. mit kritischer Anmerkung von *Ohler*, EuZW 2006, S. 372 ff.

II. Sekundär- und einfachrechtlich erfasste Internetinfrastrukturen, Dienste, Anbieter und Verantwortliche sowie sonstige Quellen

Von den relevanten primärrechtlichen Ordnungsrahmen ausgehend können die durch europäisches Sekundärrecht und die einfachrechtlich adressierten privaten Betreiber, Anbieter Dienste, Verantwortliche und sonstige Quellen identifiziert werden, für die nicht nur materiell-rechtliche Sicherheitsvorgaben, sondern auch informationsverwaltungsrechtliche Bestimmungen zur Generierung von Informationen bestehen. Dies sind insbesondere Telekommunikationsnetzbetreiber und -diensteanbieter (1.), Betreiber wesentlicher Dienste (2.), Anbieter von digitalen Diensten und Telemedien (3.) sowie datenschutzrechtlich Verantwortliche (4.).

1. Telekommunikationsnetzbetreiber und -diensteanbieter sowie Over-the-Top-Kommunikationsdienste

Während sich die zur Signalübertragung erforderlichen Netzinfrastrukturen und Dienste weitgehend unproblematisch im Telekommunikationsrecht einordnen lassen (a), ist die regulierungsrechtliche Behandlung neuer Internetdienste wie Over-the-Top-Dienste noch nicht abschließend geklärt (b).

a) Europäisches Sekundärrecht und Einordnung im deutschen nationalen Recht

Das sekundärrechtliche Telekommunikationsrecht knüpft in Art. 1 Abs. 1 S. 1 der Rahmen-RL[136] an elektronische Kommunikationsdienste, elektronische Kommunikationsnetze sowie zugehörige Einrichtungen und zugehörige Dienste an. Die Begriffsbestimmungen in Art. 2 lit. a und c Rahmen-RL entsprechen weitgehend denen in § 3 Nr. 24 und Nr. 27 TKG. Ein Telekommunikationsdienst im Sinne des § 3 Nr. 24 TKG ist ein Dienst, der überwiegend in der Signalübertragung besteht. Die Gesamtheit von Übertragungssystemen und ggf. von Vermittlungs- und Leitwegeeinrichtungen sowie anderer Ressourcen sind Telekommunikationsnetze, zu denen nach § 3 Nr. 27 TKG auch paketvermittelnde Netze wie das Internet gehören. Sowohl im europäischen[137] als auch im deutschen Recht[138] ist demnach zwischen dem Transport der Kommunikationsdaten einerseits und dem Inhalt der Kommunikation andererseits zu unterscheiden. Dienste, deren Funktionsschwerpunkt nicht in der Signalübertragung zu verorten ist und die eine inhaltliche Leistung zum Gegenstand haben, können ungeachtet

[136] RL 2002/21/EG, zuletzt geändert durch RL 2009/140/EG.
[137] Vgl. auch Erwägungsgrund 5 RL 2002/21/EG.
[138] Vgl. § 1 TMG.

weiterer möglicher Einordnungen alternativ als Dienste der Informationsgesellschaft bzw. Telemedien eingeordnet werden.[139]

Dementsprechend kann auch das Internet nicht in seiner Gesamtheit in Kategorien Telekommunikationsnetz oder Telekommunikationsdienst eingeordnet werden. Es bietet sich dagegen an, das OSI/ISO-Schichtenmodell[140] zur telekommunikationsrechtlichen Einordnung heranziehen. Die Bitübertragungsschicht (*physical layer*), die Sicherungsschicht (*data link layer*) und die Vermittlungsschicht/Netzwerkschicht (*network layer*) können problemlos der Signalübertragung zugeordnet werden. Die Transportschicht (*transport layer*), in der Aufbau, Verwaltung und bbau von logischen Verbindungen stattfinden, kann noch der Signalübertragung zugezählt werden, auch wenn selbst aufgrund bestimmter Fehlerbehandlungsfunktionen für Daten zusätzlich ein inhaltlicher Aspekt gegeben ist.[141] Die Kommunikationsschicht (*session layer*) stellt Mittel bereit, die Kommunikation zu organisieren und zu synchronisieren, sodass hier die Signalübertragung nicht mehr den Vorgang dominiert. Die Darstellungsschicht (*presentation layer*) und die Anwendungsschicht (*application layer*) sind anwendungsorientiert, d. h., sie dienen nicht unmittelbar der Signalübertragung. Sie sind grundsätzlich nicht der Telekommunikation im Sinne des TKG zuzurechnen.

Die Begriffe Telekommunikationsnetz oder -dienste werden in den Vorschriften des TKG regelmäßig nicht isoliert verwendet. Sie stehen meist im Zusammenhang mit „Betreiber“ und „Diensteanbieter“ (vgl. § 109 TKG). Diese sind es, die als Quellen staatlicher Generierung von Informationen über die Netz- und Informationssicherheit in Betracht kommen.

b) Einordnung neuer Internetdienste wie Over-the-Top-Dienste

Besondere Fragen der rechtlichen Einordnung in die Struktur von Telekommunikations- und Telemedienrecht werfen vor allem Dienste auf, die auf dem Internetprotokoll (IP) basieren. Die Einordnung hat insbesondere auch Implikationen für die Informationsgenerierung. Ist das Telekommunikationsrecht auf einen neuartigen Dienst anwendbar, erweitert sich mit Blick auf die dadurch ebenfalls anwendbaren informationsverwaltungsrechtlichen Regelungen grundsätzlich die verfügbare sicherheitsbezogene Informationsbasis der Administrative.

---

[139] Siehe § 3 C. II. 3.; zur Einordnung von nichtmenschlicher Kommunikation, beispielsweise Kommunikation Maschine zu Maschine im Internet der Dinge, *Grünwald/Nüßing*, MMR 2015, 378 (397 ff.).

[140] Siehe § 2 B.

[141] *Schütz*, in: Geppert/Schütz (Hrsg.), BeckTKG, 4. Aufl. 2013, § 6 Rn. 36 f.

Die Relevanz und die Folgen der gesetzlichen Zuordnung lassen sich am Beispiel der sog. Over-the-Top-Telekommunikationsdienste darstellen. Im Kern geht es um die Frage, ob neben den klassischen Telekommunikationsanbietern auch Over-the-Top-(OTT-)Anbieter von E-Mail-Übertragungsdiensten und Messenger-Diensten oder Voice-over-IP-Anbieter (VoIP) den Pflichten des TKG unterfallen.[142] Sind diese Dienste als Telekommunikationsdienste im Sinne des TKG zu qualifizieren, unterliegen OTT-Dienste zum einen der Aufsicht durch die Bundesnetzagentur und zum anderen ist das sicherheitsrechtliche Pflichtenprogramm samt der informationsverwaltungsrechtlichen Vorschriften anzuwenden.[143]

OTT-Dienste kennzeichnet, dass sie auf dem für alle Anwender offenen Internet auf Basis des Internet-Protokolls (IP) erbracht werden (*over the top*).[144] Abzugrenzen sind OTT-Kommunikationsdienste von OTT-Inhaltsdiensten. Bei den Kommunikationsdiensten steht die Individual- und Gruppenkommunikation im Vordergrund, bei den Inhaltsdiensten die inhaltliche Leistung.[145] Telekommunikationsrechtlich problematisch sind vor allem OTT-Kommunikationsdienste, da sie entweder als die Kommunikationsdienste der TK-Anbieter komplementierend oder erweiternd oder als Substitute für traditionelle Telefonie- und Kommunikationsdienste zu betrachten sind. Als Besonderheit kommt hinzu, dass OTT-Dienste tendenziell mehr gebündelte Leistungen anbieten. Die Anbieter streben häufig ein Leistungsbündel an, um verschiedene Funktionen auf einer Plattform zu integrieren. Informationstechnisch werden alle OTT-Dienste auf der Anwendungsschicht im Sinne des TCP/IP-Schichtenmodells realisiert. Dabei werden sowohl offene, standardisierte Anwendungsprotokolle (E-Mail) als

---

[142] Hintergrund der Debatte sind die regulatorischen Belastungen der etablierten Anbieter gegenüber den nicht regulierten Internetdienstanbietern und die damit einhergehende erschwerte Anpassung der Geschäftsmodelle. Gefordert wird ein regulatorisches „Level-Playing-Field". Siehe *Monopolkommission*, Sondergutachten 68, Wettbewerbspolitik: Herausforderung digitale Märkte, 2015, Rn. 544; eine Übersicht über die wichtigen OTT-Dienste einschließlich deren Sicherheitsstandards bietet Electronic Frontier Foundation, Secure Messaging Scorecard, abrufbar unter: https://www.eff.org/secure-messaging-scorecard.

[143] Vgl. *Grünwald*/*Nüßing*, MMR 2016, 91 (91 ff.); *Kühling*/*Schall*, CR 2015, 641 (654), die darauf hinweisen, dass aus der Erfassung als Telekommunikationsdienst nicht folgt, dass sämtliche telekommunikationsrechtlichen Regelungen anwendbar wären; vgl. auch die Vorhaben der Kommission zu „bedarfsgerechten Telekommunikationsvorschriften" Kommission, Strategie für einen digitalen Binnenmarkt in Europa, COM(2015) 192 final, S. 11 f.

[144] Dazu *Raabe*/*Dinger*/*Hartenstein*, K&R 2007, Beihefter 1, 1 (4, 6).

[145] Zur Behandlung von Mischdiensten im Allgemeinen und von Cloud Storage und Cloud Collaboration im Besonderen *Kremer*/*Völkel*, CR 2015, 501 (505), die für Letztere das Vorliegen von Telemedien annehmen; ferner zur Abgrenzung gegenüber Inhaltsdiensten *Heun*, Einführung: Grundlagen und Struktur des TKG, Marktzutritt und Übergangsrecht, in: *Heun* (Hrsg.), Handbuch Telekommunikationsrecht, 2. Aufl. 2015, Rn. 46 ff.

auch proprietäre, nicht offengelegte Anwendungsprotokolle verwendet. Gemeinsam ist den OTT-Diensten aber, dass sie die übertragenen Informationen und die Kommunikation der Nutzer über einen Port in die bzw. aus der unterhalb der Anwendungsschicht liegenden Transport- und Internetschicht (IP) ein- oder ausleiten.[146] OTT-Kommunikationsdienste können eine Client-Server- oder eine Peer-to-Peer-Architektur aufweisen, d. h. eine Ressource oder ein Dienst wird von einem Server bereitgehalten bzw. ausgeführt oder jeder Benutzer kann zeitgleich Ressourcen bereithalten und abrufen.

Für die telekommunikationsrechtliche Erfassung stellen sich nun Probleme sowohl im sachlichen als auch im persönlichen Anwendungsbereich. Sachlich ist der Anwendungsbereich eröffnet, wenn ein „öffentlich zugänglicher Telekommunikationsdienst" bzw. ein „öffentliches Telekommunikationsnetz" angeboten oder betrieben wird. Persönlich müssen die OTT-Dienste als „Anbieter" oder „Betreiber" zu qualifizieren sein.[147] Grundlegend ist die Frage, ob OTT-Dienste als Dienste im Sinne von Art. 2 lit. c) Rahmen-RL und § 3 Nr. 24 TKG anzusehen sind, die in der Regel gegen Entgelt erbracht werden und die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen. Von vorneherein ausgenommen sind nach Art. 2 lit. c) Rahmen-RL Dienste, die Inhalte anbieten oder eine redaktionelle Kontrolle über sie ausüben. Überdies nicht dazu gehören die Dienste der Informationsgesellschaft im Sinne von Art. 1 RL 98/34/EG, die nicht ganz oder überwiegend in der Übertragung der elektronischen Kommunikationsnetze bestehen. Wegen der Bündelung von Kommunikationsdiensten kann häufig nicht eindeutig bestimmt werden, ob im Schwerpunkt ein Inhaltsdienst (Audio, Video usw.) vorliegt.

Zur Beurteilung dieser Mischdienste kommen drei Ansätze in Betracht:[148] die Gesamtbetrachtung des Leistungsbündels, [149] die entgegengesetzte funktionale Betrachtung[150] und eine vermittelnde Ansicht, die danach fragt, ob bei technisch möglicher Separierung ein Leistungsbündel als wirtschaftliche Einheit betrachtet werden kann.[151]

---

[146] *Kühling*/*Schall*, CR 2015, S. 641 (644).

[147] § 3 Nr. 24 TKG. Siehe *Säcker*, in: ders. (Hrsg.), TKG, 3. Aufl. 2013, § 3 Rn. 61.

[148] Vgl. *Kühling/Schall/Biendl*, Telekommunikationsrecht, 2. Aufl. 2014, Rn. 126.

[149] Das ist der Ansatz der schwedischen Regulierungsbehörde *PTS*, Which services and networks are subject to the Electronic Communications Act?, 2009, S. 26. Bei einem E-Mail-Anbieter können etwa der E-Mail-Empfang, -Versand, die Verwaltung samt Speicherung, die Informationsdienste auf der Webseite usw. zusammen betrachtet werden.

[150] *Säcker*, in: Säcker (Hrsg.), TKG, 3. Aufl. 2013, § 3 Rn. 62a; *Holznagel*/*Schumacher,* in: Geppert/Schütz (Hrsg.), BeckTKG, 4. Aufl. 2013, Einl. C, Rn. 20. *Koenig*/*Neumann*, K&R 2004, Beilage 3, S. 1 (9).

[151] *Martini*/*von Zimmermann*, CR 2007, 427 (428); *Kühling*/*Schall*/*Biendl*, Telekommuni-

Gute Gründe sprechen auch dafür, die im Einzelnen aufgrund der Technik sehr schwierig zu subsumierenden telekommunikationsrechtlichen Voraussetzungen des Art. 2 lit. c Rahmen-RL bzw. § 3 Nr. 24 TKG für OTT-Dienste als erfüllt anzusehen. Dies sind insbesondere die Entgeltlichkeit der Diensteerbringung, das Überwiegen der Signalübertragung des Dienstes, die öffentliche Zugänglichkeit des Dienstes sowie die Anbietereigenschaft von OTT-Akteuren.[152]

Einer abschließenden Bewertung bedarf es hier nicht. Für eine Einordnung der OTT-Dienste als Telekommunikationsdienste spricht jedoch die epistemische Implikation, welche die Anwendbarkeit des sicherheitsrelevanten Informationsverwaltungsrechts nach sich zieht.[153]

Die Gewährleistungsverantwortung der Europäischen Union für die Internetsicherheit kann als normativer Anknüpfungspunkt einer unionsrechtlich gebotenen Berücksichtigung der kognitiven Dimension telekommunikationsrechtlicher Aufgabenerfüllung herangezogen werden. Da der staatliche Schutzauftrag durch einen Maßnahmenmix erfüllt werden kann, kommt für den nationalen Gesetzgeber die Mitwirkung an der Weiterentwicklung des Rechtsrahmens hinsichtlich der OTT-Dienste in Betracht.[154] Die Mitgliedstaaten könnten bei der Entscheidung über die künftige Regulierung von OTT-Diensten in die Abwägung einfließen lassen, dass dasjenige Regulierungsregime gelten soll, welches aus informationsverwaltungsrechtlicher Sicht am ehesten verspricht, in angemessenem Umfang sicherheitsbezogene Informationen zu generieren. Der Handlungsspielraum der Mitgliedstaaten in der Rechtssetzung der Union ist zwar naturgemäß auf die Mitwirkung begrenzt (vgl. Art. 16 Abs. 2 EUV), eine rechtliche Grenze der staatlichen Schutzaufträge ist darin aber nicht zu sehen. Die Schutzpflichten enden

---

kationsrecht, 2. Aufl. 2014, Rn. 126. *Kremer*/*Völkel*, CR 2015, 501 (504); a. A. *Holznagel*/*Schumacher,* in: Geppert/Schütz (Hrsg.), BeckTKG, 4. Aufl. 2013, Einl. C, Rn. 24.

[152] *Kühling*/*Schall*, CR 2015, 641 (641 ff.).

[153] In der deutschen Rechtsprechung zeichnet sich zu Recht ab, OTT-Dienste entgegen der technischen Auffassung der Kommission als elektronische Kommunikationsdienste im Wege der funktional-wertenden Betrachtung im Sinne des Art. 2 lit. c Rahmen-RL einzuordnen, VG Köln, Urteil vom 11.11.2015, Az: 21 K 450/15. Das Gericht hat die Sprungrevision zum Bundesverwaltungsgericht zugelassen. Das Gericht sah den von Google betriebenen E-Mail-Dienst Gmail als Telekommunikationsdienst im Sinne des TKG an. Zustimmend *Kühling*/*Schall*, CR 2016, 185 (185 ff.); kritisch *Gersdorf*, K&R 2016, 91 (91 ff.); *Schuster*, CR 2016, 173 (173 ff.). Die Frage wird erneut im Rahmen der Überprüfung des europäischen Rechtsrahmens für Telekommunikation virulent, siehe zu den Konsultationen im Zuge des TK-Review *Kommission*, Background to the Public Consultation – On the Evaluation of the Regulatory Framework for Electronic Communications and on its Review, 11.09.2015; vgl. auch *Monopolkommission*, Sondergutachten 66, Telekommunikation 2013: Vielfalt auf den Märkten erhalten, 2013, Rn. 10, 52, 139 ff.

[154] *Schliesky*/*Hoffmann*/*Luch*/*Schulz*/*Borchers*, Schutzpflichten und Drittwirkung im Internet, 2014, S. 159.

grundsätzlich erst dann, wenn die Unmöglichkeit beginnt (*ultra posse nemo obligatur*).[155] Die EU ist in Einklang mit dem in Art. 5 EUV verankerten Subsidiaritätsprinzip im Verhältnis zu den Mitgliedstaaten die Ebene, die vorrangig in dieser Frage einzugreifen hat. Der transnationale Charakter des Internets macht die Sicherheit ebenfalls zu einer transnationalen Angelegenheit. Der Zulässigkeit eines solchen Arguments stehen auch nicht die telekommunikationsrechtlichen Regulierungsziele entgegen. Nach § 1 TKG und § 2 Abs. 2 Nr. 2 TKG ist vor allem die Sicherstellung eines chancengleichen Wettbewerbs unter Anwendung eines technologieneutralen Ansatzes ein mit der Regulierung verfolgtes Ziel. Die Wahrung der Interessen der öffentlichen Sicherheit zählt allerdings nach § 2 Abs. 2 Nr. 9 TKG ebenfalls dazu. Den Regulierungszielen kann als Leitprinzipien ermessenseinschränkende und ermessenslenkende Bedeutung zukommen[156] und in der Anwendung des TKG bei Zweifels- und Streitfragen herangezogen werden.[157] Somit kann es geboten sein, im Sinne der Informationsgenerierung das Telekommunikationsrecht oder eine entsprechende Regulierung auf OTT-Dienste anzuwenden bzw. für diese einzuführen.

2. Betreiber wesentlicher Dienste und kritischer Infrastrukturen

Als Kernelement der europäischen Cybersicherheitsstrategie hat die Kommission 2013 die „Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit" (NIS-RL) vorgeschlagen,[158] die am 06.07.2016 vom Europäischen Parlament in zweiter Lesung angenommen wurde.[159] Die NIS-RL schaffte erstmals als Begleitmaßnahme zur Digitalisierung des Binnenmarktes umfassend Pflichten für einen Mindeststandard für die Sicherheit sowie Meldepflichten.[160] Die Richtlinie legt Maßnahmen zur Ge-

---

[155] Zur Geltung dieses Grundsatzes auch für die Schutzpflichten *Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, 2005, S. 105.

[156] *Säcker*, in: ders. (Hrsg.), TKG, 3. Aufl. 2013, § 2 Rn. 1.

[157] *Schuster*, in: Geppert/Schütz (Hrsg.), BeckTKG, 4. Aufl. 2013, § 2 Rn. 36.

[158] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union; dazu *Beucher*/*Utzerath*, MMR 2013, 362 (362 f.); *Gercke*, CR 2016, 28 (28 ff.); *Schallbruch*, CR 2016, 663 (663 ff.).

[159] Europäisches Parlament, Pressemitteilung vom 06.07.2016, REF : 20160701IPR34481; Beschlussgrundlage 2013/0027 (COD). Die Richtlinie tritt am 20. Tag nach der Veröffentlichung im Amtsblatt in Kraft.

[160] Einen europäischen Rechtsrahmen bietet bereits die Richtlinie 2008/114/EG des Rates über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern. Ein übergreifendes Gesamtkonzept bietet das „Europäische Programm für den Schutz kritischer Infrastrukturen" (EPCIP), KOM(2006) 786, das hauptsächlich ein Verfahren zur Ermittlung und Ausweisung kritischer

währleistung einer hohen gemeinsamen Sicherheit von Netz- und Informationssystemen in der Union fest (Art. 1 Abs. 1 NIS-RL). Die Mitgliedstaaten haben für diese Zwecke der NIS-RL Vorkehrungen gegen Cyberangriffe zu treffen und die europäische Kooperation auf diesem Gebiet zu verstärken. Vom Anwendungsbereich der NIS-RL erfasst sind Betreiber wesentlicher Dienste *(essential services*), Art. 1 Abs. 2 lit. d NIS-RL.[161] Diese sind den Sektoren Energie, Transport, Banken, Finanzdienstleister, Gesundheit, Wasserversorgung und digitale Infrastruktur zuzuordnen. Die Mitgliedstaaten haben nach den lediglich grob vorgegebenen Kriterien die Betreiber wesentlicher Dienste zu ermitteln (Art. 5 NIS-RL).

Parallel zur NIS-RL wurde in Deutschland das IT-Sicherheitsgesetz als Artikelgesetz[162] vorgeschlagen, das vor der NIS-RL in Kraft trat.[163] Die Novellierung des BSIG verwendet zwar nicht den Begriff „wesentliche Dienste", führt aber Regelungen für sog. kritische Infrastrukturen ein. Dabei wurde der Begriff erstmals verrechtlicht und legaldefiniert.[164] Die Vorgaben für Betreiber kritischer Infrastrukturen entsprechen grundsätzlich denen, die die NIS-RL für Betreiber wesentlicher Dienste vorsieht.

Kritische Infrastrukturen sind nach § 2 Abs. 10 BSIG Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öf-

---

Infrastrukturen und komplementäre, informelle Maßnahmen zum Schutz der Infrastrukturen vorsieht. Ein verpflichtendes Meldeverfahren oder formalisierte Kooperations- oder Reaktionsmechanismen bei Sicherheitsvorfällen sieht dieses Programm aber nicht vor.

[161] Vgl. Art. 14 und 15a der konsolidierten Entwurfsfassung der NIS-RL vom 18.12.2015, 15229/15 Rev. 2.

[162] Bei dem IT-Sicherheitsgesetz handelt es sich um ein sog. Mantel- oder auch Artikelgesetz, d. h., es werden mit einem einzigen Rechtsetzungsakt verschiedene Gesetze geändert, neu geschaffen oder aufgehoben, die in einem Sachzusammenhang, hier der IT-Sicherheit, stehen. Siehe *Bundesministerium für Justiz*, Handbuch der Rechtsförmlichkeit, 3. Aufl. 2008, abrufbar unter: http://hdr.bmj.de/page_d.4.html.

[163] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015, BGBl. I S. 1324.

[164] Allerdings zählt in § 2 Abs. 2 Nr. 3 S. 4 ROG der Schutz kritischer Infrastrukturen zu den Grundsätzen der Raumordnung, denen Rechnung zu tragen ist. Nach § 17 Abs. 1 Nr. 3 des Zivilschutz- und Katastrophenhilfegesetzes darf das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe Angaben, einschließlich personenbezogener Daten, über „Infrastrukturen, bei deren Ausfall die Versorgung der Bevölkerung erheblich beeinträchtigt wird (kritische Infrastrukturen)", erheben. Dazu *Kahrl*, DÖV 2009, 535 (536).

fentliche Sicherheit eintreten würden.[165] Die Definition der kritischen Infrastrukturen schließt weitgehend die durch NIS-RL erfassten wesentlichen Dienste ein (Art. 4 Nr. 4 in Verbindung mit Art. 5 Abs. 2 NIS-RL). Aus Art. 4 Nr. 4 NIS-RL, nicht hingegen aus dem BSIG, geht hervor, dass zu den kritischen Infrastrukturen auch öffentliche Einrichtungen zu zählen sind.

Welche Einrichtungen, Anlagen oder Teile der Infrastrukturen in den genannten Sektoren als kritische Infrastrukturen gelten sollen, wird durch eine Rechtsverordnung unter den Voraussetzungen des § 10 Abs. 1 BSIG festgelegt. In methodischer Hinsicht wird die Kritikalität nach den Kriterien Qualität und Quantität bestimmt.[166] Als Arten wesentlicher digitaler Infrastrukturen gibt die NIS-RL in Anhang II Nr. 7 Internet-Knoten (Internet Exchange Points – IXPs), Domain-Name-System-(DNS-)Diensteanbieter und Top-Level-Domain-(TLD-) Name-Registrys vor.

Internet-Knoten sind die Knotenpunkte des Internets, über die verschiedene autonome Systeme zusammengeschaltet werden. Die IXPs dienen nicht selbst dem Transport des Internetverkehrs, sondern dem Austausch zwischen unterschiedlichen Providern.[167] Die Kritikalität beurteilt sich nach der Anzahl der zusammengeschalteten Netze. Die Kritis-VO[168] stuft die Betriebsanlagen des IXPs gemäß § 5 Abs. 4 in Verbindung mit Anhang 4 Teil 3 Nr. 1.3.1 als kritisch ein.

DNS-Diensteanbieter bieten Dienste an, mit deren Hilfe Domainnamen in die für die technische Abwicklung des Verkehrs nötigen IP-Adressen umgewandelt werden.[169] Die Kritikalität bemisst sich anhand der Anzahl der beauskunfteten

---

[165] Vgl. Definition des *Bundesministeriums des Innern*, Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), Stand: 17.06.2009, S. 3; vgl. *Kahrl*, DÖV 2009, 535 (535 ff.); zur rechtspolitischen Kritik daran, dass der Bereich Kultur und Medien nicht als kritischer Sektor erfasst ist, und mit der Forderung, dass eine Regulierung ähnlich wie zwischen dem TMG und RFStV anhand von Inhalten, nicht aber nach der Technik erfolgen müsse, *Spindler*, CR 2016, 297 (298).

[166] BT-Drs. 18/4096, S. 38. Mit dem Kriterium der Qualität wird methodisch die Frage beantwortet, ob Infrastrukturen eine für die Gesellschaft kritische Dienstleistung erbringen, und mit dem Kriterium der Quantität wird gefragt, ob ein Ausfall oder eine Beeinträchtigung wesentliche Folgen für wichtige Schutzgüter und die Funktionsfähigkeit des Gemeinwesens hätten. Zur Frage der verfassungsrechtlich gebotenen Bestimmtheit der Norm hinsichtlich der Verweisung und der Bestimmung kritischer Infrastrukturen durch branchenspezifische Schwellenwerte *Leisterer*/*Schneider*, CR 2014, 573 (577); *Roth*, ZD 2015, 17 (19); *Guckelberger*, DVBl. 2015, 1213 (1217); für die Debatte über die Bestimmung kritischer Infrastrukturen durch den Erlass einer Verordnung siehe 110. Sitzung des Deutschen Bundestages, 12.06.2015, PlPr. 18/110, S. 10572 ff.

[167] Art. 4 Nr. 3 in Verbindung mit Erwägungsgrund 82 NIS-RL.

[168] Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung) vom 22. April 2016, BGBl. I S. 958.

[169] Vgl. Art. 4 Nr. 15 NIS-RL.

bzw. verwalteten Domains. Die Kritis-VO erfasst ebenfalls DNS-Diensteanbieter, teilt diese indes gemäß § 5 Abs. 4 in Verbindung mit Anhang 4 Teil 3 Nr. 1.4 in zwei kritische Dienste auf, nämlich DNS-Resolver für das Auflösen von Domainnamen in IP-Adressen und autoritative DNS-Server, die vergebene Domainnamen nachweisen.

TLD-Name-Registrys sind Bestandteil des hierarchisch unterteilten Domain-Name-Systems und verwalten die Domainnamen auf der obersten Ebene (Top Level). Alle TLD-Name-Registries sind als kritisch anzusehen. Die Kritis-VO nennt diese Untergruppe des Domain-Namen-Systems nicht, erfasst diese aber implizit durch die Aufnahme der autoritativen DNS-Server.[170]

Die Kritis-VO geht über die in der NIS-RL genannten Einrichtungsarten hinaus. Zusätzlich als kritische Internetinfrastrukturdienste sind aus dem Sektor Informationstechnik und Telekommunikation neben Anlagen und Diensten, die der Vermittlung und der Steuerung dienen, auch Sprach- und Übertragungsdienste, die den Zugang (Telekommunikationsnetze), die Übertragung (Telekommunikationslinien, Übertragungswege, Standortkopplung) sowie IP-Registrierungsdatenbanken als weitere kritische Anlagenkategorien identifiziert. Aus dem Bereich Datenspeicherung und -verarbeitung sind insbesondere Housing (Rechenzentren), IT-Hosting (Serverfarm, Content Delivery Networks) und Vertrauensdienste (Trust Center) erfasst. Da die NIS-RL für die wesentlichen Dienste gemäß Art. 3 nur von einer Mindestharmonisierung ausgeht und es den Mitgliedstaaten erlaubt, ein höheres Sicherheitsniveau zu erreichen, steht die Richtlinie weitergehenden nationalen Bestimmungen nicht entgegen.[171]

Ein verbleibendes „Delta" zwischen bedeutenden Internetinfrastrukturen und telekommunikationsrechtlich mangels Kommunikation nicht erfassten Infrastrukturen wird durch die NIS-RL und das BSIG in Verbindung mit der Kritis-VO für kritische Infrastrukturen zu einem wichtigen Teil geschlossen.

---

[170] *Schallbruch*, CR 2016, 663 (665).

[171] Die Kritis-VO sieht gemäß § 5 Abs. 4 in Verbindung mit Anhang 4 Teil 3 Nr. 2.3. auch Anlagen zur Erbringung von Vertrauensdienten als kritische Infrastrukturen im Sektor Informationstechnik und Telekommunikation an. Die NIS-RL nimmt jedoch gemäß Art. 1 Abs. 3 NIS-RL Vertrauensdienste von den Sicherheitsanforderungen und informationsverwaltungsrechtlich relevanten Meldepflichten aus, da Vertrauensdienste Gegenstand der VO (EU) Nr. 910/2014 sind, die in Art. 19 auch Sicherheitsanforderungen statuiert. Zwar dürfte für die deutsche Konkretisierung insofern Raum sein, als die Kritis-VO von „Anlagen" spricht. Vorrang hat aber nach Art. 1 Abs. 7 NIS-RL sektorspezifisches Unionsrecht, sofern mindestens gleichwertige Anforderungen an die Sicherheit der Netz- und Informationssysteme gestellt werden oder die Meldung von Sicherheitsvorfällen gewährleistet wird.

3. Anbieter digitaler Dienste und Telemedien

Eine „Schlüsselstellung für die Sicherheit" im Cyberspace nimmt eine Vielzahl von Informations- und Kommunikationsdiensten im Internet ein, auch wenn sie hinsichtlich quantitativer Bedeutung und Versorgungsgrad nicht als wesentlich einzustufen sind.[172]

Aus diesem Grund bezieht die NIS-RL in ihren Anwendungsbereich auch Anbieter sog. digitaler Dienste (*digital services*) mit ein, Art. 16 NIS-RL. Digitale Dienste sind Dienste der Informationsgesellschaft im Sinne des Art. 1 b) der RL (EU) 2015/1535, d. h. jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung. Der Unionsgesetzgeber hat die von der NIS-RL umfassten Arten digitaler Dienste über einen Verweis auf den Anhang enumerativ aufgeführt. Art. 4 Nr. 5 in Verbindung mit Anhang III NIS-RL beschränkt den sachlichen Anwendungsbereich auf Online-Marktplätze, Online-Suchmaschinen und Cloud-Computing-Dienste.

Die von der NIS-RL einbezogenen digitalen Dienste können grundsätzlich als Telemedien im Sinne des TMG eingeordnet werden, für die auch die Sicherheitsverpflichtungen des § 13 Abs. 7 TMG gelten.[173] Nach der Negativdefinition des § 1 Abs. 1 TMG sind unter Telemedien Informations- und Kommunikationsdienste zu verstehen, soweit sie nicht ausschließlich Telekommunikationsdienste nach § 3 Nr. 24 TKG darstellen, d. h., soweit sie nicht ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen oder telekommunikationsgestützte Dienste nach § 3 Nr. 25 TKG sind.

Das TMG geht über die nur „ausschnitthafte Erfassung des Cyberspace" im Anwendungsbereich der NIS-Richtlinie hinaus. Unter den Begriff des Telemediendiensteanbieters lassen sich nämlich vier verschiedene Provider-Typen fassen (vgl. § 2 Nr. 1 TMG): Content-Provider, Host-Provider, Access-Provider und Cache-Provider.[174] Content-Provider bieten eigene Inhalte zum Abruf im Internet bereit. Ein Host-Provider stellt ein System für Dritte, zum Beispiel zum Speichern fremder Inhalte, zur Verfügung. Access-Provider vermitteln mit Hilfe einer technischen Infrastruktur wie zum Beispiel einem Rechenzentrum den Zugang zu den Inhalten. Cache-Provider vermitteln den beschleunigten Zugang zu Inhalten durch Zwischenspeicherung fremder Inhalte. In persönlicher Hin-

---

[172] Vgl. BT-Drs. 18/4096, S. 2; *Gerlach*, CR 2015, 581 (581).

[173] *Schallbruch*, CR 2016, 663 (664).

[174] *Bundesamt für Sicherheit in der Informationstechnik*, Empfehlung Internet-Dienstleister, Diskussionspapier: Absicherung von Telemediendiensten, 2016, S. 1 (1 f.); vgl. auch die Unterscheidung der Providertypen bei *Hartmann*, Unterlassungsansprüche im Internet, 2009, S. 12; *Djeffal*, MMR 2015, 716 (717).

sicht können die Rollen in einer natürlichen oder juristischen Person zusammenfallen oder einzelne Rollen an andere Unternehmen ausgelagert werden. Als Telemedien sind im Gegensatz zur NIS-Richtlinie folglich auch Betreiber vom Webseiten, Soziale Netzwerke und andere Plattformen als Anbieter eigener oder fremder Inhalte oder als Zugangsvermittler erfasst. Den Mitgliedstaaten ist es auch erlaubt, weitere und strengere Anforderungen an solche Diensteanbieter zu stellen, da sich das Verbot von Zusatzpflichten in Art. 16 Abs. 10 NIS-RL nur auf die in der NIS-Richtlinie genannten Arten digitaler Dienste bezieht.

Haben Anbieter digitaler Dienste keine Niederlassung in der Union, bieten sie aber Dienste im Sinne der NIS-Richtlinie an, müssen sie gemäß Art. 18 Abs. 2 NIS-RL einen Vertreter in einem Mitgliedsstaat benennen, dessen gerichtlicher Zuständigkeit sie unterliegen. Demnach kommt es nicht auf den physischen Standort der Netz- und Informationssysteme an.[175]

4. Verantwortliche im Sinne des Datenschutzrechts

Ein großer Teil der Nutzer des Internets verarbeitet personenbezogene Daten und nutzt das Internet für deren Übermittlung. Über das Internet können auch Anlagen und Einrichtungen angesteuert werden, die solche Daten speichern. Das Datenschutzrecht schützt personenbezogene Daten. Es regelt jedoch nicht nur die Voraussetzungen der Datenverarbeitung, sondern stellt auch Anforderungen an die Datensicherheit personenbezogener Daten.[176] Adressaten dieser Sicherheitspflichten sind die datenschutzrechtlich Verantwortlichen. Nach dem weitesten Verständnis sind Verantwortliche alle natürlichen oder juristischen Personen, Behörden oder anderen Stellen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden (Art. 4 Nr. 7 DS-GVO). Wegen der Bedeutung des Datenschutzes für die Internetsicherheit sind daher auch die datenschutzrechtlich Verantwortlichen wichtige Quellen für die Gewinnung von sicherheitsrelevanten Informationen.

D. Rechtsgrundlagen zur Generierung von Informationen über die Sicherheit von Netzen und Informationssystemen

Nachdem untersucht wurde, welche privaten Akteure zur Generierung von Informationen in Betracht kommen, ist der Weg für die Frage geebnet, welche Informationen erhoben werden können. Dazu sind diejenigen Rechtsgrundla-

---

[175] Vgl. Erwägungsgründe 64 f. NIS-RL.

[176] Art. 17 der RL 95/46/EG bzw. Art. 32 DS-GVO; Art. 4 der RL 2002/58/EG, zuletzt geändert durch RL 2009/136/EG.

gen zu ermitteln, aus denen sich ergibt, dass die Diensteanbieter und Infrastrukturbetreiber den NIS-Behörden sicherheitsrelevante Informationen beibringen oder aufgrund derer die NIS-Behörden die Befugnis haben, Informationen zu erheben. Zu bestimmen ist dabei jeweils der Verpflichtungsgehalt der betreffenden Rechtsgrundlage, der die Art und den Umfang der generierbaren Informationen bemisst, da die Bestimmtheit einer Informationspflicht zugleich ein Indikator für die Gestaltungsmöglichkeit der Verwaltung ist.[177]

Ein Großteil der administrativen Informationsverarbeitung wird durch faktische und nicht durch normativ vorgegebene Informationsbeziehungen realisiert. Diese sind von den formal-rechtlich geordneten Informationsbeziehungen zu unterscheiden.[178] Der Vorteil vorrechtlicher Informationsbeziehungen ist naheliegend. Informelle Strukturen sind offener für Veränderungen der Umwelt und im Allgemeinen anpassungsfähiger als formell geregelte. Im Folgenden können die vorrechtlichen Informationsbeziehungen zwischen den Akteuren jedoch schon mangels erheblicher empirischer Befunde nicht untersucht werden. Ohnehin gilt für die Sicherheitsverwaltung das in Art. 2 EUV und Art. 20 Abs. 3 GG verankerte Rechtsstaatsgebot. Es gelten die darin zu verortenden Prinzipien des Vorbehalts und des Vorrangs des Gesetzes. Ein Grundsatz nach Art von *Gratians* Decretum des *necessitas non habet legem* gilt nicht.[179] Die Betrachtung der rechtlichen Ausgestaltung ist umso mehr geboten, als staatliche Maßnahmen dann nicht frei sind, wenn sie grundrechtssensibel sind. Wurde früher die staatliche Informationsbeschaffung noch als grundrechtsneutral angesehen, weil Grundrechtseingriffe mit imperativen Geboten, Verboten und Zwangsmaßnahmen definiert wurden, ist mit der modernen Grundrechtsdogmatik die Gewinnung von Informationen über IT-Sicherheit oder zum Zwecke der IT-Sicherheit in weiten Teilen als Grundrechtseingriff zu qualifizieren.[180] Die Informationsverarbeitung ist nicht nur für den Schutz personenbezogener, sondern auch für

---

[177] *Schmidt-Aßmann*, Strukturen europäischer Verwaltung und die Rolle des Europäischen Verwaltungsrechts, in: Blankenagel/Pernice/Schulze-Fielitz (Hrsg.), Verfassung im Diskurs der Welt, 2004, S. 395 (406).

[178] *Holznagel*, Informationsbeziehungen in und zwischen Behörden, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band II, 2. Aufl. 2012, § 24 Rn. 7, 8.

[179] Zu dieser Regel *Lauta*, Disaster Law, 2015, S. 57; zur Rolle informeller Governance außerhalb formalisierter Regelungsstrukturen und zur „Entformalisierung staatlichen Handelns" ausführlich *Schoch*, Entformalisierung staatlichen Handelns, in: Isensee/Kirchhof (Hrsg.), HbStR, Band III, 3. Aufl. 2005, § 37 Rn. 22 ff., insb. 28, 93.

[180] Zur Entwicklung der Eingriffsdogmatik bis zum Volkszählungsurteil, BVerfGE 65, 1; ferner *Gusy*, VerwArch 1983, 91 ff.; *ders*., in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, Vorbemerkung BNDG Rn. 6; zur Zugriffsproblematik *Ladeur*, Der Staat gegen die Gesellschaft, 2006, S. 119 ff., 320 ff.

den unternehmensbezogener Daten und hinsichtlich technischer Informationen relevant. In diesem Zusammenhang kommt dem Informationsrecht die Aufgabe zu, durch „Normierung der Datenströme und -operationen“[181] die Bedingungen und Voraussetzungen für eine Informationskontrolle und organisierte Transparenz des Systems zu schaffen.

Bei der Informationsgenerierung kommt ein aus dem klassischen Verwaltungsverfahren bekannter allgemeiner Amtsermittlungsgrundsatz, wie er in § 24 VwVfG enthalten ist, bei Verfahren, die keinen Verwaltungsakt bedingen, grundsätzlich nicht zur Anwendung.[182] Eine Behörde kann nach dem genannten Grundsatz einen Sachverhalt von Amts wegen ermitteln und dabei Art und Umfang der Ermittlungsarbeit selbst bestimmen. Diszipliniert wird sie bei der Informationsgewinnung durch die Pflicht zur rechtmäßigen Ermessensausübung (§ 40 VwVfG).[183] Doch der Untersuchungsgrundsatz ist Teil eines Verwaltungsverfahrens, das auf einen Verwaltungsakt ausgerichtet ist (§ 9 VwVfG).[184]

Außerhalb eines Verwaltungsverfahren kommt für das Verhältnis von Unternehmen und Verwaltung ein Kontinuum an Informationspflichten in Betracht.[185] Begrifflich besteht keine Einheitlichkeit. Ungeachtet terminologischer Abweichungen kann der materielle Regelungsgehalt gleichwohl nach dogmatischen Kriterien geordnet werden.[186]

Zentrales Elemente eines vertikalen Informationsflusses sind Informationsbeibringungspflichten. Als Informationsbeibringungspflichten können die Informationspflichten Privater gegenüber dem Staat bezeichnet werden.[187] Die Privaten können wie Nichtstörer in Anspruch genommen werden. Diese haben Informationen aktiv und selbstständig der Verwaltung beizubringen. Die Normadressaten werden von sich aus tätig, ohne dass es einer Aufforderung bedarf.

---

[181] *Steinmüller/Ermer/Schimmel*, Das System des Datenschutzes, in: dies. (Hrsg.), Datenschutz bei riskanten Systemen, 1978, S. 71 (73).

[182] Zur Bedeutung bei der Erzeugung von Wissen *Wollenschläger*, Wissensgenerierung im Verfahren, 2009, S. 8.

[183] Vgl. *Augsberg*, Informationsverwaltungsrecht, 2014, S. 44 f.

[184] Im Übrigen kann der Amtsermittlungsgrundsatz je nach Regelungsmaterie von Spezialregelungen verdrängt werden, § 128 TKG etwa verdrängt als *lex specialis* die §§ 24–27 VwVfG. Dazu *Ruffert*, in: Säcker (Hrsg.), TKG, 3. Aufl. 2013, § 128 Rn. 1 ff.

[185] Vgl. Typologie von *Sommer*, Informationskooperation am Beispiel des europäischen Umweltrechts, in: Schmidt-Aßmann/Schöndorf-Haubold (Hrsg.), Der Europäische Verwaltungsverbund, 2005, S. 57 (100 ff.); *von Bogdandy*, Die Informationsbeziehungen im europäischen Verwaltungsverbund, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band II, 2. Aufl. 2012, § 25 Rn. 13.

[186] Vgl. *Herrmann*, Informationspflichten gegenüber der Verwaltung, 1997, S. 11.

[187] Diese werden auch als Melde-, Mitteilungs- oder Unterrichtungspflichten bezeichnet. Vgl. *Stohrer*, Informationspflichten Privater gegenüber dem Staat in Zeiten von Privatisierung, Liberalisierung und Deregulierung, 2007, S. 205 mit weitergehender Aufzählung.

Die Verpflichtung besteht kraft Gesetzes. Von diesen Pflichten sind die reaktiven und unselbstständigen Informationspflichten zu unterscheiden. Es bedarf grundsätzlich der Aufforderung der staatlichen Stelle, dass der Adressat tätig wird. Die abstrakt-generell bestehende Rechtspflicht wird erst durch ein konkret-individuelles Informationsersuchen ausgelöst.[188] Solche Auskunftspflichten Privater sind begrifflich an Tatbestandsmerkmalen wie „auf Anforderung", „auf Verlangen" und vergleichbaren Formulierungen zu erkennen. Die entsprechenden Informationsbefugnisse der Verwaltung werden nachfolgend als Befugnisse zur Einholung von Informationen bezeichnet. Es bestehen auch Informationspflichten, die aktive und reaktive Bestandteile kombinieren. Der Verpflichtete hat Informationen zu beschaffen sowie bereitzuhalten und auf Verlangen der staatlichen Stelle zu übermitteln.[189]

Von Informationsbeibringungspflichten können Informationsbeschaffungspflichten unterschieden werden. Darunter können Pflichten der Mitgliedstaaten zur Beschaffung von Informationen verstanden werden, die an europäische Stellen weiterzugeben sind. Bei solchen Mitteilungspflichten können die Informationen bereits bei der der Verwaltung vorhanden sein.[190] Diese Pflichten können typologisch auch zu den Mechanismen der Informationsgenerierung gezählt werden, werden hier aber wegen des Verhältnisses von Mitgliedstaaten zur Union im Kapitel über den Transfer von Informationen berücksichtigt.[191]

Im Folgenden werden somit die aktiven Informationsbeibringungspflichten (I.) und die Befugnisse der Verwaltung zur Generierung von Informationen (II.) auf den über sie einholbaren Informationsgehalt untersucht. Auch der Aspekt Aspekt der administrativen Informations- und Wissensgenerierung, dass die Verwaltung aufgrund der technischen und gesellschaftlichen Komplexität zur Kompensation von Wissensdefiziten zunehmend verwaltungsexterne Sachkenntnis einholen muss, ist von wesentlicher Bedeutung und daher ebenfalls zu beleuchten (III.).

---

[188] *Berliner*, Informationsbefugnisse der Bundesnetzagentur im Telekommunikationsrecht, 2012, S. 32, der auch dazu Stellung nimmt, ob es sich bei einer solchen Anordnung um einen Verwaltungsakt handelt, was bestritten werden kann, weil die Erkenntnisgewinne der Verwaltung nicht immer auf eine Entscheidung oder einen Erlass einer Regelung hinauslaufen. Vgl. auch *Röhl*, Ausgewählte Verfahrensarten, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band II, 2. Aufl. 2012, § 30, Rn. 40, 47. Im Ergebnis solle es sich bei solchen Auskunftsverlangen um Verwaltungsakte handeln.

[189] Vgl. *Herrmann*, Informationspflichten gegenüber der Verwaltung, 1997, S. 11.

[190] *Sommer*, Informationskooperation am Beispiel des europäischen Umweltrechts, in: Schmidt-Aßmann/Schöndorf-Haubold (Hrsg.), Der Europäische Verwaltungsverbund, 2005, S. 57 (61).

[191] Siehe § 4.

I. Pflichten zur Beibringung von Informationen

Unionsrechtlich indiziert sind Pflichten zur Beibringung von Sicherheitsnachweisen (1.), die Meldung spezifischer Sicherheitsvorfälle (2.) und die Meldung von Datenschutzverletzungen (3.).

1. Sicherheitsnachweise

Telekommunikationsunternehmen (a), die Betreiber wesentlicher bzw. kritischer Infrastrukturen (b) und die Anbieter digitaler Dienste (c) haben gegenüber den NIS-Behörden Sicherheitsnachweise zu erbringen.

a) Vorlage des Sicherheitskonzeptes von Telekommunikationsunternehmen

Die zentralen unionsrechtlichen Vorschriften für die Netz- und Informationssicherheit im Telekommunikationsrecht sind Art. 13a und Art. 13b der RL (EG) 2002/21/EG[192] Den Betreibern von Telekommunikationsnetzen und Anbietern von Telekommunikationsdiensten werden durch die Vorschrift materiell-rechtliche Pflichten zur Gefahrenvorsorge sowie informationsverwaltungsrechtliche Pflichten auferlegt. Im Wesentlichen setzt § 109 TKG die Pflichten in nationales Recht um.

Nach § 109 Abs. 4 S. 1 TKG haben die Betreiber von öffentlichen Telekommunikationsnetzen und Erbringer öffentlich zugänglicher Telekommunikationsdienste einen Sicherheitsbeauftragten zu benennen und ein Sicherheitskonzept zu erstellen.

Die Betreiber eines öffentlichen Telekommunikationsnetzes haben das Sicherheitskonzept der Bundesnetzagentur unverzüglich nach der Aufnahme des Netzbetriebs vorzulegen (§ 109 Abs. 4 S. 2 TKG). Für die Erbringer von Telekommunikationsdiensten besteht diese Pflicht erst nach Aufforderung durch die Bundesnetzagentur (§ 109 Abs. 4 S. 3 TKG). Diese Differenzierung ergibt sich nicht aus einer geringeren Bedeutung der Informationen über das Sicherheitskonzept der Diensteanbieter. Sie dient vielmehr der Entlastung kleinerer Anbieter und der effektiveren Aufgabenerfüllung der Bundesnetzagentur.[193] Die Regelung steht mit der korrespondierenden Bestimmung in der Richtlinie nicht in Konflikt. Art. 13b Abs. 2 a) RL (EG) 2002/21/EG verpflichtet die Mitgliedstaaten lediglich dazu, sicherzustellen, dass die Behörden befugt sind, die Übermittlung der Informationen vorzuschreiben.

Hinsichtlich des Umfangs der durch die Unternehmen beizubringenden Informationen lässt die Richtlinie den Mitgliedstaaten vergleichsweise viel Raum.

---

[192] Im Folgenden jeweils in Verbindung mit der Änderungs-RL (EG) 2009/140/EG.

[193] BT-Drs. 17/5707, S. 83.

Die Behörden sollen die Übermittlung der „erforderlichen Informationen, einschließlich der Unterlagen über die Sicherheitsmaßnahmen", vorschreiben dürfen. Konkretisiert werden diese Anforderungen an den Inhalt des Sicherheitskonzepts in § 109 Abs. 4 S. 1 Nr. 1 bis 3 TKG. Mindestens aus dem Konzept hervorgehen muss, welche Telekommunikationsanlagen eingesetzt und welche Telekommunikationsdienste für die Öffentlichkeit erbracht werden (Nr. 1), die Erfassung der Gefährdungslage (Nr. 2) und welche Schutzmaßnahmen zur Einhaltung der Verpflichtungen aus § 109 Abs. 1 und 2 TKG getroffen oder geplant sind (Nr. 3).[194]

Die Umsetzung der drei Anforderungen ist konkret zu beschreiben. Eine schematische Konzeptbeschreibung reicht nicht aus. Die Bundesnetzagentur muss erkennen können, welche Anlagen eingesetzt und welche Dienste erbracht werden. Erforderlich ist die Beschreibung ihrer Funktion.[195] Hinsichtlich der Gefährdungen reicht eine abstrakte Analyse nicht aus.[196] Die Darstellung der Gefährdungen ist weit und umfasst elementare physische Gefährdungen wie Blitzeinschlag oder Vandalismus, aber auch technische Störungen und organisatorische Gefährdungen.[197] Die Gefährdungen müssen für jedes Sicherheitssystem ermittelt werden. Den Sicherheitsteilsystemen sind dann, sofern möglich, die Schutzziele der Sicherheit zuzuordnen. Hervorgehen soll aus der Beschreibung ferner, ob die Systeme personenbezogene Daten verarbeiten und speichern können.[198]

Das Erstellen eines Sicherheitskonzepts dient in kognitiver Dimension mehreren Zwecken. Zunächst dient das Sicherheitskonzept dem Betreiber zur eige-

---

[194] *Eckhardt*, in: Geppert/Schütz (Hrsg.), BeckTKG, 4. Aufl. 2014, § 109 Rn. 56 ff.

[195] Informationen über die geographischen Standorte bestimmter Telekommunikationseinrichtungen erhält die Bundesnetzagentur jedenfalls über den 2016 zur Umsetzung der Richtlinie 2014/61/EU des Europäischen Parlaments und des Rates über Maßnahmen zur Reduzierung der Kosten des Ausbaus von Hochgeschwindigkeitsnetzen für die elektronische Kommunikation ergänzten § 77a TKG. Nach § 77a Abs. 1 TKG ist die Bundesnetzagentur die zentrale Stelle des Bundes für den sog. Infrastrukturatlas. Die Bundesnetzagentur kann von Eigentümern oder Betreibern öffentlicher Versorgungsnetze, die über Einrichtungen verfügen, die zu Telekommunikationszwecken genutzt werden können, diejenigen Informationen verlangen, die für eine gebietsbezogene Übersicht erforderlich sind. Die Datenlieferungsverpflichtung gegenüber der Bundesnetzagentur umfasst sicherheits- und versorgungsrelevante Infrastrukturen. Erst in der zweiten Stufe prüft die Behörde, welche Daten sie nicht in den Infrastrukturatlas aufnimmt (vgl. § 77a Abs. 4 TKG). Siehe dazu OVG Münster, Beschluss vom 07.01.2016 – 13 A 999/15.

[196] *Eckhardt*, Öffentliche Sicherheit, in: Heun (Hrsg.), Handbuch Telekommunikationsrecht, 2. Aufl. 2007, S. 61 (86 f.).

[197] Vgl. *Bundesnetzagentur*, Leitfaden zur Erstellung eines Sicherheitskonzepts gemäß § 109 Abs. 3 TKG, Stand Januar 2006, S. 16 ff. und 37 ff.

[198] Mitteilung Nr. 985/2012 in ABl. Bundesnetzagentur 2012, S. 4156.

nen Bewusstseinsbildung über die sicherheitsrelevante Beurteilung von Sicherheitsteilsystemen und der Beurteilung der Sicherheit, Integrität und Verfügbarkeit von Netzen und Diensten.[199] Weiter erhält die Bundesnetzagentur durch die Vorlage einen metaperspektivischen Blick auf die Gefährdungslage. Die Vorlage mehrerer und verschiedener Konzepte durch die verschiedenen Betreiber und Erbringer ermöglicht einen Vergleich, sodass die Bundesnetzagentur die Plausibilität der Selbsteinschätzung überprüfen kann. Die Bundesnetzagentur wird grundsätzlich in die Lage versetzt, Sicherheitsmängel sowohl im Sicherheitskonzept als auch bei dessen Umsetzung zu erkennen (§ 109 Abs. 4 S. 4 TKG).

Die Verpflichtung zur Vorlage des Sicherheitskonzepts ist keine einmalige Handlungspflicht. Die Bundesnetzagentur bleibt auf den aktuellen Stand des Sicherheitskonzepts, da es fortzuschreiben ist, sobald sich Sicherheitsfaktoren, die dem Konzept zugrundeliegen, ändern. Die Bedeutung der Vorlage des Sicherheitskonzepts für die Sicherheitsgewährleistung lässt sich an der Kritik des Bundesverfassungsgerichts an der Vorgängervorschrift ablesen. Das Gericht hatte in seinem Urteil zur Vorratsdatenspeicherung mit Blick auf die Vorgängervorschrift § 109 Abs. 3 TKG a. F. kritisiert, dass sie keine hinreichende Datensicherheit gewährleiste, weil es an einer Verpflichtung zu einer periodisierenden Fortschreibung des Sicherheitskonzepts fehle, die eine effektive Kontrolle des einzuhaltenden Sicherheitsstandards ermögliche.[200] Nach den durch das IT-Sicherheitsgesetz eingeführten Sätzen 7 und 8 des § 109 Abs. 4 TKG überprüft die Bundesnetzagentur die Umsetzung der Konzepte nunmehr regelmäßig mindestens alle zwei Jahre. Bei der Überprüfung kann sich die Bundesnetzagentur der aufsichtsrechtlichen Informationsbefugnis des § 115 Abs. 1 und 2 TKG bedienen.[201]

b) Nachweis der Sicherheit von Betreibern wesentlicher Dienste bzw. kritischer Infrastrukturen

Die Mitgliedstaaten haben die unionsrechtliche Pflicht sicherzustellen, dass die zuständigen Behörden über die Befugnisse und Mittel verfügen, von den Betreibern wesentlicher Dienste verlangen zu können, dass diese die zur Bewertung der Sicherheit ihrer Netz- und Informationssysteme erforderlichen Informationen sowie Nachweise über die wirksame Umsetzung der Sicherheitsmaßnahmen zur Verfügung stellen (Art. 15 Abs. 2 NIS-RL). Die Pflicht ist im Wesentlichen durch § 8a Abs. 3 BSIG umgesetzt. Die Betreiber kritischer Infrastrukturen müssen die Einhaltung der Sicherheitsanforderungen alle zwei Jahre dem BSI „auf geeignete Weise" nachweisen.

---

[199] *Graulich*, in: Arndt/Fetzer/Scherer/ders. (Hrsg.), TKG, 2. Aufl. 2015, § 109 Rn. 30.

[200] BVerfGE 125, 260 (349).

[201] BT-Drs. 18/4096, S. 35; BT-Drs. 17/5707, S. 83; dazu ferner unter § 3 D. III.

Die nähere Spezifizierung der Geeignetheit der Art und Weise des Nachweises wird im Gesetz selbst, trotz der Bedeutung für die Praxis, weitgehend offengelassen. Der Nachweis kann durch Sicherheitsaudits, Zertifizierungen oder Prüfungen erbracht werden. Dabei handelt es sich nicht um synonym zu verstehende Begriffe.[202] Sicherheitsaudits bestätigen die Eignung eines Sicherheitsmanagementsystems.[203] Sicherheitszertifikate dagegen betreffen ein IT-Produkt, einen Prozess oder ein Profil.[204] Welche Bedeutung der Prüfung als dritte Variante zukommt, ist unklar. Das Anliegen der Nachweispflicht ist es, dass die Behörde darüber Kenntnis erlangt, ob ein Betreiber die für seine Branche und Technologie geeigneten und wirksamen Maßnahmen und Empfehlungen befolgt.[205] Dabei geht es vor allem um die Kenntnis davon, ob ein Informationssicherheitsmanagement, d. h. ein Sicherheits- und Risikomanagement, eingerichtet ist, ob kritische Anlagen und Einrichtungen überhaupt identifiziert wurden und administriert werden, ob und welche Maßnahmen zur Angriffsprävention und -erkennung betrieben werden, ob ein Betriebs-Kontinuitätsmanagement implementiert ist oder ob branchenspezifische Besonderheiten berücksichtigt sind.[206]

Das Gesetz trifft entgegen der sonst im technischen Sicherheitsrecht bekannten Vorgaben keine Regelung hinsichtlich der Qualifikation und Akkreditierung der durchführenden Stellen, der Verfahrensanforderungen und der materiellen Standards.[207] Die korrespondierende Unionsvorschrift in Art. 15 Abs. 2 NIS-RL erfordert es aber, dass ein „qualifizierter Prüfer" die Sicherheitsüberprüfung durchführt. Durch § 8 Abs. 4 BSIG wird das BSI allerdings ermächtigt, Anforderungen an das Prüfungsverfahren, die auszustellenden Nachweise sowie die fachlichen und organisatorischen Stellen nach Anhörung der betroffenen Betreiber und Wirtschaftsverbände festzulegen. Aus epistemischer Sicht hat das BSI dadurch einen erheblichen Einfluss auf die generierbaren Informationen, da das Ergebnis der Prüfung maßgeblich davon abhängig ist, wer ein Audit oder Zertifikat ausstellt und nach welcher Methode und in welchem Ver-

---

[202] Vgl. aber *Eckhardt*, ZD 2014, 599 (601).

[203] Siehe *Roßnagel*, Datenschutzaudit, 2000, S. 56 ff.

[204] *Roßnagel*, Das Konzept des Datenschutzaudits, in: ders. (Hrsg.), Handbuch Datenschutzrecht, 2003, S. 437 (462 ff.).

[205] Zur erheblichen Relevanz von Schwachstellenberichten für Unternehmen siehe die Anordnung der Federal Trade Commission, In Re ASUSTeK, Agreement Containing Consent Order, File No. 1423156; zur Gefahr der Bürokratisierung durch *Neumann*, A-Drs. 18(4)284 F S. 9.

[206] BT-Drs. 18/4096, S. 44.

[207] *Spindler*, CR 2016, 297 (300). Die §§ 2 Abs. 7, 9 BSIG betreffen die Zertifizierung die IT-Sicherheit der Bundesverwaltung durch das BSI als zertifizierende Stelle. Zur Kritik *Hornung*, A-Drs. 18(4)284 G, S. 9; *Heinickel/Feiler*, CR 2014, 708 (712); *Roth*, ZD 2015, 17 (21).

fahren (z. B. aussagekräftige Penetrationstests) das Ergebnis zustande gekommen ist.

Das Fehlen gesetzlicher Vorgaben ist insofern problematisch, als ein konkreter Maßstab für die Sicherheitsprüfungen fehlt, sofern noch kein branchenspezifischer Sicherheitsstandard gemäß § 8a Abs. 2 BSIG besteht bzw. noch nicht im Wege der Selbstregulierung etabliert wurde oder sich der Betreiber nicht zur Implementierung eines solchen Standards entschieden hat. Wenig praktikabel wäre es, die materiell-rechtliche Verpflichtung zu „angemessenen" technischen und organisatorischen Schutzvorkehrungen gemäß § 8a Abs. 1 BSIG als Auditing-Maßstab heranzuziehen, da auch diese nicht hinreichend gesetzlich bestimmt sind. Aus diesem Grunde kann vor dem Hintergrund des Wesentlichkeits- und Bestimmtheitsgebot gefordert werden, dass die methodischen Kriterien gesetzlich bestimmt sind,[208] zumal die Legitimation der Nachweiserstellung maßgeblich von akzeptierten Kriterien abhängt. Wegen entsprechender verfassungsrechtlicher Bedenken im Hinblick auf die Tätigkeit von Zertifizierungsstellen wurde die Vorschrift des § 18 SigG eingeführt,[209] der gesetzlich näher die Anforderung an die anerkennenden und prüfenden Stellen bei Zertifizierungen von Produkten elektronischer Signaturen regelt.

Zu übermitteln sind dem BSI eine „Aufstellung" der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der durch sie aufgedeckten Sicherheitsmängel (§ 8a Abs. 3 S. 3 BSIG). Mit Blick auf Art. 15 Abs. 2 NIS-RL bleibt die Bestimmung damit unter der unionsrechtlichen Anforderung. Danach müssen die Mitgliedstaaten über die Mittel- und Befugnisse verfügen können, die „Ergebnisse" der Prüfungen aufzufordern. Die Verwendung des Wortes „Aufstellung" kann auch so verstanden werden, dass lediglich eine Auflistung der durchgeführten Maßnahmen erforderlich ist. Insofern besteht für § 8a Abs. 3 S. 3 BSIG Klarstellungsbedarf.

c) Nachweis der Sicherheit von Anbietern digitaler Dienste

Anbieter digitaler Dienste haben wie die Betreiber wesentlicher Dienste Nachweise über ihre Sicherheitsgewährleistung zu erbringen. Gemäß Art. 17 Abs. 2 a) NIS-RL müssen die mitgliedstaatlichen Behörden über die Befugnisse und Mittel verfügen, von den Anbietern digitaler Dienste die zur Beurteilung der Sicherheit ihrer Netz- und Informationssysteme erforderlichen Informationen einschließlich der nachweislichen Sicherheitsmaßnahmen einzufordern.

---

[208] *Eckhardt* ZD 2014, 599 (601).

[209] *Gramlich*/*Orantek*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 3. Aufl. 2015, SigG, § 18 Rn. 5.

Diese Pflicht ist *de lege lata* nicht in das deutsche Recht umgesetzt, weder im BSIG, noch, soweit digitale Dienste in den Anwendungsbereich des TMG fallen, in § 13 TMG.

Die Umsetzung kann sich nicht gänzlich an der Regelungstechnik orientieren, die für den Sicherheitsnachweis durch Betreiber kritischer Infrastrukturen gilt. Die Einhaltung der Sicherheitspflichten dürfen die nationalen Behörden nicht im Vorhinein, sondern nur im Nachhinein überwachen. Im Wege einer *Ex-post*-Überwachungsmaßnahme darf die NIS-Behörde nur dann tätig werden, wenn ihr ein Nachweis darüber vorliegt, dass ein Anbieter die Sicherheitsanforderungen nicht einhält.[210] Als Nachweise sollen auch solche Feststellungen gelten, die der NIS-Behörde von den zuständigen Behörden eines anderen Mitgliedstaats vorgelegt werden (§ 17 Abs. 2 S. 2 NIS-RL). Auf diese Weise können Fälle erfasst werden, in denen der Ort der Hauptniederlassung und die Netz- und Informationssysteme, die im Rahmen der Bereitstellung der digitalen Dienste genutzt werden, in unterschiedlichen Mitgliedstaaten gelegen sind.

Der durch die Anbieter zu erbringende Sicherheitsnachweis ist in inhaltlicher Hinsicht bestimmter als die Nachweispflicht der Betreiber wesentlicher Dienste. Während den Behörden bei den Betreibern wesentlicher Dienste sekundärrechtlich die zur „Bewertung" erforderlichen Informationen zur Verfügung gestellt werden müssen, sind ihnen von den Anbietern digitaler Diente die zur „Beurteilung" erforderlichen Informationen zur Verfügung zu stellen. Eine Beurteilung ist insofern zu ermöglichen, als die materiellen Sicherheitsanforderungen spezifischer sind. Art. 16 Abs. 1 S. 2 NIS-RL fordert, dass durch die dem Risiko angemessenen Sicherheitsmaßnahmen der Anbieter digitaler Dienste der Sicherheit der Systeme und Anlagen, der Bewältigung von Sicherheitsvorfällen, dem Betriebskontinuitätsmanagement, der Überwachung, Überprüfung und Erprobung sowie der Einhaltung der internationalen Normen Rechnung zu tragen ist. Im Umkehrschluss daraus ergibt sich, dass aus dem Nachweis hervorgehen muss, inwiefern die genannten Maßnahmen berücksichtigt wurden und inwiefern sie bestehenden Risiken angemessen sind. Gegenstand der anlassbezogen zu erbringenden Nachweise sind darüber hinaus die Maßnahmen, die aufgrund der von der Kommission nach Art. 16 Abs. 8 NIS-RL erlassenen Durchführungsakte, welche die Sicherheitsanforderungen genauer bestimmen, von den Anbietern getroffen wurden.[211]

---

[210] Zur Möglichkeit, dass dieser Nachweis im Wege des Informationsaustausches mit einem anderen Mitgliedstaat vorgelegt werden kann, siehe § 4 B. II., III.

[211] Zur Funktion der Durchführungsrechtssetzung in der Informationsgenerierung und der Abgrenzung von delegierter Rechtssetzung siehe § 3 D. I. 2. c) bb).

2. Meldepflichten bei Sicherheitsverletzungen

Ein wichtiges informationsverwaltungsrechtliches Instrument zur Generierung von Erkenntnissen über Sicherheitsvorfälle in Unternehmen sind Meldepflichten. Die Betreiber von Telekommunikationsnetzen und Anbieter von Telekommunikationsdiensten (a), die Betreiber wesentlicher Dienste bzw. kritischer Infrastrukturen (b) als auch Anbieter digitaler Dienste (c) haben unter bestimmten Voraussetzungen aktuelle und potenzielle Störungen der NIS-Behörde zu melden. Informationen über Sicherheitsvorfälle können daneben auf Basis freiwilliger Meldungen generiert werden (d).

a) Betreiber von Telekommunikationsnetzen und Anbieter von Telekommunikationsdiensten

Die Mitgliedstaaten haben gemäß Art. 13b Abs. 3 UAbs. 1 RL 2009/140/EG[212] sicherzustellen, dass die Unternehmen, die öffentliche Kommunikationsnetze oder öffentlich zugängliche elektronische Kommunikationsdienste bereitstellen, der zuständigen nationalen Regulierungsbehörde eine Verletzung der Sicherheit oder einen Verlust der Integrität mitteilen, die bzw. der beträchtliche Auswirkungen auf den Betrieb der Netze oder die Bereitstellung der Dienste hatte. Der Umsetzung dieser Pflicht dient § 109 Abs. 5 TKG. Nach dessen Satz 1 haben die Betreiber und Anbieter unverzüglich solche Beeinträchtigungen von Telekommunikationsnetzten und -diensten der Bundesnetzagentur mitzuteilen, die zu beträchtlichen Sicherheitsverletzungen führen oder führen können.

aa) Anlass der Meldung

Der Anlass einer Meldung ist zunächst eine Beeinträchtigung. Eine Beeinträchtigung erfordert nicht, dass bereits eine Auswirkung eingetreten ist.[213] Die Beeinträchtigung muss zu einer beträchtlichen Sicherheitsverletzung führen oder führen können. Der Begriff der Sicherheitsverletzung ist im TKG an keiner Stelle definiert. Durch Abgrenzung zu der Benachrichtigungspflicht in § 109a TKG zeigt sich, dass eine Sicherheitsverletzung nicht notwendig inhaltsgleich mit der Verletzung des Schutzes personenbezogener Daten ist.[214] Die sich aus einer solchen Verletzung ergebende Benachrichtigungspflicht für die betroffenen Nutzer resultiert nämlich aus § 93 Abs. 3 TKG in Verbindung mit § 109a TKG. Eine gleichlautende Auslegung würde zu einer systemwidrigen Dopplung

---

[212] RL (EG) 2002/21/EG, geändert durch die RL (EG) 2009/140/EG.

[213] Kritisch *Heinickel*/*Feiler*, CR 2014, 708 (714).

[214] *Eckhardt*, in: Geppert/Schütz (Hrsg.), BeckTKG, 4. Aufl. 2013, § 109 Rn. 71, § 109a Rn. 5, 15.

der Meldepflicht führen, zumal § 109a TKG der Umsetzung einer anderen Richtlinie dient.[215]

Die Bestimmung der tatbestandlichen Voraussetzungen der Meldepflicht hat sich daher an den sich aus Art. 13 RL 2009/140/EG und § 109 TKG ergebenden Verpflichtungen zu orientieren. Aus der Zusammenschau von Art. 13a Abs. 3 RL 2009/140/EG in Verbindung mit § 109 Abs. 5 S. 1 TKG sowie mit den in Art. 13a Abs. 1 und 2 RL 2009/140/EG bzw. § 109 Abs. 1 und 2 TKG niedergelegten materiell-rechtlichen Pflichten zur Sicherheitsgewährleistung folgt zum einen, dass die Sicherheit durch die Verletzung der Vertraulichkeit, Integrität, Authentizität oder Einschränkung der Verfügbarkeit betroffen ist, und zum anderen, dass mit Sicherheitsverletzung insbesondere „Störungen" von Telekommunikationsnetzen oder -diensten gemeint sind (vgl. auch § 109 Abs. 5 S. 2 TKG: „Dies schließt Störungen ein, […]"). Der zentrale Begriff der Störung ist seinerseits auslegungsbedürftig. Mangels näherer Bestimmung in der Vorschrift selbst bietet sich eine Anlehnung an den Störungsbegriff des § 100 TKG an. Dort ist der Begriff zentral für die möglichen Abwehrmaßnahmen von Anbietern von Telekommunikationsdiensten gegen Cyberangriffe.[216] Telekommunikationsdiensteanbieter können auf Grundlage von § 100 Abs. 1 S. 1 TKG Bestands- und Verkehrsdaten erheben und verwenden, „um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen." Nach einem herkömmlichen Verständnis bezieht sich die Störung auf Veränderungen der physikalischen Beschaffenheit von den für die Telekommunikation verwendeten Gerätschaften. Für dieses Verständnis lässt sich der Begriff der Telekommunikationsanlage in § 3 Nr. 23 TKG heranziehen, die als „technische Einrichtung oder System" verstanden wird. Ein enges Verständnis des Störungsbegriffs wird jedoch den Schutzzielen der Netz- und Informationssicherheit nicht gerecht. Geboten ist vielmehr eine weite Auslegung, die den Begriff der Störung funktional versteht. Eine Störung liegt dann auch vor, wenn die eingesetzte Technik die ihr zugedachten Funktionen nicht mehr richtig oder nicht vollständig erfüllen kann.[217] Erfasst ist folglich jede nicht gewollte Veränderung der vom Telekommunikationsdiensteanbieter für sein Telekommunikationsangebot genutzten technischen Einrichtung. Dazu zählen Fälle von Sicherheitslücken, Schadprogrammen und erfolgte und versuchte – darunter auch erfolgreich abgewehrte – Angriffe auf die Sicherheit in der Informationstechnik, aber auch außergewöhnliche und unerwartete technische

---

[215] Inhaltlich setzt § 109a TKG den Art. 4 Abs. 3 bis 4 der RL (EG) 2002/58/EG um.

[216] Siehe § 3 E. II. 2. a).

[217] BGH, NJW 2014, 2500 (2501); siehe auch BGH, NJW 2011, 1509 (1511); *Gramlich*, in: Manssen (Hrsg.), Telekommunikations- und Multimediarecht, 36. Aufl. 2015, C, § 100, Rn. 16; *Mozek,* in: Säcker (Hrsg.), TKG, 3. Aufl. 2013, § 100, Rn. 7.

Defekte mit Bezug zur Informationstechnik, etwa ein Ausfall von physischen Anlagen wie der Serverkühlung oder Defekte nach Softwareupdates.[218]

Die meldepflichtigen Sicherheitsverletzungen schließen nach § 109 Abs. 5 S. 2 TKG auch solche Störungen ein, die zur Einschränkung der Verfügbarkeit der über diese Netze erbrachten Dienste oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können. Die Formulierung „über diese Netze erbrachten Dienste" verweist auf Schutzgüter, die von denen in Abs. 5 S. 1 abweichen. Dort sind diese ein „Netz" oder ein „Dienst". Durch Satz 2 einbezogen sind auch Fälle im Vorfeldbereich, d. h. dem Stadium, in dem Angreifer Nutzersysteme mit Schadsoftware infizieren, um die Telekommunikations- und Datenverarbeitungssysteme der Nutzer zu einem Botnetz zusammenschließen und später für einen gezielten Missbrauch ausnutzen zu können.[219]

Die Meldepflicht auslösende Schwelle ist im Vergleich zur alten Fassung[220] der Vorschrift durch die Novellierung des Wortlauts durch das IT-Sicherheitsgesetz[221] in zweifacher Hinsicht gesenkt worden. Zum einen bezog sich nach § 109 Abs. 5 S. 1 TKG a. F. die Meldepflicht auf „Sicherheitsverletzungen einschließlich Störungen". § 109 Abs. 5 Abs. 1 TKG bezieht sich dagegen nur auf „Beeinträchtigungen von Telekommunikationsnetzen und -diensten". Die Meldeschwelle ist insofern niedriger, als ähnlich wie im Gefahrenabwehrrecht eine Beeinträchtigung noch nicht den Grad einer Störung erreichen muss. Die Meldepflicht kann dadurch tendenziell früher ausgelöst werden. Zum anderen waren nach der alten Fassung der telekommunikationsrechtlichen Meldepflicht nur solche Sicherheitsvorfälle zu melden, durch die „beträchtliche Auswirkungen […] entstehen." Nunmehr erstreckt sich die Meldepflicht auch auf Störungen, die nicht nur zu einer Einschränkung der Verfügbarkeit führen, sondern auch „führen können". Diese für die Telekommunikationsunternehmen als Eingriff wirkende Pflichtenerweiterung kann damit gerechtfertigt werden, dass eine Verbesserung des Lagebildes bezüglich des Vorfeldbereichs erforderlich ist, weil Telekommunikationsdienste zum „Rückgrat der Informationsgesellschaft"

---

[218] BT-Drs. 18/4096, S. 46.

[219] *Roos*, MMR 2014, 723 (727). Als Botnetz wird ein Verbund von Systemen bezeichnet, die von einem fernsteuerbaren Schadprogramm befallen sind. Prinzipiell kann jedes internetfähige System Teil eines Botnetzes werden. Der Zugriff auf Bots erfolgt über zentrale Systeme (sog. Command-and-Control-Server), die von den Botnetz-Betreibern kontrolliert werden und die es ermöglichen, den Bots Steuerbefehle zu schicken. Siehe dazu Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland, 2016, S. 26.

[220] § 109 Abs. 5 TKG (a. F.) angefügt mit Wirkung vom 10.5.2012 durch Gesetz vom 3.5.2012 (BGBl. I S. 958).

[221] § 109 Abs. 5 TKG neu gefasst mit Wirkung vom 25.7.2015 durch Gesetz vom 17.7.2015 (BGBl. I S. 1324).

gehören.[222] Eine höhere Bewertung der Gefährdung und Schutzwürdigkeit von Informationstechnik und Telekommunikation genügt somit § 2 Abs. 10 S. 1 Nr. 1 BSIG, nach dem die benannten Sektoren zu den kritischen Infrastrukturen gehören. Vor der Neufassung waren tatsächliche Störungen außerdem nur dann meldepflichtig, wenn die verursachten Auswirkungen beträchtlich waren.

Dem Wortlaut nach ist die Meldepflicht nicht auf eigene Netze oder Dienste beschränkt. Daraus kann gefolgert werden, dass bemerkte Beeinträchtigungen in fremden Netzen oder Diensten ebenfalls meldepflichtig sind. Beispielsweise wäre die Kenntnis über einen mit Schadsoftware infizierten Server meldepflichtig, wenn dieser versucht, fremde Systeme erheblich zu beeinträchtigen.[223]

Eingeschränkt wird die Meldepflicht durch das tatbestandliche Erfordernis einer „beträchtlichen" Sicherheitsverletzung. Wann eine Sicherheitsverletzung als beträchtlich zu qualifizieren ist, ist nicht näher bestimmt. Ausgehend von der allgemeinen Bedeutung meint „beträchtlich" so viel wie „sehr", „wahrnehmbar" oder „erheblich".[224] Die Sicherheitsverletzung muss also eine Signifikanz aufweisen, die aus aus der Menge der sonstigen Sicherheitsverletzungen herausstechen lässt. Meldepflichtig ist folglich nicht bereits jede tatsächliche oder mögliche Störung von Telekommunikationsnetzen und -diensten. Der systematische Vergleich ergibt, dass die Meldepflicht für Betreiber kritischer Infrastrukturen an eine „erhebliche Störung" anknüpft (§ 8b Abs. 4 S. 1 BSIG). Aufgrund der Vergleichbarkeit des meldepflichtigen Ereignisses bietet sich eine Anlehnung an den Begriff der Erheblichkeit der Störung an.[225] Das qualifizierende Merkmal „beträchtlich" gleicht die Weite des Störungsbegriffs aus. Es bedarf daher keiner teleologischen Reduktion des Verständnisses von „Störung".

Die Bundesnetzagentur als Adressatin der Meldepflicht geht davon aus, dass es den Verpflichteten obliegt, mit einer Bewertung in eigener Verantwortung festzustellen, ob eine Beeinträchtigung zu einer beträchtlichen Sicherheitsverletzung führen kann. Das Umsetzungskonzept der Bundesnetzagentur zu § 109 Abs. 5 TKG legt nahe, die darin beschriebenen Kriterien zur fallbezogenen Bewertung heranzuziehen.[226] Zu den Bewertungskriterien gehören die betroffenen Teilnehmerstunden (zeitliche Beeinträchtigung der Integrität, Vertraulichkeit, Authentizität oder Verfügbarkeit), die Auswirkung auf internationale Zusammenschaltung (Zusammenschaltungspunkte mit internationaler Zielrichtung)

---

[222] BT-Drs. 18/4096, S. 62.

[223] *Leisterer/Schneider*, CR 2014, 574 (576).

[224] *Duden*, Eintrag „beträchtlich", http://www.duden.de/rechtschreibung/betraechtlich.

[225] Siehe § 3 D. I. 2. b).

[226] So *Bundesnetzagentur*, Umsetzung des § 109 Absatz 5 TKG zur Mitteilung einer Sicherheitsverletzung (Umsetzungskonzept), Abl. [Nr. 2], Stand: 27.07.2016, Version 3.0, S. 4, online abrufbar.

und die Auswirkung auf die Notruflenkung. Bei entsprechender Ausprägung kann jedes Kriterium für sich alleine bereits hinreichend für eine Einstufung als mitteilungspflichtige Beeinträchtigung sein.[227]

Obwohl das BSI die zentrale Meldestelle für die Betreiber kritischer Infrastrukturen ist, sind die Meldungen nur an die Bundesnetzagentur zu richten. Inwieweit dies dem Anliegen, ein möglichst vollständiges Lagebild über Beeinträchtigungen beim BSI zu erzeugen, widerstrebt, ist vor allem eine Frage der Weitergabe der Informationen.[228]

bb) Inhalt der Meldung

Die Umsetzung der Meldepflicht ist weitgehend den Mitgliedstaaten überlassen. Die Kommission kann gemäß Art. 13a Abs. 4 RL 2009/140/EG geeignete technische Durchführungsmaßnahmen zur Harmonisierung der Meldepflicht beschließen.[229] Dazu gehören Maßnahmen, mit denen Umstände, Form und Verfahren der Meldung festgelegt werden. Die Expertise der ENISA ist dabei „weitestgehend" zu berücksichtigen. Die Kommission hat solche Maßnahmen bislang nicht festgelegt.[230]

Der Struktur des § 109 Abs. 5 TKG folgend, ist hinsichtlich der im Einzelnen in der Meldung anzugebenden Daten und Informationen zwischen der initialen Kurzmitteilung, der vollständigen Mitteilung und dem detaillierten Bericht zu unterscheiden. Die initiale Kurzmitteilung ist geboten, da die Meldung „unverzüglich" zu erfolgen hat (§ 109 Abs. 5 S. 1 TKG). Noch ausstehende Informationen über die Beeinträchtigung können in einer vollständigen Mitteilung nachgereicht werden. Einen detaillierten Bericht kann die Bundesnetzagentur verlangen, wenn die Auswertung der vollständigen Mitteilung über eine tatsächlich eingetretene beträchtliche Sicherheitsverletzung ergibt, dass die Umstände genauer untersucht werden müssen (vgl. § 109 Abs. 5 S. 3 TKG).

Die initiale Meldung muss dem Wortlaut nach Angaben zu der Störung sowie zu den technischen Rahmenbedingungen enthalten. Als Umkehrschluss aus der möglichen Berichtspflicht folgt, dass sie nicht umfassend sein muss. Sie wird aus Gründen der Dringlichkeit oder des unvollständigen Informationsstands auf die bereits vorliegenden Informationen über die Beeinträchtigung beschränkt. Der Begriff der Rahmenbedingung besagt, dass diejenigen technischen Bedin-

---

[227] *Bundesnetzagentur*, Umsetzung des § 109 Absatz 5 TKG zur Mitteilung einer Sicherheitsverletzung (Umsetzungskonzept), Abl. [Nr. 2], Stand: 27.07.2016, Version 3.0, S. 7, online abrufbar.

[228] Siehe § 4 B.

[229] Siehe zu den Durchführungsmaßnahmen § 3 D. I. 2. (3).

[230] Vgl. *ENISA*, Technical Guideline on Security measures for Article 4 and Article 13a, Version 1.0, 2014, S. 42.

gungen anzugeben sind, die zum maßgeblichen Zeitpunkt bestanden und kausal für das beeinträchtigende Ereignis sein könnten („Rahmen*bedingung*"). Enthalten muss die Meldung also Informationen über die Randbedingungen, Vorbedingungen oder Voraussetzungen der Beeinträchtigung. Zu melden sind folglich auch die allgemeinen technischen Gegebenheiten des konkreten Gelingens bei einem Angriff von außen. In jedem Falle sind die vermutete oder tatsächliche Ursache der Störung anzugeben sowie die betroffene Informationstechnik zu nennen. Die im Gesetz beschriebenen meldepflichtigen Umstände sind jedoch nicht abschließend („insbesondere").

Der weiteren Spezifikation der meldepflichtigen Parameter dient das Umsetzungskonzept der Bundesnetzagentur, das bei Bedarf angepasst wird und dessen dritte Version 2016 veröffentlich wurde.[231] Neben der Meldeschwelle werden darin der Verfahrensablauf sowie der Inhalt, die Form und die Übermittlung der Meldung konkretisiert. Die im Umsetzungskonzept aufgeführten Kriterien sind angelehnt an die Technischen Richtlinien zur Meldung von Sicherheitsverletzungen der ENISA.[232] Letztere verstehen sich freilich aber nicht als verbindliche Standards, sondern als Darstellung möglicher Meldesysteme („[…] is not intended as guidance, but rather as an illustration of the range of different national reporting schemes across the EU […]").[233] Auch dem Umsetzungskatalog kommt keine unmittelbare rechtliche Qualität zu. Die Tatbestandsvoraussetzungen der Meldepflicht sind unbestimmte Rechtsbegriffe, die durch einen Kriterienkatalog nicht in einer rechtlich verbindlichen Weise konkretisiert werden. Ein Kriterienkatalog kann allenfalls unverbindliche Hinweise geben, an die ein Gericht jedoch nicht gebunden wäre. Der Umsetzungskatalog entfaltet auch keine Bindung der Bundesnetzagentur. An eine Selbstbindung der Verwaltung ist bereits deshalb nicht zu denken, weil die Meldepflicht außerhalb der Leistungsverwaltung liegt. Die Norm lässt der Bundesnetzagentur indes einen Spielraum, die Meldekategorien und -arten näher zu klassifizieren.

Die initiale Meldung ist gemäß Umsetzungskatalog der Bundesnetzagentur per E-Mail oder Fax mitzuteilen. Sie soll die Kontaktdaten, die ersten Erkenntnisse über Art, Ausmaß und Dauer der Störung sowie erste Einschätzungen der Ursachen und Auswirkungen bezüglich der Bewertungskriterien enthalten.[234]

---

[231] *Bundesnetzagentur*, Umsetzung des § 109 Absatz 5 TKG zur Mitteilung einer Sicherheitsverletzung (Umsetzungskonzept), Abl. [Nr. 2], Stand: 27.07.2016, Version 3.0, online abrufbar.

[232] *Bundesnetzagentur*, Umsetzung des § 109 Absatz 5 TKG zur Mitteilung einer Sicherheitsverletzung (Umsetzungskonzept), Abl. [Nr. 2], Stand: 27.07.2016, Version 3.0, S. 7.

[233] *ENISA*, Technical Guideline on Incident Reporting, Version 2.1, 2014, S. 7.

[234] *Bundesnetzagentur*, Umsetzung des § 109 Absatz 5 TKG zur Mitteilung einer Sicher-

Der Inhalt der vollständigen Mitteilung ergibt sich neben dem Umsetzungskonzept aus dem von den Betreibern und Anbietern zu verwendenden, von der Bundesnetzagentur zur Verfügung gestellten Formblatt.[235] Sie soll grundsätzlich in Textform erfolgen. Zu beschreiben sind insbesondere die Umstandsdaten der Beeinträchtigung (betroffener Grundwert der Sicherheit, Zeitpunkt der Entdeckung, geographische Ausprägung usw.) sowie die ggf. betroffene Informationstechnik. Diesbezüglich sind vor allem die allgemeinen Kategorien informationstechnischer Angriffe mitzuteilen (Ausnutzen bestimmter Schwachstellen, initialer Angriff bei mehrstufig kombinierten Angriffen, Art des Schadprogramms, Vorliegen von Hacking, Identitätsmissbrauch, Verhinderung von Diensten usw.). Bei einem informationstechnischen Angriff sind ferner die Art, die Anzahl und auf freiwilliger Basis die vermutete Motivation anzugeben. Zu den nicht freiwilligen Angaben gehört die Nennung der forensischen Daten, die dem BSI zur Verfügung gestellt werden können. Anzugeben sind schließlich auch ergriffene Abhilfe- und Präventivmaßnahmen.

Der erforderliche Inhalt des detaillierten Berichts ergibt sich aus dem Umsetzungskonzept nicht. Mit Blick auf die Meldungen muss der Bericht jedenfalls mehr als nur Metainformationen, die auf äußere Merkmale der Beeinträchtigung verweisen, dokumentieren. Aus dem Sinn und Zweck der Meldepflicht folgt, dass die Aussagekraft der Berichte grundsätzlich so groß sein muss, dass die Bundenetzagentur die generierten Informationen und das daraus gewonnene Wissen für die Erstellung des Katalogs an Sicherheitsforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen (§ 109 Abs. 6 TKG) nutzen kann. Der Katalog ist Grundlage für die Sicherheitskonzepte und für die zu implementierenden Schutzmaßnahmen der Telekommunikationsunternehmen.[236] Der gesetzliche Auftrag zur Erstellung von Sicherheitsanforderungen setzt eine entsprechende informationelle Rückkopplung seitens der Betreiber und Anbieter voraus. Der Informationswert einer Meldung sollte daher so hoch sein, dass Rückschlüsse auf abstrakt-generelle Abhilfemaßnahmen gezogen werden können. Auf Grundlage des Berichts sollten Anforderungen aufgestellt werden können, die eben solche Sicherheitsverletzungen, welche die Meldung ausgelöst hat, zukünftig verhindert.

---

heitsverletzung (Umsetzungskonzept), Abl. [Nr. 2], Stand: 27.07.2016, Version 3.0, S. 9; vgl. auch BT-Drs. 17/5707, S. 83 zu § 109 Abs. 5 a. F.

[235] Bundesnetzagentur, Mitteilung nach § 109 Absatz 5 Telekommunikationsgesetz, Formblatt, online abrufbar.

[236] *Graulich*, in: Arndt/Fetzer/Scherer/ders. (Hrsg.), TKG, 2. Aufl. 2015, § 109 Rn. 49.

b) Betreiber wesentlicher Dienste und Kritischer Infrastrukturen

Die Betreiber wesentlicher Dienste im Sinne von Art. 4 Abs. 4 NIS-RL haben den nationalen NIS-Behörden oder den nationalen CSIRTs unverzüglich Sicherheitsvorfälle zu melden. Der Umsetzung dieser Pflicht dient § 8b Abs. 4 BSIG, der eine Meldepflicht für Betreiber kritischer Infrastrukturen regelt.

aa) Anlass der Meldung

Das unionsrechtlich meldepflichtige Ereignis ist ein Sicherheitsvorfall, der erhebliche Auswirkungen auf die Verfügbarkeit der von den Betreibern bereitgestellten wesentlichen Dienste hat, Art. 14 Abs. 3 NIS-RL. Die Formulierung des Meldetatbestands impliziert, dass es tatsächlich zu einer nachteiligen Auswirkung auf die Netz- und Informationssicherheit gekommen ist. Aus dem, in systematischer Hinsicht in den Regelungen für Anbieter digitaler Dienste fehlplatzierten Artikel 16 Abs. 5 NIS-RL folgt, dass Anbieter wesentlicher Dienste auch dann meldepflichtig sind, wenn der Sicherheitsvorfall durch einen Dritten als Anbieter digitaler Dienste, dessen Dienste der Anbieter wesentlicher Dienste in Anspruch nimmt, verursacht wird.[237]

Zur kohärenteren Feststellung des Ausmaßes der Auswirkungen eines Sicherheitsvorfalls gibt die NIS-Richtlinie in Art. 14 Abs. 4 drei zu berücksichtigende Parameter vor. Zu diesen quantitativen Kriterien gehören die Zahl der von der Unterbrechung betroffenen Nutzer, die Dauer des Sicherheitsvorfalls und die geografische Ausbreitung in Bezug auf das betroffene Gebiet. Anders als für die Sicherheitsvorfalle bei Anbietern digitaler Dienste besteht hier für die Kommission nicht die Möglichkeit, die Parameter der Erheblichkeitsschwelle mittels Durchführungsrechtsakten zu spezifizieren. Die im Rahmen der europäischen NIS-Kooperationsgruppe zusammenarbeitenden nationalen NIS-Behörden[238] können jedoch nach Art. 14 Abs. 7 NIS-RL Leitlinien ausarbeiten und annehmen, um die Umstände des meldepflichtigen Ereignisses und die Parameter zur Feststellung des Ausmaßes näher zu bestimmen. Leitlinien sind unionsrechtlich als Handlungsform für die Unionsorgane sowie die Festlegung der Unionspolitik oder Koordinierung der Politik der Mitgliedstaaten ausdrücklich vorgesehen.[239] Sie sind jedoch ihrer Natur nach grundsätzlich nicht verbindlich. In dem Katalog der Rechtsakte ist Art. 288 AEUV nicht genannt. Eine gewisse Verbindlichkeit kann Leitlinien jedoch zukommen, wenn sich dies dem Primär- oder Sekundär-

---

[237] Vgl. Erwägungsgrund 52 NIS-RL.

[238] Siehe § 4 B. II. 1. a).

[239] 26 Abs. 1 EUV, Art. 148 Abs. 2, Art. 171 Abs. 1 AEUV.

recht entnehmen lässt.[240] Im Sekundärrecht findet sich dann etwa der Imperativ der „weitestgehenden" Berücksichtigung der Leitlinien, teilweise mit Regelung einer Sanktionsfolge.[241] Aus den Leitlinien der NIS-Behörden im Sinne von Art. 14 Abs. 7 NIS-RL dürfte sich allenfalls ein schwach ausgeprägter Verbindlichkeitsgrad ergeben. Die Leitlinien-Kompetenz wird gerade keinem Unionsorgan zugewiesen. Eine Indikation der Verbindlichkeit gibt die Norm dem Adressaten nicht. Da die Leitlinien durch diejenigen Behörden angenommen werden, die sie auch anwenden, kommt den Leitlinien eine Verbindlichkeit im Sinne einer nicht sanktionsbewehrten Beachtungs- bzw. Berücksichtigungspflicht mit dem Zweck des einheitlichen Melde- und Verwaltungsvollzugs zu.

Nach der deutschen Umsetzung der Meldepflicht in § 8b Abs. 4 S. 1 BSIG müssen die Betreiber kritischer Infrastrukturen über eine Kontaktstelle dem BSI „erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen 1. führen können oder 2. geführt haben", gemeldet werden. Gemessen an der NIS-Richtlinie ist die deutsche Umsetzung der Meldepflicht strenger. Zur Voraussetzung der Meldepflicht gehört es gerade nicht, dass ein Sicherheitsvorfall Auswirkungen hat. Es genügt eine potenziell erhebliche Auswirkung oder Beeinträchtigung. Außerdem ist Bezugspunkt der Meldung eine Störung nicht nur der Verfügbarkeit, sondern auch der übrigen Schutzziele der Netz- und Informationssicherheit. Da die NIS-Richtlinie nach Art. 4 keine Voll-, sondern eine Mindestharmonisierung bezweckt, können die Mitgliedstaaten strengere Bestimmungen, mit denen ein höheres Sicherheitsniveau erreicht werden soll, erlassen oder aufrechterhalten.

Für die weitere Bestimmung der Merkmale des Meldetatbestandes kann aufgrund der terminologischen Unterschiede zu § 109 Abs. 5 TKG nicht von vorneherein auf die telekommunikationsrechtliche Meldepflicht verwiesen werden. Während Betreiber kritischer Infrastrukturen „erhebliche Störungen" zu melden haben, „die zu einem Ausfall oder einer Beeinträchtigung" führen können, haben Telekommunikationsnetzbetreiber oder -diensteanbieter „Beeinträchtigungen" zu melden, „die zu beträchtlichen Sicherheitsverletzungen" führen können und bestimmte „Störungen" einschließen können.

Die Nichtkongruenz der Meldetatbestände wirkt sich aber nicht am zentralen Begriff der Störung aus, sondern eher auf die Folge der Störung. Der Störungsbegriff wird im BSIG nicht näher bestimmt. Der Gesetzgeber geht jedoch davon

---

[240] *Ehlers*, in: Erichsen/Ehlers (Hrsg.), Allgemeines Verwaltungsrecht, 14. Aufl. 2010, § 5 II 5, Rn. 27.

[241] Zwei Beispiele bei *Rademacher*, Realakte im Rechtsschutzsystem der Europäischen Union, 2014, S. 127 f.

aus, dass Störung entsprechend dem telekommunikationsrechtlichen Verständnis und der Rechtsprechung zu § 100 Abs. 1 TKG funktional und insofern weit verstanden werden kann.[242] Für eine Störung kommt es daher auch im Rahmen von § 8b BSIG darauf an, ob die eingesetzte Technik die ihr zugedachte Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann oder ob versucht wurde, entsprechend auf sie einzuwirken.[243] Störung ist demnach mehr als nur die physikalische Beeinträchtigung technischer Einrichtungen und umfasst Fälle von Sicherheitslücken, Schadprogrammen und erfolgten oder versuchten oder erfolgreich abgewehrten Angriffen auf die Sicherheit in der Informationstechnik.[244]

Fraglich ist, wie das Merkmal der Erheblichkeit der Störung zu verstehen ist. Die Formulierung und der Relativsatz („erhebliche Störung […], die […]") deuten darauf hin, dass die Meldeschwelle am Grad der Störung zu messen ist und nicht auf den Grad der Beeinträchtigung der Funktionsfähigkeit einer kritischen Infrastruktur bezogen ist. Würde die Erheblichkeit am Grad der Störung gemessen, läge darin eine Abweichung von Art. 14 Abs. 4 NIS-RL, der ausdrücklich an die Erheblichkeit der Auswirkung des Vorfalls anknüpft. Ganz im unionsrechtlichen Sinne sieht der Gesetzgeber selbst eine erhebliche Störung dann als gegeben, wenn die Funktionsfähigkeit der erbrachten kritischen Dienstleistung bedroht ist.[245]

Gleichwohl lässt die Vorschrift wegen des unmittelbaren Zusammenhangs der Erheblichkeit zur Störung auch eine weitere Lesart zu.

Bei der Bestimmung der Erheblichkeit einer Störung könnte auch der durch eine Meldung generierte Erkenntnisgewinn berücksichtigt werden. Sofern der Gesetzgeber daran anknüpft, ob ein IT-Vorfall neuartig oder außergewöhnlich ist und nicht bereits automatisiert oder mit wenig Aufwand mit Hilfe der Maßnahmen, die dem „Stand der Technik" entsprechen sollen, abgewehrt werden können,[246] entspricht dieses Verständnis sogar der Regelungsintention. Nicht meldepflichtig sind dann alltägliche Vorfälle, die durch Spam, gewöhnliche Schadsoftware und typische Hardwareausfälle verursacht werden.[247] Erheblich sind nach diesem Verständnis Störungen, wenn sie durch Angriffe mit neuartigen Modi operandi verursacht wurden oder wenn sie unerwartete Vorkommnisse darstellen. Insbesondere sind dies fortgeschrittene und andauernde Cyberbedrohungen, d. h. komplexe, zielgerichtete und effektive Angriffe (sog. Advanced

---

242 BT-Drs. 18/4096, S. 27; vgl. *Moos*, MMR 2015, 636 (639).
243 BGH, NJW 2014, 2500 (2501).
244 BT-Drs. 18/4096, S. 27.
245 BT-Drs. 18/4096, S. 28.
246 BT-Drs. 18/4096, S. 28.
247 Vgl. auch *Gitter*/*Meißner*/*Spauschus*, DuD 2016, 7 (9).

Persistent Threats, APTs).[248] Für die Bestimmung der Erheblichkeit kann in diesem Sinne auch der Ressourcenaufwand als tauglicher Indikator herangezogen werden. Meldepflichtig sind demnach nur solche Angriffe, die nur mit erhöhtem Ressourcenaufwand, d. h. mit erhöhtem Koordinationsaufwand, durch Hinzuziehen von Experten, Nutzung einer besonderen Aufbauorganisation oder Einberufung eines Krisenstabs usw., abgewehrt oder in ihren Folgen neutralisiert werden können.

Gegen das Verständnis der Erheblichkeit, das auf den möglichen Neuigkeitswert einer Meldung abstellt, kann eingewandt werden, dass dann „einfache" Störungen, die zu fatalen Betriebsbeeinträchtigungen führen können, nicht meldepflichtig wären. Für eine insofern restriktivere Auslegung spricht, dass eine Vielzahl ausgelöster Meldungen sowohl die Unternehmen als auch die Behörden als Adressaten der Meldung überfordern könnte, sofern die Meldungen zusätzlich manuell bearbeitet werden müssen.

Vorzugswürdig ist schließlich jedoch ein Verständnis von Erheblichkeit, dass sowohl dem unionsrechtlichen Verständnis entspricht als auch den Bedarf der Informations- und Wissensgenerierung berücksichtigt. Die Erheblichkeit ist demnach mit Blick auf die Auswirkung eines Vorfalls, d. h. die Funktionsbeeinträchtigung, auszulegen. Hierbei sind die von Art. 14 Abs. 4 NIS-RL grob vorgegebenen Parameter und die nach Art. 14 Abs. 7 NIS-RL angenommenen Leitlinien heranzuziehen. Zusätzlich kann der Neuigkeitswert der Meldeinformationen berücksichtigt werden, indem die Erheblichkeit auch nach den Ursachen der Störung beurteilt wird. Überzogene Anforderungen dürfen hier aber an die Erheblichkeit nicht gestellt werden, da ein umfänglich die Risiken abbildendes Lagebild alle Störungen, die erhebliche Auswirkungen haben können, erfassen sollte.

Sofern die erhebliche Störung nur möglicherweise zu einem Ausfall oder einer Beeinträchtigung führt, obliegt die Entscheidung, ob eine Meldepflicht besteht, den Infrastrukturbetreibern. Sie haben insofern eine eigene Prognose zu stellen. Da dem Wortlaut nach bereits die entfernte Möglichkeit einer Beeinträchtigung genügt, um die Meldepflicht auszulösen, bietet sich für die Prognose die Anwendung einer „je-desto"-Formel an: Je schwerwiegender die durch die Beeinträchtigung verursachten Schäden sein können, desto geringer sind die Anforderungen an die Wahrscheinlichkeit der Beeinträchtigung.

bb) Inhalt der Meldung

Die zu meldenden Angaben werden durch § 8b Abs. 4 S. 2 BSIG gesetzlich abstrakt bestimmt. Notwendig sind vier Angaben. Die Meldungen müssen Angaben zur Störung, zu den technischen Rahmenbedingungen, insbesondere der

[248] Zu dieser Art Angriff *BSI*, Die Lage der IT-Sicherheit in Deutschland 2015, 2015, S. 26.

vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zur Branche des Betreibers enthalten. Die zu meldenden Informationen sind nicht abschließend genannt („insbesondere"). Eine Befugnis entsprechend § 4 Abs. 6 BSIG zur weiteren Konkretisierung durch Verwaltungsvorschrift oder entsprechend § 10 BSIG zur weiteren Bestimmung durch Rechtsverordnung sieht § 8b BSIG nicht vor. Insofern kann das BSI keine verbindliche, gesetzesausfüllende Regelung treffen. Die Gesetzesbegründung gibt an, dass das BSI unter Einbeziehung der Betreiber kritischer Infrastrukturen und der ansonsten zuständigen Aufsichtsbehörden Kriterien für meldungsrelevante Sicherheitsvorfälle aufstellt und entsprechend der jeweils aktuellen Sicherheitslage weiterentwickelt.[249] Solche Spezifizierungen für die meldepflichtigen Unternehmen sind zwar ebenfalls nicht verbindlich, zumal es sich bei den Tatbestandsvoraussetzungen – wie bei der telekommunikationsrechtlichen Meldepflicht – grundsätzlich um gerichtlich überprüfbare unbestimmte Rechtsbegriffe handelt.[250] Allerdings kann das Unterlassen einer nach der Konkretisierung nicht zu meldenden Information auch nicht sanktioniert werden.

Die maßgeblichen Kriterien für eine Präzisierung des Meldeinhalts sind am Zweck der Meldepflicht auszurichten. Dieser wird zunächst durch die organisationsrechtlichen Aufgabenbestimmungen des BSI vorgegeben. Nach § 8b Abs. 1 und 2 BSIG ist das BSI die zentrale Meldestelle, die die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik wesentlichen Informationen sammelt und auswertet, insbesondere mit Blick auf die Auswirkungen auf die Verfügbarkeit von kritischen Infrastrukturen analysiert und die das Lagebild über die Sicherheit kritischer Infrastrukturen kontinuierlich aktualisiert (vgl. auch § 3 Abs. 1 S. 2 Nr. 2 BSIG). Die Meldungen dienen demnach nicht dazu, der Meldebehörde lediglich die nachträgliche Kontrolle der implementierten technisch-organisatorischen Sicherheitsmaßnahmen zu ermöglichen. Dies ergibt sich außerdem aus der Differenzierung der Pflicht zur Nennung des Betreibers in der Meldung. Im Falle einer nur möglichen Beeinträchtigung durch die Störung kann die Meldung auch ohne Nennung des betroffenen Betreibers erfolgen. Nur bei einer tatsächlich eingetretenen Beeinträchtigung ist nach § 8b Abs. 4 BSIG eine pseudonyme Meldung nicht möglich.[251] Die Meldungen sollen dem BSI auch im Vorfeld konkreter Schadenseintritte ermöglichen, eine „möglichst umfassende und frühzeitige Warnung möglicherweise ebenfalls betroffener Betreiber Kritischer Infrastrukturen zu gewährleisten".[252] Die Meldungen sollen dazu beitragen,

[249] BT-Drs. 18/4096, S. 28.
[250] *Spindler*, CR 2016, 297 (301).
[251] Siehe dazu unter § 3 E. III. 2. (3).
[252] BT-Drs. 18/4096, S. 28.

die „Cyberbedrohungslage“ zu erfassen und „fundierte Aussagen zur IT-Sicherheitslage“ zu treffen.[253] Mit Blick auf die Informationsgenerierung erscheint ein detaillierter Meldekatalog nicht schon deshalb unverhältnismäßig, weil mit ihm eingriffsintensiver Aufwand für die Unternehmen verbunden ist.[254] Ein Großteil des Aufwandes zur Umsetzung der Meldepflicht würde bereits bei der Meldung des bloßen Umstandes eines Sicherheitsvorfalles entstehen.

Soweit die Betreiber bei der Meldung nur möglicher Beeinträchtigungen eine Prognose der Ausfall- und Beeinträchtigungswahrscheinlichkeit stellen, entspricht es dem Zweck der Meldung, auch andere Betreiber über Sicherheitsvorfälle zu informieren, sodass die meldepflichtigen Betreiber auch berücksichtigen, inwiefern auch andere Betreiber kritischer Infrastrukturen derselben Branche betroffen sein könnten. Dafür sprechen nicht zuletzt mögliche Interdependenzen und die mit einer Beeinträchtigung einhergehenden Kaskadeneffekte.[255] Die Betreiber könnten sich hier jedoch auf den Wortlaut von § 8b Abs. 4 S. 1 BSIG stützen, der auf die Funktionsfähigkeit „der von ihnen betriebenen“ kritischen Infrastrukturen abstellt und insofern keine Informationen über die Betroffenheit anderer Infrastrukturen erfordert. Allerdings ist unionsrechtlich erforderlich, dass die nationale NIS-Behörde in die Lage versetzt werden, die grenzüberschreitenden Auswirkungen eines Sicherheitsvorfalles zu bestimmen (Art. 14 Abs. 3 NIS-RL), um die Behörde in einem anderen Mitgliedstaat informieren zu können. Die Unternehmen müssten demnach verpflichtet werden, auch hinsichtlich des etwaigen grenzüberschreitenden Charakters des IT-Sicherheitsvorfalls eine Einschätzung zu melden.

Das vom BSI entwickelte Musterformular erfordert neben allgemeinen Informationen auch die Beschreibung der IT-Störung und der vermuteten Ursachen.[256] Im Wesentlichen sind dabei die einschlägigen Werte bei möglicher Mehrfachnennung anzukreuzen. Insgesamt fordert das BSI keine Beschreibung des Sicherheitsvorfalls unter Angabe aller verfügbarer Informationen, sondern nur eine Umschreibung. So ist etwa auch die Angabe sonstiger Informationen wie der CVE-Nummer, einem Industriestandard für die Bezeichnung und Kate-

---

[253] BT-Drs. 18/4096, S. 28.

[254] Zur Bürokratiekostenabschätzung die Studie im Auftrag des BDI von *KPMG*, IT-Sicherheit in Deutschland, Handlungsempfehlungen für eine zielorientierte Umsetzung des IT-Sicherheitsgesetzes, 2014, S. 27 ff., 34.

[255] Kritisch *Bräutigam*/*Wilmer*, ZRP 2015, 38 (40 f.).

[256] Bundesamt für Sicherheit in der Informationstechnik, Meldeformular nach § 8b Abs. 4 BSIG, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/Meldeformular_BSIG8b_Muster.pdf;jsessionid=6286F9CDCFEE52B9CA1A587A73D600EF.2_cid351?__blob=publicationFile&v=3.

gorisierung bekannter Sicherheitslücken,[257] den Betreibern anheimgestellt.[258] Das Muster sieht dagegen die Angabe der im Rahmen der bis zur Meldung durchgeführten Analyse der IT-Störung angefallenen Daten mit Blick auf eine etwaige nachträgliche Zurverfügungstellung vor. Insofern soll die Meldung dem BSI erlauben, die Relevanz für weitergehende Auskunftsanordnungen zu prüfen. Die Angabe aller dem Betreiber vorliegenden Informationen im Rahmen der Meldung dürfte aber wohl auf Grundlage von § 8b Abs. 4 BSIG nicht verlangt werden können, da in technischer Hinsicht nur die „Rahmenbedingungen" zu nennen sind. Insofern besteht zur telekommunikationsrechtlichen Meldepflicht kein wesentlicher Unterschied.

Ein Unterschied besteht vor dem Hintergrund der Eilbedürftigkeit auch nicht in der Frage einer gestuften Meldung. Um möglichst schnell in Krisensituationen zu reagieren und andere potenziell betroffene Kreise vor vergleichbaren Vorfällen zu warnen, ist eine schnellstmögliche Meldung ohne weiteren Rechercheaufwand ausreichend. Der Nachtrag zur initialen Meldung muss dann erschöpfend die Informationen enthalten, mit denen das BSI aus den Meldungen weitere Handlungen ableiten kann.

Aus der datenschutzrechtlichen Regelung in § 8b Abs. 7 BSIG ergibt sich, dass eine Meldung auch personenbezogene Daten enthalten kann.[259] Durch den Verweis auf § 5 Abs. 7 S. 3 bis 8 BSIG, der die Analyse von Daten im Rahmen der Sicherheitsgewährleistung der Kommunikationstechnik des Bundes betrifft, scheint der Gesetzgeber sogar davon auszugehen, dass Erkenntnisse aus dem Kernbereich privater Lebensgestaltung oder besonders sensible Daten erlangt werden können. Solche Erkenntnisse dürfen jedoch nicht verwendet werden und sind unverzüglich zu löschen.

c) Anbieter digitaler Dienste

Anbieter digitaler Dienste haben nach Art. 16 Abs. 3 NIS-RL Sicherheitsvorfälle an die zuständigen NIS-Behörden unverzüglich zu melden. Soweit die erfassten digitalen Dienste als Telemedien einzustufen sind, besteht *de lege lata* Umsetzungsbedarf für den Gesetzgeber, da im TMG keine Meldepflicht statuiert ist.

---

[257] Common Vulnerabilities and Exposures (CVE), dazu Mitre Corporation, abrufbar unter: http://cve.mitre.org/about/.

[258] Zweifelnd daran, ob der Inhalt der Meldung tatsächlich in der Praxis ausreicht, um genügend Informationen zu sammeln, *Spindler*, CR 2016, 297 (301); vgl. auch *Roth*, ZD 2015, 17 (21); *Roos*, MMR 2014, 723 (727); *Roßnagel*, DVBl. 2015, 636 (640).

[259] Siehe § 3 E. II.

aa) Anlass der Meldung

Während die Meldepflicht für die Betreiber wesentlicher Dienste an die Auswirkungen für die Verfügbarkeit der wesentlichen Dienste anknüpft, sind die Auswirkungen bei den digitalen Diensten nach Art. 16 Abs. 3 NIS-RL an deren „Bereitstellung" (engl. *provision*) zu messen. Die Bereitstellung bezieht sich dem Wortlaut nach zwar auch auf den Betrieb und damit auf die Verfügbarkeit des Dienstes. Die Verwendung verschiedener Begriffe für die Meldepflicht deutet jedoch auf eine unterschiedliche Bedeutung der Tatbestandsmerkmale hin. In systematischer Hinsicht ergibt sich dies auch aus Art. 16 Abs. 2 NIS-RL, der die Mitgliedstaaten dazu verpflichtet, sicherzustellen, dass die Anbieter digitaler Dienste Maßnahmen treffen, „damit die Verfügbarkeit [engl. *continuity*] dieser Dienste gewährleistet wird." Erwägungsgrund 48 der NIS-Richtlinie weist darauf hin, dass „die Sicherheit, Verfügbarkeit und die Verlässlichkeit der […] digitalen Dienst[e]" für das Funktionieren vieler Unternehmen von wesentlicher Bedeutung sei. Diese Erwägung deutet auf ein weites Verständnis von Bereitstellung in dem Sinne hin, dass sich die Bereitstellung nicht auf das Schutzziel der Verfügbarkeit beschränkt, sondern darüber hinaus auch Schutzziele wie die Integrität und Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder entsprechender Dienste umfasst (vgl. Art. 4 Nr. 2 NIS-RL).

Die Meldeschwelle ist im Vergleich zur Meldepflicht von Betreibern wesentlicher Dienste darüber hinaus in zwei Punkten modifiziert. Bei der Feststellung, ob die Auswirkungen eines Sicherheitsvorfalles erheblich sind, werden zusätzliche Parameter berücksichtigt. So sind die Zahl der betroffenen Nutzer, die Dauer des Sicherheitsvorfalls, das Ausmaß der Unterbrechung der Bereitstellung des Dienstes sowie das Ausmaß der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten zu berücksichtigen (Art. 16 Abs. 4 NIS-RL).

Eingeschränkt wird die Meldepflicht dadurch, dass sie nur greift, wenn der Anbieter Zugang zu den Informationen hat, die benötigt werden, um die Auswirkungen eines Sicherheitsvorfalls zu bewerten. Diese Regel hat zwei informationsrechtliche Implikationen. Zum einen spricht sie dafür, dass die Anbieter nicht schon aus der Meldepflicht heraus verpflichtet sind, alle oder bestimmte Aktionen in ihren Computersystemen und Netzwerken zu Analysezwecken zu protokollieren. Zum anderen wird damit die Effektivität der Informationsgenerierung abgeschwächt. Die Anbieter digitaler Dienste haben es ein Stück weit selbst in der Hand, die Meldepflicht zu aktivieren. So könnte etwa aus Kostengründen die grundsätzlich bestehende Pflicht umgangen werden, indem Unternehmen verhindern, Daten für die Bewertung von Sicherheitsvorfällen zu erheben.

bb) Konkretisierung durch Durchführungsakte der Kommission

Anders als bei den Meldungen der Infrastrukturbetreiber hat die Kommission die aufgrund von Art. 291 Abs. 2 AEUV und der NIS-RL als Basisrechtsakt eingeräumte Möglichkeit, eine Feinsteuerung der Notifizierungspflicht vorzunehmen und unionsweit zu vereinheitlichen. Art. 16 Abs. 8 und 9 NIS-RL geben der Kommission die Kompetenz, Durchführungsakte zu erlassen, um zum einen die Parameter zur Bestimmung der Erheblichkeit eines Sicherheitsvorfalls und zum anderen die Form und das Verfahren, welche für Meldepflichten gelten, festzulegen.

Abweichend von der Regelvollzugszuständigkeit der Mitgliedstaaten können Sekundärrechtsakte gemäß Art. 291 Abs. 2 AEUV Befugnisse zur Durchführung an die Kommission übertragen. Durchführung im Sinne von Art. 291 AEUV meint den Erlass detaillierter Regelungen, die die Anwendung des Unionsrechts erleichtern, indem sie die darin gemachten Vorgaben konkretisieren.[260] Von der Durchführung nicht umfasst ist der Erlass normativer Akte zur Ergänzung oder Änderung nicht wesentlicher Vorschriften eines Gesetzgebungsakts. Diese Befugnis unterfällt der Delegation nach Art. 290 AEUV.[261]

Durchführungsakte der Kommission können neben individuell-konkreten Rechtsakten auch solche mit allgemeiner Geltung umfassen. Dies ergibt sich aus Art. 267 und 277 AEUV, bei denen es um die Auslegung und Geltung von „Rechtsakten allgemeiner Geltung" eines Organs, einer Einrichtung oder einer sonstigen Stelle der Union geht. Wenn mit „Einrichtungen" auch Agenturen gemeint sind, gilt dies erst recht für die Kommission bei der Durchführung von Unionsrecht.[262] In diesem Sinne sah auch der Entwurf einer neuen Interinstitutionellen Vereinbarung zur besseren Rechtsetzung vor, dass eine allgemeine „Maßnahme, die sich auf Vorkehrungen für die Bereitstellung von Informationen" bezieht, in der Regel als Durchführungsrechtsakt der Kommission erlassen werden soll, da eine solche Vorgabe „im Allgemeinen keine Ergänzung der Verpflichtung zur Bereitstellung von Informationen [darstellt], sondern […] vielmehr eine einheitliche Durchführung ermöglicht."[263] Allgemeine Durchführungsakte nach Art. 16 Abs. 9 NIS-RL in Verbindung mit Art. 291 Abs. 2 AEUV sollen damit technische Details vorgeben, die die weitere Durchführung leiten. Konkretisiert werden können also etwa die Bemessungsmaßstäbe der Er-

[260] GA *Jääskinen*, Schlussanträge in der Rs. C-270/12, Rn. 77; a. A. *Stelkens*, EuR 2012, 511 (544).

[261] EuGH, C-427/12, Rn. 36.

[262] *Weiß*, EuR 2016, 631 (645); vgl. GA *Jääskinen*, Schlussanträge in der Rs. C-270/12, Rn. 79.

[263] Entwurf zu einer Interinstitutionellen Vereinbarung über bessere Rechtsetzung, COM (2015) 216 endg., Anhang 1, Rn. 13.

heblichkeit eines Sicherheitsvorfalles, das Format oder das anzuwendende Meldeverfahren. Wesentliche Ergänzungen oder Änderungen dürfen nicht über die Durchführungsakte geregelt werden.

Die allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren, werden gemäß Art. 291 Abs. 3 AEUV durch Verordnung im Voraus festgelegt. Die Verordnung (EU) Nr. 182/2011 (Komitologie-VO) stellt diese Regeln auf und bestimmt, wie Detailentscheidungen in Ausschüssen der EU-Mitgliedstaaten unter Vorsitz der Kommission getroffen werden. Für die mitgliedstaatliche Kontrolle durch die Mitgliedstaaten der Wahrnehmung der Durchführungsbefugnisse durch die Kommission enthält die Komitologie-VO zwei Verfahren, das Beratungsverfahren (*advisory procedure*), Art. 4, und das Prüfverfahren (*examination procedure*), Art. 5 Komitologie-VO. Im regulären Beratungsverfahren gibt der Ausschuss eine Stellungnahme mit einfacher Mehrheit seiner Mitglieder ab. Die Kommission kann die Stellungnahme berücksichtigen, ist aber in keiner Weise an sie gebunden. Im strengeren Prüfverfahren kann sich die Kommission grundsätzlich nicht über eine Ablehnung des Ausschusses mit qualifizierter Mehrheit hinwegsetzen. Welches der beiden Verfahren angewendet wird, soll im Basisrechtsakt festgelegt werden.

Die Durchführungsrechtsakte werden gemäß Art. 16 Abs. 8 und 9 in Verbindung mit Art. 22 Abs. 2 NIS-RL im Prüfverfahren erlassen. Die Kommission wird gemäß Art. 22 Abs. 1 NIS-RL von dem Ausschuss für die Sicherheit von Netz- und Informationssystemen unterstützt.

Die Wahl des Prüfverfahrens indiziert, dass es sich beim Erlass den konkretisierenden Rechtsakte um solche von allgemeiner Tragweite mit potenziell bedeutenden Auswirkungen handeln kann.[264] Im Ergebnis ist damit bei der Ausgestaltung der Meldepflicht zwar die Erfüllung des europäischen Informationsinteresses von ausschlaggebender Bedeutung. Der Einfluss der Mitgliedstaaten ist aber durch ihre Repräsentation im Ausschuss für die Sicherheit von Netz- und Informationssystemen und den Entscheidungsmodus im Prüfverfahren gesichert.

cc) Inhalt der Meldung

Zum Inhalt der Meldung macht Art. 16 NIS-RL kaum Vorgaben. Nach Art. 16 Abs. 1 S. 2 NIS-RL müssen die Meldungen lediglich Informationen enthalten, die es der zuständigen Behörde oder dem CSIRT ermöglichen, das Ausmaß etwaiger grenzübergreifender Auswirkungen des Sicherheitsvorfalls festzustellen. Näher bestimmt wird der Inhalt auch nicht durch die Durchführungsakte

[264] Art. 2 und Erwägungsgrund 11 VO (EU) Nr. 182/2011.

der Kommission, da diese neben der Meldeschwelle nur die Form und das Verfahren der Meldung betreffen.

Aus dem Sinn und Zweck der Meldepflicht ergibt sich aber auch hier, dass sich der Inhalt nicht auf die Meldung des Umstands eines Sicherheitsvorfalls als solchen beschränken kann. Die Meldung der Tatsache, dass es zu einem Vorfall gekommen ist, würde zudem kaum als „Nachweis" (engl. *evidence*) im Sinne des Art. 17 Abs. 1 NIS-RL genügen, um die NIS-Behörden zur nachträglichen Überprüfung der implementierten Sicherheitsmaßnahmen zu veranlassen. Die Meldung lediglich des Sicherheitsvorfalls würde nur dann einen nachvollziehbaren Zweck erfüllen, wenn für die *Ex-post*-Überwachungsmaßnahmen bereits Anhaltspunkte dafür, dass der Anbieter die Sicherheitsanforderungen nicht einhält, ausreichten, da der gemeldete Vorfall ein Hinweis auf ein ungenügendes Risikomanagement bei dem Anbieter sein kann.

Da die NIS-Behörde ggf. bei Betroffenheit von zwei oder mehr Mitgliedstaaten deren NIS-Behörden unterrichtet, werden zu dem wesentlichen Meldeinhalt auch Informationen über die im Einzelnen betroffenen Mitgliedstaaten zu rechnen sein. Außerdem dürfte zum Mindestgehalt der Meldung die Angabe derjenigen Informationen gehören, aus denen sich die Erheblichkeit des Sicherheitsvorfalls ergibt, denn Art. 16 Abs. 4 S. 2 NIS-RL knüpft die Meldepflicht daran, dass der Anbieter auch Zugang zu diesen Informationen hat.

Die Mitgliedstaaten sind im Übrigen weitgehend frei darin, den Meldeinhalt zu konkretisieren. Unterschiedliche und strengere Anforderungen an die Meldungen in den Mitgliedstaaten sind auch nicht durch Art. 16 Abs. 10 NIS-RL ausgeschlossen, da diese Regelung den Mitgliedstaaten nur untersagt, den Anbietern digitaler Dienste keine weiteren Sicherheits- oder Meldepflichten aufzulegen.

d) Meldung auf freiwilliger Basis

Meldungen müssen nicht notwendig auf Rechtspflichten beruhen. Informationen über Sicherheitsvorfälle können auch auf Basis freiwilliger Meldungen generiert werden.

Freiwillige Meldungen kommen insbesondere für diejenigen Unternehmen in Betracht, die nicht in den Anwendungsbereich der NIS-Richtlinie fallen, d. h. vor allem Kleinst- sowie kleine und mittlere Unternehmen im Sinne der Empfehlung 2003/361/EG. Diese sind unter dem Gesichtspunkt der Verhältnismäßigkeit nicht von den technisch-organisatorischen Sicherheitsanforderungen und den Meldepflichten betroffen. Die NIS-Richtlinie geht davon aus, dass eine Meldung aufgrund der autonomen Entscheidung des Unternehmens möglich

sein soll, wenn es im öffentlichen Interesse ist, dass der Auftritt eines Sicherheitsvorfalls gemeldet wird.[265]

Ein eigenständiges Meldeverfahren besteht für freiwillige Meldungen nicht. Art. 20 Abs. 1 NIS-RL trifft jedoch eine Regelung für die freiwillige Meldung solcher Sicherheitsvorfälle, die erhebliche Auswirkungen auf die Verfügbarkeit von vom meldenden Unternehmen angebotenen Dienste haben. Melden die Unternehmen, die nicht vom persönlichen Anwendungsbereich der NIS-Richtlinie erfasst sind, einen solchen Sicherheitsvorfall freiwillig, findet das für die Betreiber wesentlicher Dienste vorgesehene Meldeverfahren Anwendung (Art. 20 Abs. 2 NIS-RL). Auf die Leitlinien der Kooperationsgruppe kommt es insofern nicht an, weil diese die Umstände näher bestimmen, unter denen Sicherheitsvorfälle gemeldet werden müssen.

Der spezifische Anreiz, der von der Möglichkeit derartiger Meldungen ausgeht, dürfte weniger altruistisch sein. Die von dem Sicherheitsvorfall betroffenen Unternehmen haben ein rechtlich schützenswertes Interesse daran, den Schaden zu begrenzen, der durch den Sicherheitsvorfall bei Dritten entstehen kann. Ein Unternehmen, dass von einem vorsätzlichen Cyberangriff betroffen ist, trifft zwar grundsätzlich kein Mitverschulden. Es gilt der Grundsatz, dass ein fahrlässiges Mitverschulden des Geschädigten bei Vorsatz des Angreifers regelmäßig zurücktritt.[266] Ein zivilrechtliches Mitverschulden gemäß § 254 Abs. 2 S. 1 BGB nach einem erfolgten Cyberangriff wäre aber denkbar, wenn das angegriffene Unternehmen nach dem Angriff keine schadensmindernden Maßnahmen vornimmt und sich der Schaden weiter ausweitet.[267] Die Anreizwirkung wird prinzipiell verstärkt durch die unionsrechtliche Vorgabe in Art. 20 Abs. 2 UAbs. 2 NIS-RL, nach der die freiwillige Meldung keine Haftungsfolge nach sich ziehen darf, die das Unternehmen ohne die Meldung nicht hätte.

Inwiefern ein Schaden durch die freiwillige Meldung verhindert oder begrenzt werden kann, ist davon abhängig, wie zügig die Meldung bearbeitet wird. Aus Art. 20 Abs. 2 S. 2 NIS-RL folgt, dass Pflichtmeldungen vorrangig von der NIS-Behörde oder dem CSIRT bearbeitet werden können. Im Übrigen besteht der Anspruch auf Bearbeitung der Meldung auch nur, wenn sie für den Adressaten keinen unverhältnismäßigen oder unzumutbaren Aufwand darstellt (Art. 20 Abs. 2 S. 3 NIS-RL).

Dass die Meldungen von den zuständigen Behörden nicht prioritär zu verarbeiten sind, hat zwar keine unmittelbaren Auswirkungen für die Wissensproduktion auf administrativer Seite. Relevant mit Bezug auf die informationsverwaltungs-

---

[265] Erwägungsgrund 67 NIS-RL.

[266] *Grüneberg*, in: Palandt, BGB, 75. Aufl. 2016, § 254 Rn. 65.

[267] Zu den Haftungsverhältnissen bei Cyberangriffen und zum Mitverschulden *Mehrbrey/Schreibauer*, MMR 2016, 75 (80).

rechtliche Effektivität freiwilliger Meldungen ist jedoch, dass die Anwendung des Meldeverfahrens nur bei Sicherheitsvorfällen greift, die erhebliche Auswirkungen auf die „Verfügbarkeit" der von den Unternehmen angebotenen Dienste haben. Für Angriffe auf die Authentizität, die Integrität oder die Vertraulichkeit entsprechender Dienste, also auf grundsätzlich von der NIS-Richtlinie umfassten Schutzzielen (Art. 4 Nr. 2 NIS-RL), gilt demnach das Melderegime für freiwillige Meldungen nicht. Daraus folgt noch nicht, dass eine Generierung freiwillig gemeldeter Informationen für andere Angriffsklassen nicht erfolgt. Die rechtliche Anreizwirkung wird durch die Begrenzung allerdings geschwächt.

3. Meldepflicht bei Datenschutzverletzungen

Betrifft eine Sicherheitsverletzung zugleich die Sicherheit personenbezogener Daten, sind unter bestimmten Voraussetzungen sowohl die Aufsichtsbehörden als auch die Betroffenen über Verletzungen zu informieren. Ist die Aufsichtsbehörde zu informieren, handelt es sich um Meldepflichten. Davon abzugrenzen sind die Benachrichtigungspflichten, aufgrund derer die Betroffenen selbst durch den datenschutzrechtlich Verantwortlichen zu benachrichtigen sind.[268] Zu unterscheiden sind die Meldepflichten auf Grundlage des allgemeinen Datenschutzrechts, das auch für Anbieter von Telemediendiensten Anwendung findet (a), von denen im Telekommunikationsrecht (b).

a) Meldepflicht im allgemeinen Datenschutzrecht

Alle datenverarbeitenden Stellen trifft nach § 42a BDSG eine Benachrichtigungspflicht im Falle einer bestimmten Verletzung des Schutzes personenbezogener Daten. Für Anbieter von Telemediendiensten gilt § 42a BDSG über den Rechtsfolgenverweis in § 15a TMG entsprechend. Eine europarechtliche Grundlage für § 15a TMG besteht ebenso wenig wie für § 42a BDSG. Der materielle Rechtsgedanke einer Informationspflicht der verantwortlichen Stelle bei bestimmten Verstößen gegen geltendes Datenschutzrecht knüpft jedoch an die damals noch im Entwurfsstadium befindliche Änderungsrichtlinie RL 2009/136/EG an.[269]

In der DS-GVO finden sich entsprechende Meldepflichten gegenüber der Aufsichtsbehörde (Art. 33) und gegenüber der betroffenen Person (Art. 34). Da die Art. 32 ff. DS-GVO im Abschnitt 2 „Sicherheit personenbezogener Daten" enthalten sind, können sie in systematischer Hinsicht der Datensicherheit zugeordnet werden. Zusätzliche datenschutzrechtliche Meldepflichten im Unions-

---

[268] *Hanloser*, MMR 2010, 300 (300).

[269] *Kühling*/*Seidel*/*Sivridis*, Datenschutzrecht, 3. Aufl. 2015, Rn. 670.

recht sind insbesondere nicht für Anbieter digitaler Dienste ausgeschlossen, da Art. 16 Abs. 10 NIS-RL nur zusätzliche Meldepflichten untersagt, die die Mitgliedstaaten auferlegen.

aa) Anlass der Meldung

Die datenschutzrechtliche Informationspflicht des § 42a BDSG gegenüber Aufsichtsbehörden greift bei Datenschutzverletzungen. Anlass zur Meldung sind nach § 42a BDSG jedoch nur solche Vorfälle, die besonders sensible Daten betreffen. Dazu gehören solche Daten, die als besondere Arten personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG zu qualifizieren sind (etwa Angaben zu Gesundheit, religiösen oder philosophischen Überzeugung), personenbezogene Daten, die einem Berufsgeheimnis unterliegen, die im Zusammenhang mit der Strafverfolgung stehen oder die Bank- bzw. Kreditkarten betreffen.

Die maßgebliche Verletzung nach § 42a BDSG ist die unrechtmäßige Übermittlung oder die unrechtmäßige Kenntnisnahme durch Dritte. Unrechtmäßig ist die Übermittlung oder Kenntniserlangung durch Dritte, wenn sie weder durch eine Rechtsvorschrift gedeckt ist noch die Einwilligung des Betroffenen vorliegt, § 4 Abs. 1 BDSG. Ist die Übermittlung Ergebnis einer Interessenabwägung, kommt es darauf an, ob die Abwägung „offensichtlich unhaltbar" ist.[270] Gewissheit darüber, ob es zu einer Kenntnisnahme durch Dritte gekommen ist, ist nicht erforderlich. Zum Teil sollen tatsächliche Anhaltspunkte dafür genügen.[271] Die Meldepflicht des BDSG greift zudem nur, wenn schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen. Auch wenn jede Sicherheitspanne, die personenbezogene Daten betrifft, *per se* eine Missbrauchsgefahr zu Lasten des Betroffenen darstellt, hängt die Entstehung der Meldepflicht von den potenziellen Auswirkungen der Datenschutzverletzung ab.[272] Mit der Beschränkung der Pflicht auf schwerwiegende Beeinträchtigungen hat der Gesetzgeber vor allem eine Hürde normiert, um Bagatellfälle auszuschließen und so Gewöhnungs- und Abstumpfungseffekte zu vermeiden.[273]

Mit Art. 33 DS-GVO ist die Schwelle für das Entstehen einer Meldepflicht erheblich gesenkt worden. Während die Pflicht des § 42a BDSG nur im Fall der Verletzung besonders sensibler Daten greift, erweitert Art. 33 DS-GVO den Anwendungsbereich unterschiedslos auf alle Arten personenbezogener Daten.

---

[270] *Dix*, in: Simitis, BDSG, 8. Aufl. 2014, § 42a Rn. 7.

[271] *Hornung*, NJW 2010, 1841 (1842); *Herbst*, in: Auernhammer, BDSG, 4. Aufl. 2014, § 42a Rn. 18.

[272] Vgl. *Duisberg*/*Picot*, CR 2009, 823 (824).

[273] *Hanloser*, CCZ 2010, 25 (26).

Eine nähere Spezifizierung nimmt Art. 33 Abs. 1 DS-GVO nicht vor. Allerdings definiert Art. 4 Abs. 3 DS-GVO den Begriff der Verletzung. Die Definition knüpft ausdrücklich an die „Verletzung der Sicherheit" an. Erfasst ist nicht nur die beabsichtigte oder unbeabsichtigte Vernichtung, der Verlust oder die Veränderung, sondern auch die unbefugte Offenbarung von bzw. der unbefugte Zugang zu verarbeiteten Daten.

Die unionsrechtliche Meldepflicht des Art. 33 Abs. 1 DS-GVO ist ebenfalls abhängig von der Qualität der Datenschutzverletzung. Nach Art. 33 Abs. 1 Hs. 2 DS-GVO ist die Verletzung lediglich dann nicht zu melden, wenn positiv festgestellt werden kann, dass ein Risiko für die Rechte und Freiheiten natürlicher Personen aus der Datenschutzverletzung nicht folgt („es sei denn"). Erforderlich ist, dass der Verantwortliche eigenverantwortlich eine Risikoabwägung („voraussichtlich") vornimmt.[274] Kriterien für eine Risikoabschätzung sind in der Norm nicht vorgegebenn. Aus dem Wortlaut der Vorschrift ergibt sich, dass bereits ein einfaches Risiko für die Begründung der Meldepflicht ausreicht („zu einem Risiko"). Eine schwerwiegende Beeinträchtigung für Rechte und Freiheiten muss gerade nicht drohen. Überdies sind nicht nur die Rechte und Freiheiten des Betroffenen (etwa eines Kunden) erfasst. Zu berücksichtigen sind die geschützten Rechtsgüter aller natürlichen Personen („natürlicher Personen"). Für die weitere Risikobewertung kann der Risikokatalog in Erwägungsgrund 75 der DS-GVO herangezogen werden. Bei der Abwägung sind materielle und immaterielle Schäden zu berücksichtigen.

In zeitlicher Hinsicht ist die Meldung an die Aufsichtsbehörden nicht davon abhängig, ob der Verantwortliche angemessene Sicherheitsmaßnahmen getroffen hat. Die Benachrichtigung der Betroffenen kann davon abhängig gemacht werden, ob ein Software-Hersteller über eine Sicherheitslücke informiert und ihm eine Frist zur Beseitigung von Schwachstellen gesetzt wurde. Die Meldung ist an die Aufsichtsbehörde hat dagegen unverzüglich und möglichst binnen 72 Stunden zu erfolgen. Die Benachrichtigung an die betroffenen Personen hat dagegen eine höhere Meldeschwelle. Der Behörde wird aufgrund des Geheimnisschutzes ein höherer Grad an Verschwiegenheit beigemessen,[275] sodass weder die Strafverfolgung gefährdet noch das Ausnutzen einer Schwachstelle seitens der Datenschutzaufsicht als grundsätzliche Gefahr angenommen wird.

bb) Inhalt der Meldung

Die der Aufsichtsbehörde zu meldenden Informationen lassen sich gliedern in solche der Risikobewertung, der Faktenmitteilung sowie der Folgenanalyse.

[274] Vgl. Erwägungsgrund 85 DS-GVO.

[275] *Dix*, in: Simitis (Hrsg.), BDSG, 8. Aufl. 2014, § 42a Rn. 16.

Der Aufsichtsbehörde sind nach § 42a S. 2 bis 4 BDSG neben der Information über den Umstand, dass Daten unrechtmäßig Dritten übermittelt wurden oder zu deren Kenntnis gelangt sind, Informationen über die „Art der unrechtmäßigen Kenntniserlangung" zu geben, die möglichen nachteiligen Folgen der Verletzung darzulegen sowie die von der verantwortlichen Stelle ergriffenen Abwehrmaßnahmen mitzuteilen. Art. 33 Abs. 3 lit. a bis d DS-GVO verlangt hinsichtlich des Mindestinhalts darüber hinaus die „Beschreibung" der Art der Verletzung, und, soweit möglich, die Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze, die Kontaktdaten sowie die Beschreibung vorgeschlagener Abhilfemaßnahmen.

Die Art der Verletzung des Schutzes personenbezogener Daten bezieht sich auf die vier datenschutzrechtlich zu unterscheidenden Verletzungsmöglichkeiten Vernichtung, Verlust, Veränderung und unbefugte Offenbarung (vgl. Art. 4 Nr. 12 DS-GVO). Die weiteren Angaben zu den Datenkategorien stehen unter Machbarkeitsvorbehalt („soweit möglich").

Da sich im Umkehrschluss aus Art. 34 DS-GVO für die Meldepflicht des Art. 33 DS-GVO keinerlei Formanforderungen ergeben, können weitere inhaltliche Vorgaben keinen diesbezüglichen Konkretisierungen entnommen werden. Aus Art. 33 Abs. 3 DS-GVO ergibt sich lediglich, dass die Informationen schrittweise, d. h. in Form einer Erst- und Zweitmeldung, übermittelt werden können.

Wie umfassend der Inhalt der Meldung, insbesondere die Beschreibung der Art der Verletzung, sein muss, ist letztlich eine Frage des mit der datenschutzrechtlichen Meldepflicht verfolgten Zwecks.

Der systematische Vergleich mit der Benachrichtigung der Betroffenen ergibt, dass der Aufsichtsbehörde zusätzliche Informationen mitzuteilen sind (vgl. § 42a S. 3 BDSG, Art. 34 Abs. 3 DS-GVO). Der Erkenntnisgewinn der Behörde soll demnach weitergehend sein. Aus der umfassenden Dokumentationspflicht des Verantwortlichen bei Datenpannen gemäß Art. 33 Abs. 5 DS-GVO folgt wiederum eine Begrenzung der zu meldenden Informationen. Die Dokumentation soll der Aufsichtsbehörde die Überprüfung der Einhaltung der Meldepflicht ermöglichen. Die Dokumentationspflicht zu Kontrollzwecken wäre weitgehend funktionslos, wenn die zu meldenden und dokumentierenden Informationen deckungsgleich wären. Die Dokumentationspflicht ist sehr weit, da ausnahmslos jede Datenschutzverletzung unabhängig von der Risikoabwägung zu dokumentieren ist („dokumentiert Verletzungen"). Mit der Dokumentation ist ein erheblicher Aufwand für Datensammlung verbunden. Erfasst sind alle mit der Verletzung im Zusammenhang stehenden „Fakten", Auswirkungen und ergriffenen Maßnahmen. Im Umkehrschluss folgt daraus, dass die Mitteilung einer „Be-

schreibung der Art der Verletzung“ nach Art. 33 Abs. 3 lit. a DS-GVO nicht notwendig so zu verstehen ist, dass detaillierte Informationen über das „Wie“ der Verletzung, d. h. über Schwachstellen oder die für einen Angriff ausgenutzten Sicherheitslücken, zu melden sind.

Dass die Datenschutzaufsicht durch die Meldepflicht nicht zu einer umfassenden Generierung von sicherheitstechnischen Informationen im Kontext von Datenschutzverletzungen angehalten werden soll, entspricht auch der Intention des Gesetzgebers. Die Meldepflicht soll die Behörde vor allem in den Stand versetzen, sicherzustellen, dass der datenschutzrechtliche Verstoß beseitigt wird.[276] Auch Art. 33 DS-GVO soll in erster Linie dem verfahrensrechtlichen Schutz der Rechte und Freiheiten des Betroffenen durch Verbesserung des aufsichtsbehördlichen Informationsstands dienen.[277] Demnach sind nur Informationen erforderlich, die für aufsichtsrechtlichen Maßnahmen nach § 38 Abs. 5 BDSG bzw. Art. 58 Abs. 6 DS-GVO erforderlich sind.[278] Um die Aufsicht in die Lage zu versetzen, die Erforderlichkeit des Abrufs der genauer dokumentierten Informationen zu prüfen, bedarf es in der Vorstufe zunächst nichts weiter als der Meldung von Metadaten über die Umstände der Datenschutzverletzung. Der möglichen Intervention durch die Aufsichtsbehörde dient letztlich auch die mitzuteilende Folgenabschätzung, denn in Verbindung mit Erfahrungswerten kann die Behörde darauf eine eigene Bewertung stützen. Der Mitteilung technischer Einzelheiten und damit eventuell verbunden der Preisgabe von Betriebs- und Geschäftsgeheimnissen bedarf es für die Entscheidung des weiteren Vorgehens noch nicht.[279] Es reicht daher grundsätzlich eine typisierende Darstellung des Vorfalls.[280] Wird der Sinn der Meldepflicht auch darin gesehen, präventiv den „Verheimlichungsinteressen“ der Unternehmen an der Offenlegung von Datenmissbräuchen entgegenzuwirken[281] oder ihnen Anreize für die Implementation besserer Sicherheitsstandards zu setzen,[282] ergibt sich ebenfalls kein Erfordernis einer umfassenden Meldung, da diese Zwecke auch mit einem Weniger an Informationen erfüllt werden. Im Übrigen können zur zwangsweisen Durchsetzung der Verpflichtungen der verantwortlichen Stelle, insbesondere dazu, dem

---

[276] BT-Drs. 16/12011, S. 35.

[277] *Martini*, in: Paal/Pauly, DS-GVO, 2017, Art. 33 Rn. 10, 61.

[278] Vgl. Erwägungsgrund 87 S. 3 DS-GVO.

[279] *Hornung*, NJW 2010, 1841 (1843).

[280] *Hanloser*, CCZ 2010, 25 (28).

[281] Vgl. *Höhne*, jurisPR-ITR 20/2009 Anm. 3, B.

[282] *Picanso*, Fordham L. Rev. 2006, 355 (382 ff.); vgl. *Hornung*, NJW 2010, 1841 (1841); ENISA, Data breach notifications in the EU, 2011, S. 8; ferner Bericht der *University of California – Berkeley School of Law*, Security Breach Notification Laws, 2007, S. 7; *Krupna*, BB 2014, 2250 (2252) mit dem Hinweis darauf, dass durch detailreiche Meldungen Bußgelder vermieden und damit der Verwaltungsaufwand insgesamt reduziert werden kann.

Betroffenen Abhilfemaßnahmen zu empfehlen, hilfsweise ergänzende Informationen angefordert werden. Daher sind in der Meldung zwingend auch die Kontaktdaten anzugeben.

Die Sammlung von Informationen zur präventiven und strukturellen Abwehr von Gefahren für die Informationssicherheit ist kein primärer Zweck der datenschutzrechtlichen Meldepflicht. Soweit aus den gemeldeten Informationen Wissen produziert werden kann, stellt sich dies als positiver Reflex der Meldepflicht dar.

b) Meldepflicht im Telekommunikationsrecht

Für Anbieter von Telekommunikationsdiensten besteht ebenfalls eine Meldepflicht, die an die Verletzung des Schutzes personenbezogener Daten anknüpft. Sie beruht aber nicht auf dem allgemeinen Datenschutzrecht, sondern auf der sektorspezifischen Regelung in Art. 4 Abs. 3 und 4 RL 2002/58/EG in Verbindung mit der Änderungs-RL 2009/136/EG (E-Privacy-Richtlinie).[283] Die Regelung wurde mit § 109a TKG umgesetzt. Während in binnensystematischer Hinsicht die Meldepflicht in § 109 TKG die Sicherheit der Netzwerke und Dienste betrifft, zielt die Meldepflicht in § 109a TKG auf die Sicherheit der Verarbeitung von personenbezogenen Daten. Da eine Sicherheitsverletzung gleichzeitig eine Netzsicherheits- wie eine Datenschutzverletzung sein kann, teilen die Normen eine Schnittmenge.[284]

Im Vergleich zu den anderen an die Verletzung personenbezogener Daten anknüpfenden Pflichten ist die Meldung jedoch nicht notwendigerweise an die Datenschutzaufsichtsbehörde zu richten. Adressat ist gemäß Art. 4 Abs. 3 E-Privacy-RL die „zuständige nationale Behörde". Die mitgliedstaatliche Organisationsautonomie erlaubt insofern auch, die Regulierungsbehörde als zuständige Behörde zu bestimmten. Der deutsche Gesetzgeber hat von der Freiheit Gebrauch gemacht und sowohl die Datenschutzaufsicht, hier den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, als auch die Bundesnetzagentur zu Adressaten der Meldungen gemacht.

aa) Anlass der Meldung

In sachlicher Hinsicht wird die Pflicht durch jede Verletzung des Schutzes personenbezogener Daten ausgelöst. Nach der Terminologie von Art. 2 UAbs. 2 lit. 1) E-Privacy-RL ist darunter eine Sicherheitsverletzung zu verstehen, die auf unbeabsichtigte oder unrechtmäßige Weise zur Vernichtung, zum Verlust, zur

---

283 Vgl. Art. 95 DS-GVO.

284 *ENISA*, Technical Guidelines on Security measures for Article 4 and 13a, 2014, S. iii.

Veränderung und zur unbefugten Weitergabe von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übertragen, gespeichert oder auf andere Weise im Zusammenhang mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in der Gemeinschaft verarbeitet werden. Daraus ergibt sich zunächst, dass eine Verletzung des Fernmeldegeheimnisses nicht informationspflichtig ist.[285] Eine weiterführende Legaldefinition des Begriffs der Verletzung ergibt sich aus § 3 Nr. 30a TKG. Diese knüpft an die Verletzung der Datensicherheit an.

Was eine Verletzung der Datensicherheit ist, erschließt sich aus dem Zusammenspiel mit den materiell-rechtlichen Sicherheitsanforderungen in § 109 TKG. Demnach beinhaltet sowohl die Nichterfüllung der Anforderungen in § 109 TKG (soweit diese kausal für Belastungen personenbezogener Daten geworden sind) als auch die Überwindung der technischen wie organisatorischen Schutzvorkehrungen durch Dritte eine Sicherheitsverletzung.[286] Typische Fälle wie Hackingangriffe oder ein Datenverlust lösen folglich die Meldepflicht aus.

Aus der Definition der Datenschutzverletzung in § 3 Nr. 30a TKG ergibt sich nicht, dass das Verständnis personenbezogener Daten auf Bestands- und Verkehrsdaten beschränkt ist. So kann der Begriff prinzipiell weit verstanden werden. Auch sonst ist eine nach dem Schweregrad der Verletzung bemessene Meldeschwelle oder die Begrenzung auf eine bestimmte Situation nicht vorgesehen. Auch vermeintlich geringfügige Datenschutzverletzungen mit weniger schweren Auswirkungen sind den Aufsichtsbehörden mitzuteilen. Dies ergibt sich auch unionsrechtlich aus Art. 2 Abs. 1 der Durchführungsverordnung der Kommission VO (EU) Nr. 611/2013.[287]

Der deutsche und unionsrechtliche Wortlaut der Meldepflicht gegenüber den Behörden („hat im Fall einer Verletzung“) im Vergleich mit demjenigen betreffend die Meldepflicht gegenüber den Betroffen („ist anzunehmen“) ergibt, dass die Sicherheitsverletzung positiv festgestellt sein muss. Allein der Verdacht oder die Annahme einer Beeinträchtigung verpflichten die Unternehmen noch nicht zur Meldung des Vorfalls. Art. 2 Abs. 2 UAbs. 3 VO (EU) Nr. 611/2013 lässt sich entnehmen, dass es dafür auf eine hinreichende Kenntnis insofern ankommt, als eine „sinnvolle“ Benachrichtigung vorgenommen werden kann. Es kommt also auf die Möglichkeit an, eine aussagekräftige Meldung abzugeben.

Eine Möglichkeit, die Meldepflicht durch vorher getroffene Sicherheitsmaßnahmen abzuwenden, besteht nicht. Für die Meldung an die Behörden gilt nicht

---

[285] *Graulich*, in: Arndt/Fetzer/Scherer/ders. (Hrsg.), TKG, 2. Aufl. 2015, § 109a Rn. 14.

[286] *Heun*, in: Auernhammer, 4. Aufl. 2014, TKG, Vor. zu § 88 Rn. 112; vgl. Erwägungsgrund 59 RL 2009/136/EG.

[287] Zur erheblichen Anzahl der Meldungen siehe BfDI, 24. Tätigkeitsbericht zum Datenschutz für die Jahre 2011 und 2012, BT-Drs. 17/13000, S. 58 f.

die Ausnahme, dass eine Meldung dann nicht erforderlich ist, wenn ein Sicherheitskonzept nachgewiesen wurde, gemäß dem die betroffenen personenbezogenen Daten durch technische Vorkehrungen wie als sicher anerkannte Verschlüsselungsverfahren gespeichert wurden. Der § 109a Abs. 1 S. 3 TKG bezieht sich nur auf die Benachrichtigung an die Betroffenen, sodass die zuständigen Behörden in jedem Falle zu unterrichten sind.

In zeitlicher Hinsicht erhalten die Behörden vergleichsweise zügig eine erste Meldung. Die Verpflichteten haben bei Vorliegen einer Datensicherheitsverletzung die Behörden unverzüglich (§ 121 BGB) zu benachrichtigen. Art. 2 Abs. 3 VO (EU) Nr. 611/2013 geht von einer ersten Meldung binnen 24 Stunden nach Feststellung der Verletzung aus. Aus der zulässigen Nachmeldung innerhalb von drei Tagen folgt, dass es in der Erstmeldung zuvorderst darauf ankommt, überhaupt entscheidungsrelevante Informationen mitzuteilen, ohne dass es auf deren Vollständigkeit ankommt.

bb) Inhalt der Meldung

Die bereits im Gesetzestext von Art. 4 Abs. 3 UAbs. 3 E-Privacy-RL sowie § 109a Abs. 2 S. 2 TKG angelegten Vorgaben zum Inhalt der Meldung entsprechen denen der DS-GVO.

Zur Sicherstellung einer unionsweit einheitlichen Anwendung der Meldepflicht werden nach Art. 4 Abs. 5 E-Privacy-RL die Umstände, die Form und das Verfahren durch von der Kommission zu erlassende Durchführungsmaßnahmen ergänzt. Vorbehaltlich dieser Maßnahmen kann die Bundesnetzagentur, nicht aber auch der Datenschutzbeauftragte Leitlinien erlassen.

Die nach Art. 2 Abs. 2 UAbs. 2 der Durchführungs-VO (EU) Nr. 611/2013 aufzuführenden Angaben gehen über die notwendigen Meldeinhalte der allgemeinen datenschutzrechtlichen Meldepflicht hinaus. Neben den allgemeinen Rahmendaten zum Vorfall entsprechend der Gliederung Risikobewertung, Faktenmitteilung Folgenanalyse sind „Art und Inhalt der betroffenen personenbezogenen Daten“ sowie „technische und organisatorische Maßnahmen, die der Betreiber in Bezug auf die betroffenen personenbezogenen Daten ergriffen hat“, anzugeben (Anhang I Nr. 6 und 7 VO (EU) Nr. 611/2013). *Prima facie* ergibt sich daraus das Erfordernis der Übermittlung einer Kopie der personenbezogenen Daten sowie die Darstellung der Maßnahmen zur Gewährleistung der Datensicherheit vor dem Vorfall.

Der Auslegung dahin, die Übermittlung der betroffenen Daten selbst sei erforderlich, steht entgegen, dass sie weder notwendig ist, um eine aufsichtsbehördliche Informationsbasis zu schaffen, noch um die Bedingungen des Vorfalls tiefergehend IT-forensisch zu analysieren.

Die Pflicht zur umfangreichen Mitteilung des Sicherheitsmanagements lässt sich nicht bereits mit dem Argument abtun, die Bundesnetzagentur kenne das bestehende Sicherheitskonzept der Diensteanbieter (§ 109 Abs. 4 TKG). Unionsrechtlich haben die Mitgliedstaaten lediglich sicherzustellen, dass die Behörden befugt sind, die Übermittlung zu verlangen (Art. 13b Abs. 2 a) RL 2002/21/EG in Verbindung mit Änderungs-RL 2009/140/EG). Außerdem dient der Nachweis geeigneter technischer Schutzmaßnahmen den Behörden der Prüfung, ob gemäß Art. 3 Abs. 3 UAbs. 3 E-Privacy-RL die Benachrichtigung der Betroffenen unterbleiben kann. Für das Unterbleiben der Betroffenenbenachrichtigung reicht im Übrigen nicht der formale Nachweis eines Sicherheitskonzepts. Es muss vielmehr geeignet sein, nachzuweisen, dass die Daten wirksam vor der Kenntnisnahme durch Dritte geschützt sind (Art. 4 Abs. 1 und 2 VO (EU) Nr. 611/2013). Dafür ist zu prüfen, ob die Daten auf sichere Weise kryptografisch verschlüsselt waren.

Daraus ergibt sich, dass die zuständige Behörde im Wege der Meldung erweiterte Rahmendaten erhält, die zusätzliche Schlüsse auf die Ursachen des Vorfalls zulassen können.

Im Übrigen haben die Diensteanbieter aber keine konkreten Angaben über etwaige Ergebnisse sicherheitstechnischer Analysen zu übermitteln. Spezifische technische Details, Ursachen sowie Abhilfen besonderer Sicherheitslücken sind auch nicht nach den Leitlinien, die die Bundesnetzagentur gemäß § 109a Abs. 5 TKG (Art. 4 Abs. 5 RL 2002/58/EG) vorgeben darf, zu melden.[288] Aus dem Selbstverständnis der Meldeadressaten ergibt sich insofern auch nur, dass die abgefragten Kategorien wie die Art der angegriffenen Daten, die Weise der Kenntnisnahme und des Schweregrades der Verletzung bei Häufung von Vorfällen oder anderen statistischen Signifikanzen eine Priorisierung und damit effizientere Aufsichtstätigkeit ergeben soll.[289]

Die Meldung wird technisch vollzogen, indem ein „Meldebogen" im editierbaren PDF-Format in elektronischer Form per E-Mail an die Bundesnetzagentur übermittelt wird.[290] Die Realisierung der Meldepflicht ist paradigmatisch für die Meldeprozesse im Bereich der Netz- und Informationssicherheit. Die melde-

---

[288] *Bundesnetzagentur*, Leitlinien zur Melde- und Benachrichtigungspflicht nach § 109a TKG, Stand 2014, S. 1 ff.; vgl. aber *Heun*, in: Auernhammer, 4. Aufl. 2014, TKG, § 109a Rn. 12: „Inhaltsvorgaben mit nicht unerheblicher Detailtiefe".

[289] BfDI, 24. Tätigkeitsbericht zum Datenschutz für die Jahre 2011 und 2012, BT-Drs. 17/13000, S. 59.

[290] Das Formular für Meldungen nach § 109a Abs. 1 S. 1 TKG ist abrufbar unter: http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/Datenschutz/Meldeformular.pdf?__blob=publicationFile&v=5.

relevanten Informationen müssen händisch eingeholt und auf den Meldebogen übertragen werden. Das Bestehen einer IT-gestützten Rahmenarchitektur für die automatisierte Übermittlung von Meldungen ist nicht ersichtlich. Daher können die Meldungen auch nicht in einem maschinenlesbaren Format erstellt und medienbruchfrei durchgeführt werden. Erforderlich ist je eine individuelle Interpretation der gemeldeten Daten.

Die Meldepflicht für Telekommunikationsdiensteanbieter bei Verletzung des Schutzes personenbezogener Daten ermöglicht im Vergleich zur allgemeinen datenschutzrechtlichen Meldepflicht einen erweiterten Einblick in die Datensicherheit des Anbieters. Jedoch zeigt sich an den gesetzgeberischen Vorgaben des Inhalts und der Durchführung der Meldung, dass die Meldung über ein In-Kenntnis-Setzen der Behörde nicht wesentlich hinausgeht. Für die Wissensproduktion sicherlich förderlich ist aber, dass die Bundesnetzagentur zusätzlich in den Meldeweg eingebunden ist. Durch die Parallelisierung kann es bei der Bundesnetzagentur zu Synergieeffekten kommen, da bei ihr auch die Meldungen bei sonstigen Sicherheitsverletzungen nach § 109 Abs. 5 TKG eingehen.

II. Befugnisse zur Generierung von Informationen

Über eine besondere Befugnis zur Einholung von Informationen verfügt hinsichtlich der Sicherheit von IT-Produkten und -Systemen das Bundesamt für Sicherheit in der Informationstechnik (1.). Die Bundesnetzagentur kann über eine allgemeine sicherheitsbezogene Befugnis Informationen einholen (2.). Über weitreichende Informationsbefugnisse verfügen die Nachrichtendienste (3.).

1. Untersuchung von IT-Produkten und -Systemen

a) Informationspflichten für Hersteller von Soft- und Hardware im öffentlichen Sicherheitsrecht

Für Sicherheitsmängel sind zu einem großen Teil die bei den Anbietern und Betreibern von Internetinfrastrukturen eingesetzte Soft- und Hardware oder eine Interaktion zwischen bestimmten Codes ursächlich. Angriffe über das Internet sind häufig deshalb erfolgreich, weil IT-Produkte Sicherheitslücken enthalten, die ausgenutzt werden können.

Die Verantwortlichkeit eines Herstellers endet grundsätzlich dort, wo ein Dritter vorsätzlich und rechtswidrig einen Schaden herbeiführt. Eine Verantwortlichkeit kann sich dennoch aus der vertraglichen Mängelhaftung oder der außervertraglichen Produkthaftung ergeben. Das zivilrechtliche Produkthaftungsrecht wird flankiert durch öffentlich-rechtliche Vorschriften zur Produktsicherheit. Das Produktsicherheitsgesetz (ProdSG) enthält informa-

tionsverwaltungsrechtliche Regelungen zur Informationsgenerierung der Marktüberwachungsbehörden.[291] Rechtliche Hebel zur Generierung von spezifisch IT-sicherheitsrelevanten Informationen von IT-Herstellern bestehen jedoch kaum. Zwar trifft den Hersteller im IT-Bereich auch die Pflicht zur besonders sorgfältigen Produktbeobachtung. Bei drohenden Gefahren für Leib und Leben kann sogar die Pflicht zur öffentlichen Warnung begründet sein.[292] Eine echte Pflicht zur Meldung detektierter IT-Schwachstellen besteht jedoch nicht.

Die Anwendbarkeit des ProdSG für Softwareprodukte ist ohnehin problematisch. Streitig ist insbesondere die Eigenschaft von Software als Produkt im Sinne des ProdSG. Während Hardware als verkörperter Gegenstand den Produktbegriff von § 2 Nr. 22 ProdSG erfüllt, ist dies bei Software weiterhin fraglich. Insofern kann zwischen sog. „embedded Software", d. h. solcher Software, die in ein Endprodukt integriert ist und Steuerungsfunktionen erfüllt, und solcher Software, die selbstständig zu nutzen ist, unterschieden werden.[293] Software erfüllt grundsätzlich nur in Form verkörperter Datenträger die Produkteigenschaft.[294] Außerdem bezweckt das ProdSG nur den Schutz vor Gefährdungen der Sicherheit und Gesundheit von Verwendern und Dritten. Aus Art. 2 lit. b Produktsicherheits-RL[295] und § 3 ProdSG geht hervor, dass die sicherheitstechnischen Anforderungen auf die Risiken für die körperliche Integrität der geschützten Personen zielen und nicht auf die hier relevante Sicherheit im Sinne der Schutzziele der Netz- und Informationssicherheit wie die Integrität und Vertraulichkeit informationstechnischer Systeme oder auf Risiken industrialisierter Persönlichkeitsverletzungen mit Bezug auf personenbezogene Daten.[296] Im Übrigen bestehen auch keine vertikalen Rechtsverordnungen im Sinne des § 8 Abs. 1 ProdSG, auf deren Grundlage weitere Rechtsgüter einbezogen werden könnten.[297]

Allgemeine, präventiv wirkende öffentlich-rechtliche Pflichten der IT-Hersteller, etwa zur ständigen Produktbeobachtung oder zur Bereitstellung von Informationen, sind darüber hinaus weder im BSIG, TMG noch im TKG vorgese-

---

[291] Siehe Abschnitt 7 des ProdSG für Informations- und Meldepflichten.

[292] *Spindler*, Produktverantwortung und Haftung im IT-Bereich, in: Kullmann/Pfister/Stöhr/ders. (Hrsg.), Produzentenhaftung, 07/16, (5).

[293] *Spindler*, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, 2007, S. 97; vgl. Deutscher Bundestag, Enquete-Kommission „Internet und digitale Gesellschaft", Neunter Zwischenbericht, BT-Drs. 17/12541, S. 71.

[294] *Klindt*/*Schucht*, in: Klindt (Hrsg.), ProdSG, 2. Aufl. 2015, § 2 Rn. 166; vgl. BT-Drs. 17/14031, S. 5.

[295] RL 2001/95/EG.

[296] *Schmidt-Kessel*, VuR 2015, 121 (121 f.); *Klindt*, in: ders. (Hrsg.), ProdSG, 2. Aufl. 2015, § 3 Rn. 8 f.

[297] *Rockstroh*/*Kunkel*, MMR 2017, 77 (82).

hen. Gleiches gilt für das den Gesetzen zugrundeliegende Unionsrecht. Mit dem durch das IT-Sicherheitsgesetz eingeführten § 8b Abs. 6 BSIG besteht lediglich eine Anordnungsbefugnis gegenüber Software-Herstellern. Diese können zur Mitwirkungen an der Beseitigung oder Vermeidung von Störungen verpflichtet werden.

b) Befugnis zur Untersuchung von IT-Sicherheitsprodukten

Bedeutung für die Generierung von Informationen von Soft- und Hardware hat die Befugnis zur Überprüfung der Sicherheit von IT-Produkten. Mit dem IT-Sicherheitsgesetz wurde mit § 7a BSIG eine Rechtsgrundlage geschaffen, die es dem BSI erlaubt, informationstechnische Produkte und Systeme darauf zu untersuchen, ob diese frei von Schwachstellen sind.

Der Begriff ist weit zu verstehen. Nach der Definition von IT-Sicherheitsprodukten in § 3 Abs. 1 Nr. 3 BSIG sind darunter informationstechnische Sicherheitsvorkehrungen, insbesondere informationstechnische Verfahren und Geräte, zu verstehen. Die Untersuchungsbefugnis ist zweckgebunden und bezieht sich auf die Erfüllung der in § 3 Abs. 1 S. 1 Nr. 1, 14 und 17 BSIG statuierten Aufgaben. Sie dient somit der Beratung und Warnung sowohl staatlicher Stellen als auch der Hersteller, Vertreiber und Anwender (Nr. 14). Die Verweisungskette führt in Nr. 17 zu dem eigenständigen Aufgabenkatalog in § 8b Abs. 2 BSIG, sodass zu den umfassenden Intelligence-Funktionen des BSIG als zentrale Stelle für die Informationssicherheit in kritischen Infrastrukturen auch die Untersuchungsbefugnis als Informationsbefugnis zu zählen ist.

Die Untersuchung von IT-Produkten, beispielsweise durch Reverse Engineering im Fall von Software, ist grundsätzlich mit rechtlichen Risiken behaftet. Eine solches Vorgehen kann „unbefugt" im Sinne von § 202a StGB oder §§ 17 ff. UWG sein und damit strafbares Ausspähen von Daten oder strafbaren Verrat von Betriebs- und Geschäftsgeheimnissen darstellen.

Untersuchungsgegenstände sind die auf dem Markt bereitgestellten oder dafür vorgesehenen informationstechnischen Produkte. Den Begriff „auf dem Markt bereitgestellter Produkte" bestimmt das Gesetz weiter nicht. Die Formulierung findet sich aber im ProdSG und ist dort in § 2 Nr. 4 definiert als jede entgeltliche oder unentgeltliche Abgabe eines Produkts zum Vertrieb, Verbrauch oder zur Verwendung. Die Formulierung „zur Bereitstellung auf dem Markt vorgesehen" im BSIG macht darüber hinaus deutlich, dass die Befugnis auch Hard- und Software umfasst, die zwar vom Hersteller bereits angekündigt wurden, aber noch nicht allgemein auf dem Markt verfügbar sind.

An einen näher spezifizierten Anlass ist die Ausübung des Untersuchungsrechts nicht gebunden. Über die Untersuchung muss der Hersteller nicht infor-

miert werden und im Zweifel kann sie auch gegen den Willen des Herstellers erfolgen.[298] Weitergehende Untersuchungsrechte bei Herstellern, Anbietern und sonstigen Einrichtungen werden durch die Befugnis nicht begründet.[299] Für die eigentliche Untersuchung kann sich das BSI Dritter bedienen, d. h. ein Test kann auch durch akkreditierte Institutionen vorgenommen werden.

Durch § 7a BSIG kommt dem BSI eine Marktbeobachtungsfunktion zu. Diese ist zwar durch die Begrenzung auf bestimmte Aufgaben nicht umfassend. Im Ergebnis kommt die durch § 7a BSIG entstehende Prüfkompetenz durchaus im Ansatz einem „Sicherheits-TÜV" gleich.[300]

Die praktische Reichweite der Befugnis darf allerdings nicht überschätzt werden. Die Untersuchung eines einzelnen Programms oder Hardwareprodukts kann aufgrund der Komplexität der Produkte so viele Ressourcen binden (wenn sich das BSI Dritter bedienen würde, wären dies insbesondere finanzielle Ressourcen), dass nur in Einzelfällen eine punktuelle Prüfung durchführbar sein dürfte. Eine weitreichendere Erkenntnisgewinnung wäre eher mit einer Auskunftsbefugnis zu erreichen, die Hersteller verpflichtet, ihnen bekannte Schwachstellen der NIS-Behörde unabhängig von einem Sicherheitsvorfall offenzulegen. Eine solche Auskunftsbefugnis ergibt sich aus § 7a BSIG aber nicht.

Bedeutung für die Sicherheitsgewährleistung hat die Norm nicht nur, weil sie Rechtssicherheit für die Untersuchung von IT-Produkten schafft, sondern darüber hinaus, weil sie die Weitergabe und Veröffentlichung der gewonnenen Erkenntnisse erlaubt.[301]

2. Informationsbefugnisse im sicherheitsbezogenen Telekommunikationsrecht

Bereits bei der Untersuchung der Meldepflichten wurde die Bedeutung des Telekommunikationsrechts für das sicherheitsbezogene Informationsverwaltungsrecht deutlich. Neben Informationsbeibringungspflichten stellt das TKG Informationsbefugnisse bereit, die für den Bereich der nichtökonomischen Regulierung von Bedeutung sind. Zu unterscheiden ist die spezielle Informationsbefugnis des § 115 TKG (a) von den allgemeinen Informationsbefugnissen des § 127 (b).

a) Sicherheitsbezogene Informationsbefugnis

Eine spezielle Informationsbefugnis im Bereich der nichtökonomischen Regulierung ergibt sich aus § 115 Abs. 1 S. 2 TKG. Die Norm ist systematisch an das

[298] *Hornung*, NJW 2015, 3334 (3339).
[299] BT-Drs. 18/4096, S. 41.
[300] Vgl. *Roos*, MMR 2014, 723 (728).
[301] Siehe § 5 B. I. 3.

Ende von Teil 7 des TKG gestellt und gehört somit zu den unmittelbar auf die Öffentliche Sicherheit beziehenden Vorschriften, §§ 88 bis 115 TKG (aa). Die Reichweite der Informationsbefugnis richtet sich vor allem danach, wie das Tatbestandsmerkmal der Erforderlichkeit zu verstehen ist (bb).

aa) Sicherstellung materiell-rechtlicher Sicherheitspflichten

Die Bundesnetzagentur kann gemäß § 115 Abs. 1 S. 1 TKG Anordnungen und andere Maßnahmen treffen, um die Einhaltung der Vorschriften des Teils 7 und der aufgrund dieses Teils ergangenen Rechtsverordnungen sowie der jeweils anzuwendenden Technischen Richtlinien sicherzustellen. Durch § 115 Abs. 1 S. 1 TKG erhält die Bundesnetzagentur eine Generalermächtigung zur Durchsetzung der materiell-rechtlichen Sicherheitspflichten und der aufgrund dieses Teils ergangenen Rechtsverordnungen und der jeweils anzuwendenden technischen Richtlinien.[302]

Nach § 115 Abs. 1 S. 2 TKG müssen die Verpflichteten der Bundesnetzagentur auf Anforderung die hierzu erforderlichen Auskünfte erteilen.[303] § 115 Abs. 1 S. 2 TKG erfüllt die Anforderung von Art. 13b lit. a) RL 2009/140/EG, der das Bereitstellen der erforderlichen Informationen durch die Unternehmen zur Beurteilung der Sicherheit und Integrität der Dienste und Netze vorsieht.

Die Formulierung „hierzu" stellt klar, dass sich die Auskünfte auf die Einhaltung der Vorschriften des Teils 7 beziehen und insoweit auch beschränken. Aus den in Satz 2 „Verpflichteten" ergibt sich auch der Adressat der Pflichten aus § 115 Abs. 1 TKG. Der verpflichtete Personenkreis hängt von der jeweiligen Bestimmung ab, deren Einhaltung kontrolliert oder sichergestellt werden soll. Für die sicherheitsbezogenen Pflichten sind dies primär die Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste.

Das Verhältnis der Generalermächtigung nach Satz 1 und der Auskunftspflicht nach Satz 2 ist nicht ohne Weiteres erkennbar. § 115 Abs. 1 S. 2 TKG könnte eine selbstständige Eingriffsgrundlage darstellen, die zum Erlass von Verwaltungsakten befugt.[304] Eine Auskunftspflicht könnte nach dieser Auffassung isoliert bestehen. In Betracht kommt auch, dass sich die Vorschrift akzessorisch zur generalklauselartigen Anordnungsbefugnis in Satz 1 verhält. Bei

---

[302] *Graulich*, in: Arndt/Fetzer/Scherer/ders. (Hrsg.), TKG, 2. Aufl. 2015, § 115 Rn. 2.

[303] Vgl. *Gusy*, Ziele, Aufträge und Maßstäbe der Sicherheitsgewährleistung, in: ders./Kugelmann/Würtenberger, Rechtshandbuch Zivile Sicherheit, 2017, S. 55 (75), der der Norm, ohne weiter auf sie einzugehen, Potential für „neue Fragen, aber möglicherweise auch für neue Antworten" zuschreibt.

[304] *Klesczewski*, in: Säcker (Hrsg.), TKG, 3. Aufl. 2013, § 115 Rn. 4, 9.

letzterer Auffassung wäre ein Auskunftsverlangen eine behördliche Verfahrenshandlung, die im Sinne von § 4a VwGO nur gemeinsam mit einer Anordnung nach § 115 Abs. 1 S. 1 TKG, die als „Sachentscheidung" anzusehen wäre, angegriffen werden könnte.[305] Die Auskunftspflicht kann zudem als eine über § 26 Abs. 2 VwVfG hinausgehende Mitwirkungspflicht im Sinne von § 26 Abs. 2 S. 3 VwVfG verstanden werden, die die Verpflichteten deshalb zu einer besonderen Mitwirkung verpflichtet, weil sie weitgehend die Informationsherrschaft über betriebsinterne Vorgänge haben.[306]

Der Befugnischarakter der Norm ist jedenfalls ausgehend vom Wortlaut („muss", „auf Anforderung") nicht ausgeschlossen. Die systematische Stellung der Auskunftspflicht in Satz 2 nach der Anordnungsbefugnis in Satz 1 legt nahe, dass die Auskunftserteilung an ein bestimmtes Informationsbedürfnis anknüpft. Das Auskunftsverlangen ist an die Überprüfung im Rahmen der Befolgungskontrolle gekoppelt. Die für die Wahrnehmung dieser Aufsichtsfunktion erforderlichen Informationen können den Anordnungen und Maßnahmen nach Satz 1 vorgeschaltet sein, da sie sich grundsätzlich auf eine Informationsbasis stützen müssen. Erst die behördliche Informationskompetenz begründet eine Interventionskompetenz. Insoweit ist die Informationserhebung von den Maßnahmen, mit denen die etwaige festgestellte Nichteinhaltung korrigiert wird, zu unterscheiden.[307] Demnach steht § 115 Abs. 1 S. 2 TKG zur Generalermächtigung nicht im Verhältnis der Akzessorietät, sondern der Komplementarität.[308] Eine Bindung besteht durch den Zweck des Auskunftsverlangens, das unmittelbar an die Sicherstellung der Einhaltung der Vorschriften des Teils 7 anknüpft. In diesem Sinne kann § 115 Abs. 1 S. 2 TKG als eine auf die Anordnungskompetenz zugeschnittene spezielle Eingriffsbefugnis verstanden werden.[309]

Aus einer so verstandenen Eingriffsbefugnis folgt, dass die Verpflichteten der Bundesnetzagentur Auskunft über Voraussetzungen erteilen müssen, welche die Behörde für die Prüfung des Verwaltungsaktes in Form einer Anordnung oder Maßnahme nach § 115 Abs. 1 S. 1 TKG benötigt. Die generierten Informationen müssen die Behörde in die Lage versetzen, zu entscheiden, ob

---

[305] *Graulich*, in: Arndt/Fetzer/Scherer/ders. (Hrsg.), TKG, 2. Aufl. 2015, § 115 Rn. 8.

[306] Zur entsprechenden Vorgängernorm *Trute*, in: ders./Spoerr/Bosch, TKG, 2001, § 91 Rn. 5.; vgl. *Stohrer*, Informationspflichten Privater gegenüber dem Staat in Zeiten von Privatisierung, Liberalisierung und Deregulierung, 2007, S. 206.

[307] *Berliner*, Informationsbefugnisse der Bundesnetzagentur im Telekommunikationsrecht, 2012, S. 41.

[308] *Graulich*, in: Arndt/Fetzer/Scherer/ders. (Hrsg.), TKG, 2. Aufl. 2015, § 115 Rn. 9.

[309] *Berliner*, Informationsbefugnisse der Bundesnetzagentur im Telekommunikationsrecht, 2012, S. 41.

und ggf. welche Anordnungen oder weitere Aufsichts- und Kontrollmaßnahmen getroffen werden müssen.

Sprachlich bezieht sich eine Auskunft auf die Erteilung sachlich begrenzter Informationen.

Die Behörde ist im Rahmen einer Auskunftsbefugnis daher grundsätzlich nicht berechtigt, zur Erleichterung ihrer Aufgabenwahrnehmung subjektive Einschätzungen und Beurteilungen einzufordern.[310] Noch auf das Auskunftsrechtdürfte sich die Vorlage eines Umsetzungskonzepts zur Einhaltung sicherheitsrechtlicher Pflichten stützen.[311] Im Umkehrschluss aus § 127 Abs. 2 S. 1 Nr. 2 und Abs. 4 TKG kann jedoch nicht die eingriffsintensivere Übersendung oder Aushändigung von Unterlagen unter Aufgabe des Gewahrsams verlangt werden.[312]

Die Verpflichteten müssen die Auskünfte „auf Anforderung" erteilen. Anders als bei selbstständigen Informationsbeibringungspflichten sind die Informationen nicht aufgrund bestimmter Ereignisse oder aus Eigeninitiative zu übermitteln.[313]

bb) Kriterium der Erforderlichkeit aus der Wissensperspektive

Die NIS-Behörden haben grundsätzlich einen kontinuierlichen Bedarf an aktuellen Informationen. Aus eben diesem Grund gehört es gemäß § 8b Abs. 2 Nr. 3 BSIG zu den Aufgaben des BSI, „das Lagebild bezüglich der Sicherheit in der Informationstechnik […] kontinuierlich zu aktualisieren". Soweit Telekommunikationsinfrastrukturen kritische Infrastrukturen sind (vgl. § 8c BSIG), besteht

---

[310] *Berliner*, Informationsbefugnisse der Bundesnetzagentur im Telekommunikationsrecht, 2012, S. 50.

[311] OVG Münster, MMR 2010, 134 (134 f.). Die Bundesnetzagentur durfte das Konzept zur Umsetzung der Verpflichtungen zur Vorratsdatenspeicherung aus § 113a TKG auf Grundlage von § 115 Abs. 1 S. 1 TKG, auch wenn sie die Rechtsgrundlage in dem Bescheid selbst nicht nannte, als Begleitmaßnahme zur Aufforderung, die technischen Voraussetzungen zur Einhaltung der Verpflichtungen zu schaffen, stützen.

[312] Im Übrigen legt diese Restriktion die Abgrenzung zu § 127 TKG nahe. Die Betretungsbefugnis nach § 115 Abs. 1 S. 3 TKG reicht weniger weit als das in § 127 Abs. 2 S. 1 Nr. 2 TKG. Während § 127 TKG auch die Einsicht und Prüfung der Unterlagen erlaubt, ist in § 115 TKG lediglich das Betreten und Besichtigen der Geschäfts- und Betriebsräume erlaubt. Siehe *Eckhardt*, in: Geppert/Schütz (Hrsg.), BeckTKG, 4. Aufl. 2013, § 115 Rn. 5; *Klesczewski*, in: Säcker (Hrsg.), TKG, 3. Aufl. 2013, § 115 Rn. 9, 15. *Heun*, in: Auernhammer, BDSG, TKG, § 115, Rn. 6 und 8 weist darauf hin, dass die Vorlage von Unterlagen und nähere Einblicke in die Funktionsweise von Telekommunikationsanlagen und IT-Systemen ggf. verbunden mit der Auskunftsverpflichtung sowie den Rechten aus § 109 Abs. 4 TKG zur Vorlage eines Sicherheitskonzepts in entsprechendem Umfang abgedeckt sein können. Dagegen aber *Mozek*, in: Säcker (Hrsg.), TKG, 3. Aufl. 2013, § 115 Rn. 7.

[313] Vgl. *Jarass*, in: ders. (Hrsg.), BImSchG, § 52 Rn. 36.

bei der Bundesnetzagentur in tatsächlicher Hinsicht ein gleichgelagerter Informationsbedarf. In rechtlicher Hinsicht ist der telekommunikationsrechtliche Gewährleistungsauftrag aus § 1 TKG nicht auf konkrete Gefahrensituationen begrenzt. Die Bundesnetzagentur ist nicht nur permanent auf Entscheidungswissen angewiesen, sondern muss auch ausreichend mit Informationen versorgt sein, um ihre Rückfallposition in der Gewährleistungsverantwortung für die Bereitstellung der Telekommunikationsdiente wahrnehmen zu können.[314] Eine kontinuierliche und umfassende Information mag ein Stück weit der Gefahr einer Informationssteuerung der Regulatoren durch die Regulierten vorbeugen, die bei Bestehen einer Asymmetrie in der Informationslage zwischen Privaten und Regulierungsverwaltung entstehen kann. Die Bundesnetzagentur ist in ihrer originären Funktion für die Sicherheit der Telekommunikationsinfrastrukturen und in ihrer Funktion in der Weitergabe von Informationen an das BSI daher im Grundsatz nicht weniger auf einen kontinuierlichen Informationsfluss im Vorfeld spezifischer Ereignisse auf Informationen angewiesen als das BSI.

Angesichts der strukturellen Offenheit der Regulierungsaufgaben, zu denen nach § 2 Abs. 2 Nr. 9 TKG die Interessen der öffentlichen Sicherheit gehören, und der dadurch bedingten Vermehrung der Informationsbedürfnisse, stellt sich die Frage, wie das Gesetz einer „Entgrenzung des behördlichen Informationsgebarens“ entgegenwirkt.[315]

Der Wortlaut von § 115 Abs. 1 S. 2 TKG weist auf eine Begrenzung der behördlichen Informationserhebung hin. Informationen dürfen nur abgefragt werden, soweit sie für die Anordnungen oder sonstigen Maßnahmen „erforderlich“ sind.

Allerdings ist damit noch nicht gesagt, welcher Maßstab an die Erforderlichkeit der Auskünfte zu legen ist.[316]

Mit Blick auf § 127 TKG, der informationellen Generalbefugnis für Auskunftsverlangen, die sich auf den gesamten Zuständigkeitsbereich der Bundesnetzagentur erstreckt und nach der die Betreiber „Auskünfte zu erteilen [haben], die für den Vollzug dieses Gesetzes erforderlich sind“, wird zum Teil das Merkmal der Erforderlichkeit sehr weit ausgelegt. Zum einen seien die kartell-

---

[314] Vgl. *Eifert*, Regulierungsstrategien, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. I, 2006, § 19 Rn. 151; vgl. zu den unzureichenden Formen der Informationsbeschaffung im TKG *Röhl*, Der rechtliche Kontext der Wissenserzeugung, DV, Beiheft 9, Wissen – Zur kognitiven Dimension des Rechts, 2010, S. 65 (83); vgl. aber *Ruffert*, in: Säcker (Hrsg.), TKG, 3. Aufl. 2013, § 127 Rn. 8.

[315] Kritisch *Gärditz*, Regulierungsrechtliche Auskunftsanordnung als Instrument der Wissensgenerierung, DVBl. 2009, 69 (71).

[316] Vgl. *Eifert*, Die gerichtliche Kontrolle der Entscheidungen der Bundesnetzagentur, ZHR 174 (2010), 449 (472); *Holznagel/Schulz*, MMR, 2002, 364 (366).

rechtlichen Eingriffsvoraussetzungen, wie sie sich aus der parallelen Auskunftsbefugnis im GWB ergäben, nicht unbesehen zu übertragen.[317] Zum anderen erfordere die spezifische regulierungsverwaltungsrechtliche Notwendigkeit der Wissensgenerierung eine kontinuierliche Informationserhebung, die über die Informationserhebung zur Ausübung der ordnungsrechtlichen Aufsichtstätigkeit, und damit über die Kontrolle rechtskonformen Verhaltens, hinausgeht.[318]

Fraglich ist, ob sich diese weite Auslegung auf § 115 Abs. 1 S. 2 TKG übertragen lässt.

Ebenso wie § 115 Abs. 1 S. 2 TKG handelt es sich bei § 127 Abs. 1 TKG um eine Rechtsgrundlage für Auskunftsanordnungen als Instrument der Informationsgenerierung. Die Vorgängernorm von § 127 TKG, § 72 TKG-1996, wurde dem wettbewerbsrechtlichen § 59 GWB nachgebildet.[319] Die Erforderlichkeit des Auskunftsverlangens dient dort dazu, die Wettbewerbsbehörde in ihrer Sachverhaltsermittlung auf spezifisches Missbrauchsverhalten von Unternehmen zu begrenzen. Das Auskunftsverlangen knüpft an das konkrete kartellrechtswidrige Verhalten von Wettbewerbsunternehmen im Einzelfall an.[320] Die Aufklärung eines Sachverhalts ist auf Grundlage eines schlüssigen Ermittlungskonzepts zu betreiben.[321] Von einer allgemeinen und anlasslosen Informationsbefugnis ist im Kartellrecht abgesehen worden, weil die unspezifische und abstrakte Gefahr wettbewerbswidrigen Unternehmensverhaltens eine solche nicht zu rechtfertigen vermag.[322] Für eine Tätigkeit der Behörde müssen verifizierbare Anhaltspunkte für einen Verstoß vorliegen, die einen gewissen Anfangsverdacht begründen, um anlass- und einzelfallbezogene Maßnahmen im Regelungsbereich treffen zu können.[323]

Die im Rahmen von § 59 GWB entwickelten Kriterien lassen sich grundsätzlich auf die Auslegung der telekommunikationsrechtlichen Auskunftsanordnungen übertragen. Allerdings kann sich aus der funktionellen Abgrenzung des

---

[317] *Berliner*, Informationsbefugnisse der Bundesnetzagentur im Telekommunikationsrecht, 2012, S. 227 ff.

[318] *Berliner*, Informationsbefugnisse der Bundesnetzagentur im Telekommunikationsrecht, 2012, S. 230 ff.

[319] *Holznagel*, Die Erhebung von Marktdaten im Wege des Auskunftsersuchens nach dem TKG, 2001, S. 45 ff.

[320] *zur Nieden*, in: Jaeger/Kokott/Pohlmann/Schroeder, Frankfurter Kommentar zum Kartellrecht, 87. Lieferung 2016, GWB, § 59, Rn. 16.

[321] Vgl. OLG Düsseldorf, BeckRS 2011, 17498 (Rn. 14); *Barth*, in: Münchener Kommentar, KartellR, 2. Aufl. 2015, GWB, § 59 Rn. 6 ff.

[322] *Böse*, Wirtschaftsaufsicht und Strafverfolgung, 2005, S. 219.

[323] KG, WuW/E OLG 2517 (2518); OVG Münster, DVBl. 2008, 460 (461); *zur Nieden*, in: Jaeger/Kokott/Pohlmann/Schroeder, Frankfurter Kommentar zum Kartellrecht, 87. Lieferung 2016, GWB, § 59, Rn. 14.

Regulierungsrechts zum Kartellrechts insbesondere vor dem Hintergrund des Wissensbedarfs der Bundesnetzagentur ein abweichendes Verständnis der Auskunftsbefugnis ergeben.[324] Ein struktureller Unterschied kann darin gesehen werden, dass die Wettbewerbsaufsicht prinzipiell negatorisch-defensiv ausgerichtet ist, da sie an ein konkretes wettbewerbswidriges Verhalten individueller Wettbewerbsunternehmen anknüpft, wohingegen zu den Aufgaben der Regulierung gezählt werden kann, gestaltende Entscheidungen zur Erreichung sektorspezifischer Regulierungsziele zu treffen.[325] Anders als das wettbewerbsbezogene Gefahrenabwehrrecht sei das telekommunikationsrechtliche Regulierungsrecht auch eine „Marktverhaltens- und Marktstrukturregulierung, also eine steuernde interventionistische Einflussnahme auf privatwirtschaftliche Tätigkeit zur Verfolgung und Sicherstellung von Gemeinwohlbelangen".[326] Die Marktregulierung gehe in weiten Teilen von einem Konzept aktiver Marktbegleitung und „nicht nur punktueller Marktinterventionen" aus und sei durch die Merkmale pro-aktives Vorgehen, finale Steuerung bzw. weitreichende Normierungsaufgaben, Multipolarität des Interessenfeldes und Zeitabhängigkeit gekennzeichnet.[327] Regulierungsentscheidungen seien insoweit besonders mit den Bedingungen von Variation, Komplexität und Ungewissheit konfrontiert.[328] Dies spricht dafür, die Dogmatik der Sachverhaltsermittlung im Kartellrecht nicht gänzlich auf das Regulierungsrecht zu übertragen und daher funktionell abzugrenzen.[329]

Allerdings ist zweifelhaft, ob die Aufwertung der Wissensgenerierung im Regulierungsrecht und damit im Rahmen der Auskunftsbefugnis in § 127 TKG auch innerhalb des TKG und somit auch im Rahmen von § 115 Abs. 1 S. 2 TKG vorgenommen werden kann.

---

[324] Allgemein *Sennekamp*, Der Diskurs um die Abgrenzung von Kartell- und Regulierungsrecht, 2016.

[325] *Ladeur*, Innovation und Telekommunikation durch Regulierung, in: Hoffmann-Riem (Hrsg.), Innovation und Telekommunikation, 2000, S. 57 (66 ff.); *Gärditz*, DVBl. 2009, 69 (72).

[326] *Berliner*, Informationsbefugnisse der Bundesnetzagentur im Telekommunikationsrecht, 2012, S. 188.

[327] *Eifert*, Die gerichtliche Kontrolle der Entscheidungen der Bundesnetzagentur, ZHR 174 (2010), 449 (463); BVerwG, NVwZ 2008, 1359 (1360); zum verwandten Topos und der Frage nach der Behandlung von Beurteilungsspielräumen aus der Wissensperspektive *Schulz*, Beurteilungsspielräume als Wissensproblem, Rewi 2012, 330 (338).

[328] Vgl. *Trute*, Regulierung – am Beispiel des Telekommunikationsrechts, in: FS Brohm, Der Wandel des Staates von den Herausforderungen der Gegenwart, 2002, S. 169 (176 f.); *Ladeur*, Innovation und Telekommunikation durch Regulierung, in: Hoffmann-Riem (Hrsg.), Innovation und Telekommunikation, 2000, S. 58 f., 62 f.

[329] *Gärditz*, DVBl. 2009, 69 (72).

Zwar ist auch der Gegenstandsbereich der Gewährleistung der Netz- und Informationssicherheit von einer hohen dynamischen Komplexität geprägt, die prinzipiell eine adäquate Produktion des administrativen Entscheidungswissens erfordert. Dennoch ist der Teil 7 des TKG, anders als der Bereich der Marktregulierung, nicht durch Befugnisse zur *Ex-ante*-Regulierung gekennzeichnet, denen ein prognostischer Charakter zugeschrieben werden kann. Anders als etwa in der Zugangs- und Entgeltregulierung, in der Regulierungsverfügungen Ausdruck einer gesetzlich ausgeformten Gestaltungsfreiheit sind, die sich auf die Verwirklichung des gesetzlichen Regulierungsauftrags und die prospektive Bewältigung der damit zusammenhängenden Probleme erstreckt,[330] findet sich in den die Netz- und Informationssicherheit betreffenden Vorschriften § 109 und § 109a TKG kein Anknüpfungspunkt für die Annahme eines gestalterischen Auftrags der Bundesnetzagentur zur Sicherheitsgewährleistung. Die Bundesnetzagentur „überprüft" (§ 109 Abs. 4 S. 7 TKG), ihr sind Beeinträchtigungen „mitzuteilen" (§ 109 Abs. 5 S. 1, vgl. § 109a Abs. 1 S. 1 TKG), sie kann einen detaillierten Bericht „verlangen" (§ 109 Abs. 5, vgl. § 109a Abs. 1 S. 4 TKG), sie „leitet weiter" (§ 109 Abs. 5 S. 5 TKG), sie kann „unterrichten" oder „auffordern" (§ 109 Abs. 5 S. 6 und 7 TKG), sie „legt vor" (§ 109 Abs. 5 S. 9 TKG) oder sie kann „anordnen" (§ 109 Abs. 7 S. 1 TKG). Soweit die Sicherheit am Stand der Technik zu messen ist (§ 109 Abs. 1 S. 2 TKG) hat die Bundesnetzagentur auf die Ausfüllung dieses Maßstabs keinen bestimmenden Einfluss. Proaktiv geht die Bundesnetzagentur im Einvernehmen mit dem BSI bei der Erstellung des Sicherheitskatalogs vor (§ 109 Abs. 6 S. 1 TKG). Allerdings ist dies keine Regelung, auf die ein dazu in Relation stehendes Auskunftsverlangen auf Grundlage von § 115 Abs. 1 S. 2 TKG gerichtet sein kann, da sich § 115 Abs. 1 S. 1 TKG auf die „Einhaltung der Vorschriften" bezieht und nicht etwa auf die Vorbereitung der der Bundesnetzagentur obliegenden Aufgaben.

Die genannten Rechtsfolgen weisen auch keine finalen Steuerungskomponenten aus. Über das allgemeine Regulierungsziel der Wahrung der Interessen der öffentlichen Sicherheit in § 2 Abs. 2 Nr. 9 TKG hinaus besteht keine Programmierung zur Verwirklichung näher spezifizierter Zielbestimmungen (vgl. dagegen § 21 Abs. 1 S. 2 oder § 27 Abs. 2 S. 2 TKG).

Auch wenn die Bundesnetzagentur in sicherheitsbezogenen Entscheidungen immer auch die Interessen der Nutzer zu berücksichtigen hat, ergibt sich dadurch in dem Sinne keine komplexe Entscheidungssituation, weil die Rechtsfolgen wenig generalisiert gefasst sind. Eine näher spezifizierte Pflicht zur regelmäßigen Beobachtung zur Revision einmal getroffener Entscheidungen besteht ebenfalls nicht. Gemäß § 109 Abs. 4 S. 6 TKG überprüft die Bundesnetzagentur zwar re-

[330] Mit Bezug auf § 9 Abs. 2 und 13 Abs. 1 und 3 TKG BVerwG, NVwZ 2008, 575 (577).

gelmäßig die Umsetzung des Sicherheitskonzepts. Ein besonderer fortlaufender Informationsbedarf über das Erforderliche hinaus ergibt sich daraus nicht.

Als weiterer begrenzender Punkt für die Interpretation der Erforderlichkeit ist heranzuziehen, dass § 115 Abs. 1 S. 1 TKG bezweckt, die Einhaltung der Vorschriften „sicherzustellen". Dem Wortlaut nach ist der mittelbare Zweck des Auskunftsverlangen in § 115 Abs. 1 S. 2 TKG enger gefasst als nach § 127 Abs. 1 S. 1 TKG, wo es dem „Vollzug dieses Gesetzes" dient. Der Vollzug geht weiter und knüpft an die Erfüllung der der Bundesnetzagentur übertragenen Aufgaben an.[331] Die Befugnis zum Sicherstellen knüpft gedanklich an einen Verstoß gegen eine Vorschrift an.[332] Die Auskünfte beziehen sich dann auf die einzelfallbezogene Überprüfung im Rahmen einer Befolgungskontrolle, sodass ein allgemeiner, „permanenter Informationsfluss", etwa über IT-Sicherheitsvorfälle, auf Grundlage von § 115 Abs. 1 S. 2 nicht institutionalisiert werden kann.[333] Die Informationsbefugnis stellt durch die Voraussetzung, die Einhaltung sicherzustellen, gerade keine „Dachkompetenz" dar, die zur generellen Überwachung von Telekommunikationsunternehmen ermächtigt. Es muss der Bundesnetzagentur um Kontrolle und Durchsetzung gehen.[334]

Nach alldem ist das Merkmal der Erforderlichkeit im Sinne des Charakters von § 115 TKG als Überwachsnorm auszulegen. Dogmatisch ist das Merkmal der Erforderlichkeit nur eine Voraussetzung der Prüfung der Verhältnismäßigkeit. Gleichwohl setzt es voraus, dass das Auskunftsverlangen geeignet ist.[335] Unzulässig ist jedenfalls eine Datenabfrage, wenn bereits aus *Ex-ante*-Sicht feststeht, dass Daten unter keinem Gesichtspunkt für den zugrundeliegenden Zweck Bedeutung haben können.[336] Bedeutung hat eine Information, wenn sie zur Beantwortung bestimmter, sachlich eingrenzbarer Fragen im Zusammenhang mit der Einhaltungsüberwachung dienen kann.

Im Ergebnis kann die Informationsbefugnis aus § 115 Abs. 1 S. 2 TKG als Instrument verstanden werden, das dazu dient, ein umfassendes Basiswissen für eine behördliche Überwachungspraxis zu generieren. Einen Beitrag in der Sicherheitsgewährleistung unterhalb der Gefahrenschwelle leistet die Überwa-

---

[331] *Meyer-Sebastian*, in: Geppert/Schütz (Hrsg.), BeckTKG, 4. Aufl. 2013, § 127, Rn. 11.

[332] Vgl. *Graulich*, in: Arndt/Fetzer/Scherer/ders. (Hrsg.), TKG, 2. Aufl. 2015, § 115, Rn. 4.

[333] So im Ergebnis, allerdings ohne nähere Begründung, *Sonntag*, IT-Sicherheit kritischer Infrastrukturen, 2002, S. 189.

[334] OVG Münster, MMR 2015, 209 (209).

[335] Vgl. mit Bezug zum kartellrechtlichen Auskunftsverlangen KG, WuW/E OLG 3721 (3722).

[336] BGHZ 172, 368 (382).

chungstätigkeit reflexartig zudem durch die durch mögliche Anordnungs- und Auskunftsverlangen stimulierte Compliance mit den Sicherheitspflichten.[337]

b) Informationelle Generalbefugnis

Da sich § 127 TKG auf das ganze Gesetz einschließlich des sicherheitsbezogenen Teils 7 des TKG, für den mit § 115 TKG die soeben behandelte spezielle Informationsbefugnis besteht, bezieht, ist klärungsbedürftig, ob der Generalbefugnis darüber hinaus Bedeutung für die sicherheitsverwaltungsrechtliche Informationsgenerierung zukommt.

Zunächst weist § 127 TKG Elemente ökonomischer Regulierung auf. Der in § 127 Abs. 1 S. 2 Nr. 1 bis 7 TKG aufgelistete Katalog an Regelbeispielen und die in Abs. 2 aufgezählten Gegenstände von Auskunfts- und Einsichtsbefugnissen beziehen sich auf wirtschaftliche und marktspezifische Informationen. Bei Hinzuziehung des zugrundeliegenden Unionsrechts erscheint § 127 Abs. 1 TKG dagegen als zweckneutrale Informationsbefugnis. In Art. 11 Abs. 1 UAbs. 1 RL 2002/20/EG heißt es zwar, dass die Behörde „nur" die Informationen für die in dem Artikel nachfolgend aufgeführten Zwecke verlangen darf. Diese weisen keinen Bezug zu sicherheitsrechtlichen Regelungen auf. Der begrenzende Wortlaut deutet auf einen abschließenden Charakter der Regelung hin. Die Regelung steht allerdings „unbeschadet anderer nationaler Berichts- und Informationspflichten". Da sich aus der Richtlinienüberarbeitung in den sicherheitsrechtlichen Artikeln 13a und 13b RL 2009/140/EG keine weiterführenden Aussagen ergeben, ist kein durchgreifender Einwand dagegen ersichtlich, die Generalklausel nicht als nationale Informationspflicht anzusehen, die nur in tatbestandlichen Konstellationen greift, die sich in der herkömmlichen Wirtschaftsaufsicht, in regulierungsverwaltungsrechtlichen Aufgabenstellungen und der bloßen Rechtsaufsicht erschöpfen. Die Informationsbefugnis zur Abdeckung des sicherheitsverwaltungsrechtlichen Informationsbedarfs heranzuziehen, ist jedenfalls nicht von vorneherein ausgeschlossen.

Wird zur Bestimmung der Reichweite der Informationsbefugnis das allgemeine Regulierungsziel der Wahrung der Interessen der öffentlichen Sicherheit in § 2 Abs. 2 Nr. 9 TKG herangezogen, zeichnet sich durchaus eine akzessorische Bedeutung der Vorschrift zur Gewinnung von sicherheitsrelevanten Informationen ab. Gegen eine Akzessorietät der Generalbefugnis spricht aber, dass die formulierten Regulierungsziele von vorneherein zu abstrakt sind, als dass sie eine hinreichend bestimmte und verhältnismäßige Grundlage für Informationseingriffe zur Verfügung stellen könnten. Zur Rechtfertigung von Grund-

[337] *Berliner*, Informationsbefugnisse der Bundesnetzagentur im Telekommunikationsrecht, 2012, S. 49.

rechtseingriffen kann das bloße Hinzuziehen einer Zieldefinition nicht genügen.[338] Andererseits darf der Gesetzgeber „bei der Ordnung von Massenerscheinungen" auch „generalisierende, typisierende und pauschalisierende Regelungen verwenden" und vor diesem Hintergrund von einem Gesamtbild ausgehen, „das sich aus den vorliegenden Erfahrungen ergibt".[339] Mit den Informationsbefugnissen zur Abfrage des allgemeinen Sicherheitszustands (§ 109 Abs. 4 TKG) und zur Sicherstellung der Einhaltung von Sicherheitspflichten (§ 115 Abs. 1 TKG) hat der Gesetzgeber jedoch informationsverwaltungsrechtliche Tatbestände in Anwendungsbereich der Netz- und Informationssicherheit geschaffen, die auf den Ausgleich typischer allgemeiner Wissensdefizite auf Seiten der Sicherheitsbehörde zielen. Ein Rückgriff auf die Auskunftsbefugnis des § 127 TKG ist damit ausgeschlossen.[340]

Für das Informationsverwaltungsrecht im Bereich der Netz- und Informationssicherheit kommt der informationellen Generalbefugnis demnach grundsätzlich keine weitergehende Bedeutung zu.

3. Nachrichtendienstliche Instrumente zur Informationsgewinnung

Die nachrichtendienstlichen Informationsbefugnisse des Bundesnachrichtendienstes (a) sowie des Bundesamtes für Verfassungsschutz (b) zum Erkennen von Cybergefahren zeichnen sich durch die Möglichkeit der Anwendung verdeckter und damit zumeist unbekannter nachrichtendienstlicher Mittel aus. Den besonderen Auskunftsverlangen der Nachrichtendienste gegenüber Telekommunikationsunternehmen und Telemediendiensteanbietern kommt lediglich eine untergeordnete Bedeutung in der Generierung von sicherheitsrelevanten Informationen zu (c).

a) Überwachung des Internetdatenverkehrs zur Erkennung von Cybergefahren

Der Bundesnachrichtendienst darf internationale Telekommunikationsbeziehungen, die von Art. 10 GG geschützt sind, strategisch beschränken, um Cybergefahren rechtzeitig zu erkennen (aa). Zu Erfüllung dieser Aufgabe kann er in weit größeren Umfang Internetdatenverkehr im Rahmen der Ausland-Ausland-Fernmeldeaufklärung überwachen (bb).

---

[338] *Holznagel/Schulz*, MMR 2002, 364 (366); *Badura*, in: ders./von Danwitz/Herdegen/Sedemund/Stern (Hrsg.), BeckPostG, 2. Aufl. 2004, § 45 Rn. 16.

[339] BVerfGE 100, 230 (236).

[340] Im Ergebnis auch *Eckhardt*, in: Geppert/Schütz (Hrsg.), BeckTKG, 4. Aufl. 2013, § 115, Rn. 7; *Meyer-Sebastian*, in: Geppert/Schütz (Hrsg.), BeckTKG, 4. Aufl. 2013, § 127, Rn. 15; zur Idealkonkurrenz zu Auskunftsverlangen mit anderer Zweckrichtung OVG NRW, MMR 2011, 698 (699).

aa) Strategische Fernmeldeaufklärung

Im Rahmen der Fernmeldeaufklärung kommen § 3 G10 für Beschränkungsmaßnahmen in Einzelfällen (Individualmaßnahmen) und § 5 G10 für strategische Beschränkungen der Informationsbefugnisse in Betracht. Die Normen weisen sowohl Aufgaben als auch Objekte der Maßnahmen zu, sie sind aber zugleich Eingriffstatbestände zur Erhebung von Telekommunikationsverkehrsdaten.

Im Rahmen der Individualmaßnahmen können deutsche Verfassungsschutzbehörden und Nachrichtendienste nach § 3 Abs. 1 S. 1 Nr. 8 G10 gezielte Beschränkungen von Art. 10 GG anordnen, wenn tatsächliche Anhaltspunkte dafür bestehen, dass jemand Straftaten nach §§ 202a, 202b und 303a, 303b StGB plant. Beim Ausspähen und Abfangen von Daten sowie bei Datenveränderung und Datensabotage handelt es sich um das sog. Cyberstrafrecht, also um Delikte mit Computer- und Internetbezug.[341] Eingeschränkt wird die Befugnis durch die Verweisung auf § 1 Abs. 1 Nr. 1 G10 und durch die Voraussetzung, dass die Befugnis nur Straftaten betrifft, die gegen die innere und äußere Sicherheit gerichtet sind, insbesondere gegen sicherheitsempfindliche Stellen von lebenswichtigen Einrichtungen. Insofern findet sich in der Norm der objektivierte Ausdruck des Gewichts der Schutzgüter.[342] Damit zielt die Befugnis auf mögliche Angriffsziele wie Betreiber von kritischen Infrastrukturen und (kritischen) Telekommunikationsunternehmen.[343] Die allgemeine Verweisung auf die Voraussetzungen des § 1 Abs. 1 Nr. 1 verdeutlicht, dass es bei dieser Befugnis um die Abwehr von drohenden Gefahren im Vorfeld akuter Krisenlagen geht und nicht originär um Strafverfolgung.

Weitergehende Befugnisse zur Sammlung von Informationen über Sachverhalte und Gefahrenbereiche sowie der Begegnung solcher Gefahren ergeben sich für die strategische Fernmeldeüberwachung. Diese obliegt dem Bundesnachrichtendienst. Ziel der strategischen Überwachung „internationaler Kommunikationsbeziehungen" ist es, Gefahren „rechtzeitig zu erkennen und einer solchen Gefahr zu begegnen", § 5 Abs. 1 S. 3 G10. Weder ist ein konkreter Tatverdacht noch eine Gefahr erforderlich.[344] Letztlich reicht eine (nahezu immer gegebene und kaum konturierte) allgemeine Bedrohungslage aus, weshalb eine permanen-

---

[341] Zum europäischen und internationalen Rechtsrahmen *Reindl-Krauskopf*, ZaöRV 2014, 563 ff.

[342] Nach BVerfGE 126, 260 (329) muss die Qualifizierung einer Straftat als schwer in der Strafnorm einen objektivierten Ausdruck finden.

[343] Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes, Bearbeitungsstand 25.03.2015, Begründung, S. 43 f.

[344] Vgl. BVerfGE 100, 313 (383).

te Überwachung stattfinden kann.[345] Die technische Fernmeldeaufklärung zur Abwehr von Cyberbedrohungen wird nachrichtendienstlich als „SIGINT Support to Cyber Defense“ (SSCD) bezeichnet.[346] Cyberbedrohungen werden mittels technischer Aufklärungsmethodik erkannt, wobei der Aufklärungsansatz in der Suche nach Schadsoftware mit SIGINT-Methoden besteht. SIGINT (Signals Intelligence) bezeichnet die Form der technischen Fernmeldeaufklärung,[347] durch die Kommunikationsströme aufgeklärt werden. Konkret ist darunter zu verstehen, dass Datenpakete der Datenströme untersucht werden.

Zulässige Aufklärungsziele strategischer Beschränkungen und bestimmte Gefahrenbereiche werden in § 5 Abs. 1 S. 3 G10 benannt und aufgezählt. Der 2016 in Kraft getretene § 5 Abs. 1 S. 3 Nr. 8 G10 erweitert die Beschränkungsmöglichkeiten des internationalen Telekommunikationsverkehrs um Cybergefahren. Die in Abs. 1 S. 3 Nr. 1 bis 7 aufgezählten Bereiche würden sich „im Hinblick auf die neuen Gefahren des Cyberraums als defizitär“ erweisen, sodass eine gesetzliche Befugnis zur Aufklärung schadbehafteter internationaler Telekommunikationsverkehre einzuräumen sei.[348] Unter dieser Kategorie sind Gefahren des „internationalen kriminellen, terroristischen oder staatlichen Angriffs mittels Schadprogrammen oder vergleichbaren schädlich wirkenden informationstechnischen Mitteln auf die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen in Fällen von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland“ zu verstehen. Eine Legaldefinition des Begriffs des Schadprogramms findet sich in § 2 Abs. 5 BSIG. Darunter sind Programme und sonstige informationstechnische Routinen und Verfahren zu verstehen, die dem Zweck dienen, unbefugt Daten zu nutzen oder zu löschen, oder die dem Zweck dienen, unbefugt auf sonstige informationstechnische Abläufe einzuwirken.

Die Erweiterung um eine cyberbezogene Gefahrbestimmung ermöglicht die Überwachung des Datenverkehrs, um Cyberangriffe in Gestalt von Cyberspionage, Cyberausspähung oder Cybersabotage insbesondere gegen kritische Infrastrukturen zu erfassen und letztere dadurch zu härten. Da § 5 Abs. 1 S. 3 Nr. 8 auch Angriffe mit informationstechnischen Mitteln auf die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen, die eine mit Schadpro-

---

345 *Bäcker*, K&R 2014, 556 (557).

346 *Schindler*, Wirtschaftsschutz – Strategien und Herausforderungen für den Bundesnachrichtendienst, Rede des BND-Präsidenten anlässlich des 11. Symposiums des Bundesamtes für Verfassungsschutz am 8. Mai 2014, online abrufbar.

347 Damit werden im nachrichtendienstlichen Sprachgebrauch die Fernmeldeaufklärung und die (sonstige) elektronische Aufklärung bezeichnet. Siehe dazu *Ferris*, Signals Intelligence in War and Power Politics, in: Johnson (Hrsg.), The Oxford Handbook of National Security Intelligence, 2010, S. 155 ff.

348 BT-Drs. 18/4654, S. 40.

grammen vergleichbare Wirkung haben, erfasst, können auch Verfügbarkeitsangriffe gegen IT-Systeme wie Denial-of-Service-Attacken, Man-in-the-Middle-Angriffe via DNS-Spoofing, Angriffe auf IT-Systeme unter Umgehung von physikalischen Grenzen (Abzug von Informationen von Systemen, die nicht an einem Netzwerk angebunden sind, unter Ausnutzung etwa der Abstrahlung) oder auch Hardwaremanipulationen von Netzwerkgeräten aufgeklärt werden.[349] Die Gesetzesbegründung führt dazu aus, dass die Erweiterung des § 5 Abs. 1 S. 3 G10 um eine Nr. 8 den Bundesnachrichtendienst in die Lage versetzen soll, „die technisch (nur) durch ihn generierbaren Erkenntnisse zur Cyber-Bedrohungslage und -Abwehr beizusteuern.“[350]

Gegenstand der strategischen Überwachung sind internationale Kommunikationsbeziehungen, soweit eine gebündelte Übertragung erfolgt. Erfasst ist auch die leitungsgebundene Telekommunikation.[351] In der Anordnung der Beschränkungsmaßnahme, für die nach § 10 G10 das Bundesministerium des Innern zuständig ist, sind die Übertragungswege, die der Beschränkung unterliegen, zu bezeichnen.

Das limitierende Tatbestandsmerkmal der „internationalen Kommunikationsbeziehungen“ in § 5 Abs. 1 S. 1 G10 ist allerdings problematisch. Die Eingrenzung entspricht an sich der Begrenzung der Aufgabe des Bundesnachrichtendienstes auf die Auslandsaufklärung.[352] Für die Internetkommunikation ist allerdings schon aufgrund der technischen Bedingungen fragwürdig, ob dieses Kriterium operabel ist. Naheliegend ist eine Auslegung des Merkmals, die auf den Ort der Kommunikationspartner abstellt. Ein internationaler Telekommunikationsverkehr läge vor, wenn mindestens einer der Teilnehmer die Kommunikation im Ausland empfängt oder absendet. Denkbar ist dagegen auch, dass die Inlandskommunikation über das Ausland realisiert wird, weil die Diensteanbieter im Ausland operieren oder weil sie die Kommunikation über Netzinfrastruktur im Ausland abwickeln. Diese Auslegung würde den Umstand berücksichtigen, dass der Datenverkehr im Internet entlang technischer und ökonomischer Parameter verläuft, nicht entlang nationaler Grenzen im Sinne eines nationalen Routings. Es soll der Staats- und Verwaltungspraxis entsprechen, das Tatbestandsmerkmal restriktiv auszulegen, wobei teilweise dennoch davon ausgegangen wird, dass im Rahmen der Fernmeldeaufklärung Telekommunikationsdaten erhoben werden, ohne dass sie sich auf die Ermächtigungen des G10

---

[349] BT-Drs. 18/4654, S. 41.

[350] BT-Drs. 18/4654, S. 41.

[351] Vgl. BVerfGE 100, 313 (376 ff.).

[352] *Huber*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, G 10, § 5, Rn. 2.

stützen.[353] Jedenfalls erfasst das Merkmal Kommunikationsbeziehungen, die von Ausländern im Ausland realisiert werden.

Der Bundesnachrichtendienst hat gemäß § 27 Abs. 2 Telekommunikations-Überwachungsverordnung (TKÜV) zunächst Zugriff auf eine vollständige Kopie der Telekommunikation (sog. Full-Take-Ansatz),[354] die gemäß § 2 Abs. 1 S. 3 G10 von den infrage kommenden Telekommunikationsdienstleistern an Übergabepunkten (beispielsweise am größten Internetknoten der Welt, DE-CIX in Frankfurt am Main) oder über eigene Einrichtungen ohne deren Mitwirkung (§ 10 Abs. 6 S. 1 G10) bereitgestellt wird.

Eine Obergrenze für die Überwachung enthalten § 10 Abs. 4 S. 3 und 4 G10. Bei Anordnung einer strategischen Beschränkungsmaßnahme darf nur ein Anteil von höchstens 20 % der zur Verfügung stehenden Übertragungskapazität des betreffenden Übertragungsweges überwacht werden. Zum einen soll durch diese Begrenzung einer lückenlosen Überwachung bestimmter Telekommunikationsbeziehungen vorgebeugt werden, zum anderen soll sie sicherstellen, dass der Ermächtigungserweiterung auf den leitungsgebundenen Telekommunikationsverkehr Rechnung getragen wird.[355] Die Telekommunikationsinhalte sind unverzüglich darauf zu überprüfen, ob sie für die Erfüllung der Zwecke nach § 5 Abs. 1 S. 3 G10 relevant sind. Andernfalls sind sie unverzüglich protokolliert zu löschen.

Für die über das Internet übermittelte Kommunikation ist die Begrenzung der Überwachung problematisch, da die Übertragungswege so angelegt sind, dass die maximale Übertragungskapazität möglichst nicht ausgeschöpft wird. Die maximale Übertragungskapazität des DE-CIX beträgt 18 Tbit/s, wobei 2015 der Rekord der Spitzenauslastung bei 5,1 Tbit/s lag.[356] Wenn die Norm in der Praxis so ausgelegt wird, dass die Übertragungs*kapazität* maßgeblich ist,[357] dann dürfte die Begrenzungswirkung der 20-%-Regelung *de facto* sehr gering

---

[353] Siehe dazu *Bäcker*, Erhebung, Bevorratung und Übermittlung von Telekommunikationsdaten durch die Nachrichtendienste des Bundes, Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 22.5.2014, unter IV. 1. mit Verweis auf die Stellungnahme der Bunderegierung in BVerfGE 100, 313 (337, 380) und auf die Gesetzesbegründung zur Änderung des G10 in BT-Drs. 14/5655, S. 18; *Papier*, NVwZ-Extra 2016, 1 (2); zur damit verbundenen Problematik, dass weder verfassungsrechtliche Restriktionen noch die in § 5 G10 Anwendung finden, sogleich im Rahmen der Überwachung der Ausland-Ausland-Telekommunikation.

[354] BT-Drs. 17/9640, S. 4.

[355] *Huber*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, G10, § 10, Rn. 10; BT-Drs. 14/5655, S. 18.

[356] *DE-CIX*, Quick facts, abrufbar unter: https://www.de-cix.net/about/quick-facts/.

[357] BT-Drs. 17/14739, S. 14.

sein.[358] Eine weniger strenge Auslegung führt dazu, dass die Begrenzung erst nach der Vorabselektion des inländischen Telekommunikationsverkehrs greift. Bei strenger Auslegung müsste das Höchstmaß am gemessenen Datenstrom bemessen werden. Der Umfang der Überwachung bestimmt sich formell nach der Anordnung des Bundesministeriums des Innern, die es auf Antrag des Bundesnachrichtendienstes mit Zustimmung der G10-Kommission erlässt (§ 5 Abs. 1 S. 1 und 2, § 10 Abs. 1 G10). Dabei legt das Bundesministerium auch die Selektoren fest, auf die die Kommunikation durchsucht werden darf (§ 10 Abs. 4 S. 1 G10).

Die Befugnis zur strategischen Fernmeldekontrolle erlaubt die systematische Untersuchung des Internetdatenverkehrs auf Gefahren für die Netz- und Informationssicherheit mit erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland. Die Effektivität dieser Befugnis bemisst sich in der Sache neben der Kapazitätsbegrenzung weitgehend nach den technischen Fähigkeiten zur Analyse großer Datenmengen auf schädliche Programme und netzbasierte Angriffe. Die gewonnenen Erkenntnisse können für die Sicherheitsgewährleistung im Rahmen des Informationsaustausches im Nationalen Cyber-Abwehrzentrum, an dem das BSI beteiligt ist, von Nutzen sein.[359]

bb) Überwachung der Ausland-Ausland-Telekommunikation

Eine weitergehende Befugnis zur Generierung von Informationen über Gefahren für die Netz- und Informationssicherheit besteht im BNDG. Mit dem 2017 in Kraft getretenen § 6 BNDG ist eine ausdrückliche Grundlage für die sog. Ausland-Ausland-Fernmeldeaufklärung geschaffen worden.

Nach § 6 Abs. 1 BNDG darf der Bundesnachrichtendienst zur Erfüllung seiner gemäß § 1 Abs. 2 S. 1 BNDG auslandsbezogenen Aufgaben vom Inland aus Informationen einschließlich personenbezogener Daten mit technischen Mitteln aus Telekommunikationsnetzen erheben und verarbeiten, wenn diese Daten dafür erforderlich sind, frühzeitig Gefahren für die innere oder äußere Sicherheit der Bundesrepublik Deutschland zu erkennen und diesen begegnen zu können (Nr. 1), um die Handlungsfähigkeit der Bundesrepublik Deutschland zu wahren (Nr. 2) oder um sonstige Erkenntnisse von außen- und sicherheitspolitischer Bedeutung zu gewinnen (Nr. 3). Eine Erforderlichkeit zur Gewinnung von sonstigen Erkenntnissen kann im Rahmen von Nr. 3 angenommen werden, wenn die Aufklärungstätigkeit im Einklang mit dem sog. Auftragsprofil der Bundesregierung (APB) steht, das das Bundeskanzleramt im Einvernehmen mit den zu-

---

[358] Vgl. aber BVerwG, NVwZ 2014, 1666 (1669).

[359] Siehe § 4 B. II. 2. c) (aa) (1).

ständigen Bundesministerien festgelegt.[360] Da auch das Bundesministerium des Innern zuständig ist, das wiederum gemäß § 1 S. 2 BSIG dem BSI übersteht, können hier Erkenntnisdefizite beim BSI im Rahmen des Einvernehmens Berücksichtigung finden.

Für die sog. Ausland-Ausland-Fernmeldeaufklärung gilt gemäß § 7 BNDG insbesondere der § 6 Abs. 1 S. 1 entsprechend.

Die Informationsgenerierung erfolgt bei dieser Fernmeldeaufklärung aus Telekommunikationsnetzen. Die Anordnungen zur Fernmeldeaufklärung richten sich folglich nicht gegen bestimmte einzelne Leitungswege, sondern auf Telekommunikationsnetze in ihrer Gesamtheit. Der Begriff bezieht sich auf die telekommunikationsrechtliche Definition in Art. 2 lit. a RL 2002/21/EG bzw. § 3 Nr. 27 TKG, die „die Gesamtheit von Übertragungssystemen […] einschließlich des Internets" erfasst. Anders als bei der strategischen Fernmeldeaufklärung nach dem G10 sind daher in der Anordnung im Sinne von § 6 Abs. 1 S. 2 BNDG, d. h. in der Bestimmung der zu überwachenden Telekommunikationsnetze, nicht die der Beschränkung unterliegenden Übertragungswege zu bezeichnen. In praktischer Hinsicht kann die Ausleitung von Telekommunikationsverkehren grundsätzlich an einer beliebigen Stelle eines Telekommunikationsnetzes erfolgen.[361] In Betracht kommen die wichtigen Backbone-Leitungen der großen Telekommunikationsnetzbetreiber, aber auch das Netz der deutschen Internetknoten.

Aus § 6 Abs. 2 BNDG ergibt sich, dass der Bundesnachrichtendienst Inhaltsdaten anhand von Suchbegriffen erheben darf. Insofern kommt eine Analyse des tieferliegenden Datenstroms in Betracht, d. h., auf Grundlage von § 6 BNDG kann grundsätzlich, im Rahmen des technisch Möglichen, das gesamte Datenpaket auf bestimmte Merkmale analysiert werden.

Anders als die strategische Fernmeldeaufklärung nach dem G10 besteht für die Ausland-Ausland-Fernmeldeaufklärung keine besondere quantitative Begrenzung des Umfangs der Ausleitung von Verkehrsdaten aus einem Telekommunikationsnetz. Eine Limitierung ergibt sich daher nur durch die Erforderlichkeit der Daten für die Aufgabenerfüllung und auf tatsächlicher Ebene durch begrenzte personelle, technische und finanzielle Mittel zur Durchführung etwaiger Maßnahmen.

Inwiefern § 6 BNDG in der Praxis zur Erkenntnisgewinnung beitragen wird, ist auch von der Frage abhängig, ob die Norm verfassungsrechtlich Bestand haben wird.[362]

---

[360] BT-Drs. 18/9041.

[361] Die Telekommunikationsdienste haben gemäß § 8 Abs. 1 BNDG Auskunft über die näheren Umstände der nach Wirksamwerden der Anordnung durchgeführten Telekommunikation zu erteilen.

[362] Dies verneint *Huber*, ZRP 2016, 162 (163). Das primäre Unionsrecht stellt für die Be-

Der Gesetzgeber geht mangels Bezeichnung im Sinne des Zitiergebots des Art. 19 Abs. 1 S. 2 GG und trotz besonderem Bezug nicht davon aus, dass Art. 10 GG durch die Maßnahmen aufgrund der Regelungen im BNDG eingeschränkt wird (vgl. § 6 Abs. 4 BNDG). Daraus lässt sich auf ein spezifisches Verständnis des durch Art. 10 GG geschützten Fernmeldegeheimnisses schließen. Der Gesetzgeber geht davon aus, dass die Ausland-Ausland-Fernmeldeaufklärung keine Relevanz für das Fernmeldegeheimnis hat. In diesem Sinne ist auch die Auffassung des Gesetzgebers zu verstehen, nach der die Norm ungeachtet ihrer Ausgestaltung als Befugnis als nicht begrenzende Konkretisierung des gesetzlichen Auftrags der Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung sind, aufzufassen ist.[363] Nach § 6 Abs. 4 BNDG ist die Erhebung von Telekommunikationsverkehrsdaten von deutschen Staatsangehörigen unzulässig. Diese Regelung lässt darauf schließen, dass der Gesetzgeber das Fernmeldegeheimnis als Deutschen-Grundrecht auslegt, obwohl es dem Wortlaut nach, anders als etwa Art. 12 GG, als Jedermann-Grundrecht formuliert ist. Gemäß Art. 3 Abs. 1 GG sind unterscheidende gesetzliche Beschränkungen grundsätzlich unzulässig. Problematisch ist zudem, dass gemäß § 6 Abs. 1 S. 1 BNDG die Ausland-Ausland-Aufklärung „vom Inland aus" durchgeführt werden kann. Aus Art. 1 Abs. 3 GG folgt, dass die vollziehende Gewalt vor allem auf dem Territorium der Bundesrepublik Deutschland der Grundrechtsbindung unterliegt.[364]

Aus der fehlenden Bindung an Art. 10 GG folgt, dass bei Maßnahmen auf Grundlage von § 6 BNDG die Beschränkungen des § 5 Abs. 2 S. 2 G10 nicht gelten. Danach ist es verboten, Suchbegriffe in die Filterung aufzunehmen, die aufgrund bestimmter Merkmale zu einer gezielten Erfassung bestimmter Telekommunikationsanschlüsse führen.[365] Dagegen dürfen nach § 6 Abs. 3 Nr. 1

---

wertung nachrichtendienstlicher Tätigkeit der Mitgliedstaaten außerhalb des Anwendungsbereichs grundsätzlich keinen unmittelbaren Bewertungsmaßstab dar. Zu berücksichtigen ist, dass gemäß Art. 4 Abs. 2 S. 3 EUV die nationale Sicherheit weiterhin in die alleinige Verantwortung der Mitgliedstaaten fällt. In den Sekundärrechtsakten bestehen im Übrigen regelmäßig Bereichsausnahmen für die nachrichtendienstliche Tätigkeit, vgl. Art. 2 Abs. 2 DS-GVO, Art. 1 Abs. 3 sowie Erwägungsgrund 11 RL 2002/58/EG.

[363] Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes, BT-Drs. 18/9041, S. 22.

[364] Die extraterritoriale Schutzwirkung von Art. 10 Abs. 1 GG betont das Bundesverfassungsgericht ausdrücklich in BVerfGE 100, 313 (363 f.).

[365] Von diesem Verbot macht § 5 Abs. 2 S. 3 G10 wiederum eine Ausnahme. Ausgenommen von dem Verbot sind Telekommunikationsanschlüsse im Ausland, sofern ausgeschlossen ist, dass Anschlüsse, deren Inhaber oder regelmäßige Nutzer deutsche Staatsangehörige sind, gezielt erfasst werden. Darin sehen einen Verstoß gegen den Vorbehalt des Gesetzes in Art. 10 Abs. 2 GG *Huber*, NJW 2013, 2572 (2574); *Bäcker*, K&R 2014, 556 (559); *Papier*,

BNDG Suchbegriffe auch zur gezielten Erfassung von Einrichtungen der Europäischen Union, von öffentlichen Stellen ihrer Mitgliedstaaten oder von Unionsbürgerinnen oder Unionsbürgern führen, wenn dies erforderlich ist, um Gefahren im Sinne des § 5 Abs. 1 S. 3 G10, d. h. auch die in Nr. 8 genannten Angriffe auf die Netz- und Informationssicherheit, zu erkennen und zu begegnen.

Als weiteres Problem sind mögliche Defizite des Filtersystems anzusehen. Um den Datenverkehr, der nur im Rahmen von Beschränkungsmaßnahmen nach dem G10 analysiert werden kann, zu separieren, setzt der Bundesnachrichtendienst ein mehrstufiges automatisiertes Filtersystem ein, um den von der Erfassung ausgenommenen Verkehr zu erkennen und ihn unverzüglich und unwiederbringlich zu löschen.[366] Zwar können kommerzielle Filtersysteme zur Separierung von IP-Verkehren mit Regionalbezug Filterqualitäten von 99,5 % erreichen, das vom Bundesnachrichtendienst selbst entwickelte System zur Filterung der G10-Verkehren soll aber nur eine Genauigkeit von circa 95–96 % erreichen.[367] Legte man dennoch für die Filterung im Rahmen von § 6 BNDG eine Genauigkeit von 95,5 % oder höher zugrunde, könnte das am Netzknoten DE-CIX, an dem täglich mehrere Milliarden IP-Verbindungen verarbeitet werden, zu mehreren Millionen fehlerhaft erfassten Verbindungen führen, die an sich auf Grundlage von G10 verarbeitet werden müssten. Das aufgrund des vom NSA-Untersuchungsausschuss ergangenen Beweiserhebungsbeschlusses[368] erstellte Sachverständigengutachten zur Frage nach erprobten oder wissenschaftlich anerkannten Methoden der länderübergreifenden Geolokalisierung von IP-Adressen bzw. IP-Datenpaketen und deren Zuverlässigkeit für eine Zuordnung zum Standort Deutschland betont, dass etwaige Verfahren sich hinsichtlich Genauigkeit und Aussagekraft direkt oder indirekt negativ beeinflussen lassen.[369]

NVwZ-Extra 2016, 1 (7; 5: „in jeder Hinsicht und offenkundig […] unhaltbar"); aus prozessualen Gründen offengelassen in BVerfGE 100, 313 (284).

[366] BT-Drs. 18/9041, S. 24; vgl. BT-Drs. 17/9640, S. 6: „mehrstufiges Bewertungsverfahren"; BT-Drs. 17/14739, S. 14 ff.

[367] Verband der Internetwirtschaft e.V. (eco), Praktische Auswirkungen und technische Implikationen des Entwurfs eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes (BT-Drs. 18/9041), Stellungnahme vom 14.10.2016, S. 7.

[368] Beweisbeschluss SV-13 vom 14. April 2016 im Rahmen des Untersuchungsauftrags BT-Drs. 18/843, Frage 8.

[369] *Rodosek*, Sachverständigengutachten zu Frage 8 des zum Beweisbeschlusses SV-13 im Rahmen des Untersuchungsauftrags BT-Drs. 18/843, 1. Untersuchungsausschuss der 18. Wahlperiode, S. 29 f.; *Rechthien*, Sachverständigengutachten zu Frage 8 des Beweisbeschlusses SV-13 im Rahmen des Untersuchungsauftrags BT-Drs. 18/843, 1. Untersuchungsausschuss der 18. Wahlperiode, S. 13 f.

Damit kann festgehalten werden, dass im Rahmen der Ausland-Ausland-Fernmeldeaufklärung auf Grundlage des BNDG Cybergefahren, insbesondere solche für kritische Infrastrukturen, weitreichend detektiert werden können. Insgesamt stellen damit §§ 6 und 7 BNDG Ermächtigungen zur Analyse des Datenstroms über das Internet dar, die dem Bundesnachrichtendienst weitreichenden Handlungsspielraum eröffnet. Auf Grundlage der Norm ist es eine Frage der technischen Möglichkeiten, den betreffenden Ausland-Ausland-Telekommunikationsverkehr vom Datenstrom zu separieren und die darin enthaltenen Schadprogramme oder vergleichbar schädlich wirkenden Angriffe mit informationstechnischen Mitteln auf die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen zu erkennen. Welche Kenntnisse gewonnen werden, richtet sich außerdem nach dem Auftragsprofil der Bundesregierung. Bei der Erstellung des Auftragsprofils können etwaige Erkenntnisdefizite beim BSI Berücksichtigung finden. Der Bestand von § 6 BNDG ist mit Blick den Grundrechtskonflikt allerdings noch klärungsbedürftig.

b) Besondere nachrichtendienstliche Mittel zum Schutz kritischer Infrastrukturen

Zum Schutz kritischer Infrastrukturen kann neben dem Bundesnachrichtendienst das Bundesamt für Verfassungsschutz (BfV) von Informationsbefugnissen Gebrauch machen. Der Zuständigkeitsraum und das Tätigkeitsfeld des BfV beginnen im Vorfeld der konkreten Gefahr. Die Befugnisse, die dem BfV zur Erfüllung der Aufgaben zur Verfügung stehen, sind in §§ 8 ff. BVerfSchG und im G10 zur Überwachung der Telekommunikation niedergelegt. Informationen und Daten, auch personenbezogene, dürfen nach § 8 Abs. 2 BVerfSchG mit besonderen nachrichtendienstlichen Mitteln erhoben werden.[370] Die Aufzählung der im Gesetz genannten Mittel ist nur beispielhaft („wie"). Sie deckt auch andere nachrichtendienstliche Mittel, deren Einsatz etwa aufgrund neuer technischer oder tatsächlicher Entwicklungen möglich oder notwendig werden kann.[371] Die Informationsbeschaffung darf heimlich stattfinden. Es sind in der Aufzählung alle Methoden erfasst, mit denen getarnt werden soll, dass das BfV eine Information gewinnen will.[372] Voraussetzung zur Sammlung und Auswertung von Informationen ist, dass tatsächliche Anhaltspunkte vorliegen.[373] So

[370] Dazu gehören der Einsatz von Vertrauensleuten und Gewährspersonen, Observationen, Bild- und Tonaufzeichnungen, Tarnpapiere und Tarnkennzeichen. Siehe BVerfG, NJW 2013, 1499 (1504, Rn. 117 ff.).

[371] BT-Drs. 11/4306, S. 85; *Roth*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2014, BVerfSchG, § 8 Rn. 24.

[372] BT-Drs. 11/4306, S. 61; BayVerfGH, NVwZ-RR 1998, 273 (278).

[373] Die Voraussetzung ist systemwidrig in § 4 Abs. 1 S. 3 BVerfSchG geregelt, der Be-

könnten etwa Honeypots dann eingesetzt werden, wenn Anhaltspunkte geeignet sind, einen Verdacht verfassungsfeindlicher Bestrebungen zu begründen. Honeypots werden in der Computersicherheit eingesetzt, um Informationen über Angriffsmuster und Angreiferverhalten zu erhalten. Dabei wird ein Netzwerkdienst oder das Verhalten eines Anwenders simuliert.[374] Obwohl es sich dabei nur um ein vorgetäuschtes System handelt, kann jeder Zugriff darauf als Angriffsversuch bewertet werden. Wichtige Anhaltspunkte für Angriffe kann das BfV zudem indirekt generieren. Das BSI unterstützt die Verfassungsschutzbehörden bei der Auswertung und Bewertung von Angriffen mit terroristischem oder nachrichtendienstlichem Bezug (§ 3 Abs. 1 S. 2 Nr. 13 b) BSIG). Insbesondere gibt das BSI Informationen über Gefahren, potenzielle Auswirkungen und das Lagebild an das BfV weiter (§ 8b Abs. 2 Nr. 4 b) BSIG).[375]

Zu den nachrichtendienstlichen Maßnahmen zählt auch die heimliche Telekommunikationsüberwachung. Solche Maßnahmen haben allerdings im G10 eine besondere und abschließende Regelung gefunden.[376] Als zulässiges nachrichtendienstliches Mittel zählt aber der heimliche Zugriff auf im Internet nicht öffentlich zur Verfügung stehender Daten oder der heimliche Zugriff auf informationstechnische System, indem entsprechende Sicherheitsvorkehrungen überwunden werden.[377]

c) Nachrichtendienstliche Auskunftsverlangen

Die Nachrichtendienste können Auskunft über Bestands- und Nutzungsdaten (aa) und über Strukturen der Telekommunikationsdienste- und netze verlangen (bb).

aa) Auskunft über Bestands- und Nutzungsdaten bei Anbietern von Telemediendiensten

Eine sicherheitsrechtliche Informationsbefugnis im Telemedienrecht findet sich in § 14 Abs. 2 TMG, auf dessen Grundlage Auskünfte über Bestandsdaten er-

griffsbestimmungen vornimmt. Es handelt sich dabei aber um eine materiell-rechtliche Voraussetzung, siehe *Roth*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, BVerfSchG, § 8 Rn. 21.

[374] Fraunhofer FOKUS Kompetenzzentrum Öffentliche IT: Das ÖFIT-Trendsonar der IT-Sicherheit – Honeynet, April 2016, S. 22.

[375] Siehe § 4 B. II. 2. c) aa).

[376] BVerfGE 120, 274 (306 ff.).

[377] *Roth*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2014, BVerfSchG, § 8 Rn. 40; BVerfGE 120, 274 (302 ff.).

teilt werden dürfen. Über § 15 Abs. 5 S. 4 TMG findet das Auskunftsrecht auch auf Nutzungsdaten Anwendung.

§ 14 Abs. 2 TMG ist eine Erlaubnisnorm im Sinne von § 12 Abs. 2 TMG, d. h. die Norm stellt selbst keine Ermächtigungsgrundlage zur Datenabfrage dar. Lediglich die datenschutzrechtliche Zulässigkeit der Datenübermittlung wird sichergestellt. Die Vorschrift beruht auf den Leitgedanken des unionsrechtlichen Datenschutzes.[378] Darüber hinaus gibt es bis auf den Zweck der Durchsetzung der Rechte am geistigen Eigentum zur (vorzeitigen) Umsetzung der Enforcement-Richtlinie[379] keine europarechtliche Vorgabe. Allerdings ist sowohl nach der RL 2002/58/EG (Art. 15) als auch nach der DS-GVO (Art. 2, 23) eine Datenverarbeitung grundsätzlich zulässig, sofern sie für die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten notwendig, angemessen und verhältnismäßig ist.

Eine Auskunft nach Art. 14 Abs. 2 TMG darf nur für Zwecke der Strafverfolgung, der Gefahrenabwehr durch die Polizeibehörden der Länder, zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes oder des Bundeskriminalamtes im Rahmen seiner Aufgabe zur Abwehr von Gefahren des internationalen Terrorismus erteilt werden. Diensteanbieter wie Host-Provider dürfen danach auf Anordnung der zuständigen Stellen im Einzelfall Auskunft über diese Daten erteilen. Die Tätigkeit des BSI oder der Bundesnetzagentur fällt nicht unter die abschließende Aufzählung der Zwecke.[380]

Im Vorfeld der polizeilichen Gefahrenabwehr kann für die Netz- und Informationssicherheit insbesondere die Aufgabenerweiterung des Bundesnachrichtendienstes nach § 3 Abs. 1 Nr. 8 bzw. § 5 Abs. 1 Nr. 8 G10 im Rahmen der Fernmeldeaufklärung Bedeutung erlangen. Die zur Erlaubnisnorm für Diensteanbieter komplementäre Ermächtigungsgrundlage des Bundesnachrichtendienstes findet sich in § 2a BNDG in Verbindung mit §§ 8a, 8b BVerfSchG. Der Bundesnachrichtendienst darf zur Erfüllung seiner Aufgaben nach § 1 Abs. 2 BNDG Auskünfte einholen.

---

[378] *Schreibauer*, in: Auernhammer, 4. Aufl. 2014, TMG, § 14 Rn. 2.

[379] RL 2004/48/EG.

[380] Vgl. *Hornung*, NJW 2015, 3334 (3338), der daraus schlussfolgert, dass nach § 8b BSIG keine Befugnis zur Übermittlung an das BSI von Bestands- und Nutzungsdaten nach dem TMG besteht. Siehe auch *Hullen*/*Roggenkamp*, in: Plath (Hrsg.), BDSG, 2013, § 14 Rn. 22, die § 14 Abs. 2 TMG analog auch für andere Rechtsverletzungen, hier Persönlichkeitsrechtsverletzungen, heranziehen wollen. Eine analoge Anwendung zum Zwecke des Schutzes anderer Verletzungen und Gefahren scheidet aber aus, vgl. BGH, NJW 2014, 2651 (2652 f.).

Allerdings kann auf Grundlage der Auskunftsbefugnis eine tiefergehende und systematische Datenanalyse nicht stattfinden. Ein Auskunftsverlangen ist nur gerechtfertigt, wenn es im Einzelfall erforderlich ist. Gegenstand eines Herausgabeverlangens können außerdem nur vorhandene Bestands- und Nutzungsdaten sein, die eher bei der Attribution eines Angriffs als bei der Analyse der Angriffsmuster und des Angreiferverhalten helfen können. Eine Datensammlungs- und Speicherpflicht für die Diensteanbieter begründet die Vorschrift im Übrigen nicht.[381]

bb) Auskunft über Strukturen der Telekommunikationsdienste und -netze

Mit § 114 Abs. 1 TKG besteht eine indirekte Informationsbefugnis des BND, die darauf zielt, Informationen über die Strukturen der Telekommunikationsdienste und -netze sowie bevorstehende Änderungen zu erlangen. Der konkrete Zweck der Unterrichtung des BND lässt sich dem Wortlaut der Vorschrift nicht entnehmen. Die historische Auslegung weist auf die Strukturen der eingesetzten Technik und Verfahren hin.[382] Das Anfragerecht besteht demnach jedenfalls nur hinsichtlich der Strukturen der Telekommunikationsdienste im Sinne von § 3 Nr. 24 TKG und der Telekommunikationsnetze im Sinne von § 3 Nr. 27 TKG. Inhaltlich ist die Auskunft an die Erfüllung der Aufgaben nach den §§ 5 und 8 G10 sowie die Maßnahmen nach den §§ 6, 12 und 14 BNDG geknüpft. Durch den Verweis auf § 5 G10 ist die Informationsbefugnis des BND auf gebündelte Übertragungen beschränkt und die ersuchte Information muss eine Bedeutung in Bezug auf internationale Kommunikationsbeziehungen haben.[383] Dem § 114 Abs. 2 S. 2 TKG lässt sich entnehmen, dass die Daten nur für den Zweck verwendet werden dürfen, den BND in die Lage zu versetzen, die Struktur zu verstehen, um (technische) Maßnahmen zur Cyberabwehr zu implementieren. Eine Verwendung bei dem am zweistufigen Auskunftsverfahren beteiligten Bundesministerium für Wirtschaft und Energie, etwa für die Politikgestaltung, ist ausgeschlossen.[384] Insofern ist nach § 114 Abs. 2 S. 1 TKG Voraussetzung für die Zulässigkeit einer Anfrage ein entsprechendes Ersuchen des Bundesnachrichtendienstes.

Die Informationsbefugnis zur Auskunft über die technischen Strukturen bei den Telekommunikationsunternehmen ist somit eine Voraussetzung für die Implementierung strategischer Fernmeldebeschränkungen. Über § 114 TKG kann der Bundesnachrichtendienst ermitteln, an welchen Knotenpunkten etwa eine

---

381 *Roßnagel*, NVwZ 2007, S. 743 (748).

382 Zu § 89 TKG a. F. BT-Drs. 13/3609, S. 57.

383 *Eckhardt*, in: Geppert/Schütz (Hrsg.), BeckTKG, 4. Aufl. 2013, § 114 Rn. 6.

384 *Klesczewski*, in: Säcker (Hrsg.), TKG, 3. Aufl. 2013, § 114 Rn. 15.

Ausleitung des Internetdatenverkehrs technisch möglich ist und ob eine Verpflichtung der Diensteanbieter für die Durchführung einer Maßnahme in Betracht kommt. Eine unmittelbare epistemische Relevanz in der Sicherheitsgewährleistung kommt der Norm somit nicht zu.

III. Übernahme verwaltungsexternen Wissens

Die Verwaltung ist zur Produktion sicherheitsrelevanten Wissens neben der Informationsgewinnung über die an Unternehmen adressierten Pflichten auf die kooperative Übernahme von Wissen und Expertise bei Privaten angewiesen.[385] Sie kann sich schon aufgrund der Geschwindigkeit der technischen Veränderungen, des Erkenntnisfortschritts in der Netz- und Informationssicherheit sowie der personellen und organisatorischen Möglichkeiten nicht allein auf die Informationsgenerierung vermittels der aufgezeigten Informationsbefugnisse verlassen. Dies betrifft nicht nur den Bereich der Netz- und Informationssicherheit. Es ist eine allgemeine Beobachtung, dass Verwaltungen in Zeiten zunehmender Komplexität auf die Übernahme von Sachverstand und Expertise aus verwaltungsexternen Quellen angewiesen sind.[386] Gerade im äußerst dynamischen Regulierungsrecht stellt der Rückgriff auf externen Sachverstand nicht die Ausnahme dar, sondern hat sich zum Regelfall entwickelt.[387] Der Wissensbedarf bezieht sich auf Sachverstand, sachkundige Personen mit theoretischem als auch praktischem Fach- und Erfahrungswissen sowie auf wissenschaftlichen Sachverstand.[388] Begründet werden kann der Rückgriff insbesondere mit einer „besonderen Problemnähe“ entsprechender Fachkompetenzen,[389] aber auch mit den begrenzten personellen wie organisatorischen Ressourcen der Behörden, die nicht ausreichen, um gegenstandsadäquat Spezialinformationen zu generieren.[390]

Ein Sachverständigenbeteiligungsrecht im Sinne des Allgemeinen Verwaltungsrechts besteht nicht. Es liegt mit § 26 Abs. 1 Nr. 1 VwVfG lediglich eine Grundregel vor, nach der die Behörde zur Ermittlung des Sachverhalts Auskünfte jeder Art einholen, d. h. Sachverstand zu Rate ziehen kann. In dem die

---

385 Vgl. Erwägungsgrund 35 NIS-RL.

386 Vgl. *Nußberger*, Sachverständigenwissen als Determinante verwaltungsrechtlicher Einzelentscheidungen, AöR 129 (2004), 282 (284 ff.).

387 Zum Bereich Telekommunikation *Wollenschläger*, Wissensgenerierung im Verfahren, 2009, S. 116 ff.

388 Zur Differenzierung *Nußberger*, AöR 129 (2004), 282 (291 f.); *Scholl*, Der private Sachverständige im Verwaltungsrecht, 2005, S. 98 ff.

389 *Augsberg*, Informationsverwaltungsrecht, 2014, S. 118.

390 *Voßkuhle*, Sachverständige Beratung des Staates, in: Isensee/Kirchhof (Hrsg.), HbStR III, § 43 Rn. 2 ff.

Netz- und Informationssicherheit betreffenden Verwaltungsrecht finden sich darüber hinaus spezielle Bestimmungen, welche die Beteiligung Privater an der Wissensgenerierung zu fördern geeignet sind.

1. Kooperation mit Privaten

Das BSI hat gemäß § 3 Abs. 1 Nr. 15 BSIG die gesetzliche Aufgabe, „im Verbund mit der Privatwirtschaft" für die Krisenfrüherkennung, Krisenreaktion und Krisenbewältigung geeignete Kommunikationsstrukturen zur Gewährleistung der Sicherheit in der Informationstechnik kritischer Infrastrukturen aufzubauen.

Es besteht damit nicht nur eine lediglich im Ermessen des BSI bestehende Möglichkeit zur Kooperation, sondern ein zur Pflicht verdichteter Kooperationsauftrag, der sowohl den Austausch theoretischen als auch anwendungsbezogenen Wissens umfassen kann.

Eine Verfahrensregelung neben der Zuweisung der Koordinierungsfunktion beim BSI lässt sich aus der Aufgabennorm nicht ableiten. Auf unionsrechtlicher Ebene lässt sich Erwägungsgrund 59 der NIS-RL lediglich zu entnehmen, dass die Marktteilnehmer mit dem öffentlichen Sektor neben den verfahrensrechtlich strukturierten Verfahren einen informellen Austausch anstreben sollen.[391] Neben der vagen prozeduralen Vorgabe finden sich Konkretisierungen der Kooperation mit Privaten zur behördlichen Informations- und Wissensgenerierung.[392]

a) Vorschlag von technischen Sicherheitsstandards durch Branchenverbände

Für die Einhaltung materiell-rechtlicher Sicherheitspflichten der Betreiber kritischer Infrastrukturen ist der „Stand der Technik" maßgeblich (§ 8a Abs. 1 S. 2 BSIG). An welchen technischen Standards sich dieser Maßstab orientiert, ist ein die IT-Sicherheit perennierendes Problem.[393] Der mit dem IT-Sicherheitsgesetz eingeführte § 8a Abs. 2 BSIG intendiert Abhilfe zu schaffen. Branchenverbände können Standards vorschlagen, die vom BSI akzeptiert werden können. Der Umsetzungsplan Kritische Infrastrukturen (UP KRITIS) als öffentlich-private

---

[391] Zu den meist fehlenden verfahrensbezogenen Regelungen *Hofmann*, Externer Sachverstand im Verwaltungsverfahren, in: Spiecker gen. Döhmann/Collin (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, 2008, S. 176 (184 f.).

[392] Siehe auch BT-Drs. 18/5121, S. 13 für den Vorschlag, die Finanzierung regelmäßiger und unabhängiger Überprüfung sicherheitsrechtlicher Software (*bug bounty*) gesetzlich zu verankern. Zur Aufforderung, das „NIS-Wissen" durch Hacker-Wettbewerbe zu verbessern, Europäischer Wirtschafts- und Sozialausschuss, Stellungnahme zu NIS-RL, TEN/513, S. 3.

[393] Dazu *Schmidt-Preuß*, in: Kloepfer, Schutz kritischer Infrastrukturen, 2010, S. 67 ff.; *Spindler*, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, 2007, S. 26 ff.

Kooperation zwischen Betreibern kritischer Infrastrukturen stellt eine Plattform für die Zusammenarbeit bereit.[394] Normungsorganisationen wie das Deutsche Institut für Normung e.V. sollen ihre Fachkompetenz einbringen. Die Kooperation zur Ermittlung der Sicherheitsstandards, die dem Stand der Technik entsprechen müssen, soll die im „hohen Maße erforderliche Fachkompetenz und [den] Ressourcenaufwand" ausgleichen.[395]

b) Ausgestaltung des Verfahrens der Sicherheitsaudits, Prüfungen und Zertifizierungen

Die Betreiber kritischer Infrastrukturen müssen alle zwei Jahre die Einhaltung der Sicherheitsanforderungen durch geeignete Maßnahmen nachweisen. Das Gesetz lässt die Form des Nachweises weitgehend offen und nennt nur Sicherheitsaudits, Prüfungen oder Zertifizierungen (§ 8a Abs. 3 S. 2 BSIG). Im BSIG findet sich außer zur Zertifizierung (§ 2 Abs. 7 BSIG) keine Vorgabe dafür, wie und durch wen die Nachweisprüfungen vorgenommen werden können. Die Verordnungsermächtigung (§§ 10 Abs. 2, 8a Abs. 4 BSIG) kompensiert allerdings das gesetzliche Defizit.[396] Die Anforderungen an die Art und Weise der Durchführung, der auszustellenden Nachweise und der organisatorischen Anforderungen an die prüfende Stelle kann das BSI festlegen. Zuvor hat sie die Vertreter der betroffenen Infrastrukturbetreiber und Wirtschaftsverbände anzuhören (§ 8a Abs. 4 BSIG).

c) Einbindung bei der Erstellung von Sicherheitskatalogen

Im Telekommunikationssicherheitsrecht besteht mit § 109 Abs. 6 S. 2 TKG eine weitere prozedurale Ausgestaltung der Wissensgenerierung durch Unterstützung von Privaten. Bei der Erstellung des Katalogs von Sicherheitsanforderungen erhalten die Hersteller, die Verbände und die Betreiber öffentlicher Kommunikationsnetze sowie die Verbände der Anbieter öffentlich zugänglicher Telekommunikationsdienste Gelegenheit zur Stellungnahme.

d) Einkauf von Expertise und Informationen über Sicherheitslücken

Der Blick in die behördliche Praxis zeigt, dass über gesetzlich vorgesehene oder angedeutete Verfahren hinaus bei kommerziellen Sicherheitsdienstleistern eingekauft wird. So vergibt das BSI regelmäßig Aufträge zur Durchführung von

---

394 *UP KRITIS*, Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen, 2014.

395 Entwurf eines IT-Sicherheitsgesetzes vom 25.02.2015, BT-Drs. 18/4096, S. 34.

396 Kritisch *Roßnagel*, DVBl. 2015, 1206 (1209).

Studien, um Sicherheitsanalysen zu realisieren oder Leitfäden zu erstellen.[397] Bei der Verteilung auf Auftragspakete wird deutlich, dass das Ergebnis präjudiziert sein kann.[398] Als weiteres Beispiel kann der Ankauf von Informationen über Sicherheitslücken dienen. Das BSI hatte zum Schutz der Regierungsnetze einen Vertrag mit einem französischen IT-Dienstleister über den Ankauf von besonders sensiblen Zero-Day-Schwachstellen und ähnlichen Informationen zum präventiven Schutz vor Gefährdungen durch neu aufgedeckte Schwachstellen in weitverbreiteten Softwareprodukten geschlossen.[399]

e) Einsatz wissenschaftlicher Kommissionen

Für die Bundesnetzagentur hat der Gesetzgeber den Kontakt zur wissenschaftlichen Expertise institutionalisiert und verstetigt. Zur Vorbereitung ihrer Entscheidungen, aber auch zur Begutachtung von Regulierungsfragen, zu denen nach § 2 Abs. 2 Nr. 9 in Verbindung mit §§ 108 ff. TKG die öffentliche Sicherheit gehört, kann die Agentur wissenschaftliche Kommissionen einsetzen. Deren Mitglieder müssen nicht nur ökonomisch versiert sein, sondern auch über besondere technologische oder rechtliche Erfahrungen verfügen. Aus dem Wortlaut von § 125 Abs. 2 S. 1 TKG, nach dem die Bundesnetzagentur „fortlaufend wissenschaftliche Unterstützung" „erhält", ergibt sich, dass es auch die Pflicht der Behörde ist, die Unterstützung anzunehmen (und dass im Bundeshaushalt entsprechende Mittel bereitzustellen sind).[400]

2. Dysfunktion und Zulässigkeit der Informationsgenerierung über Private

Bei der Informations- und Wissensübernahme sind die strukturellen und bereichsspezifischen Probleme zu berücksichtigen, die bei der Mitwirkung verwaltungsexterner Dritten bestehen (a). Die unmittelbare Einbeziehung Privater bei der Informationsgenerierung ist bei der bestehenden Ausgestaltung grundsätzlich zulässig (b).

---

[397] BSI, www.bsi.bund.de, Publikationen, Studien.

[398] *Scherschel*, BSI-Audit: OpenSSL ohne große Schwachstellen, aber mit Entropie-Problemen, Heise vom 10.02.2016, online abrufbar, wo bemerkt wird, dass in der untersuchten OpenSSL-Bibliothek keine neuen Schwachstellen gefunden wurden, nach diesen aber auch nicht explizit gesucht wurde.

[399] Vgl. Antwort des Bundesministeriums des Innern auf schriftliche Frage von *Andrej Hunko*, MdB, vom November 2014, Arbeitsnummer 11/37, abrufbar unter: http://www.andrej-hunko.de%2Fstart%2Fdownload%2Fdoc_download%2F523-schriftliche-frage-zum-ankauf-von-zero-day-exploits-oder-aehnlichen-informationen-ueber-schwachstellen-in-softwareprodukten-durch-bsi-und-bnd.

[400] *Attendorn*/*Geppert*, in: Geppert/Schütz (Hrsg.), BeckTKG, 4. Aufl. 2013, § 125 Rn. 14.

a) Wissensübernahme von Privaten im Bereich Sicherheit

Für die Leitfrage des Beitrags des Informationsverwaltungsrechts zur Gewährleistung der Sicherheit drängt sich hinsichtlich der Übernahme verwaltungsexternen, sicherheitsbezogenen Wissens die Frage potenzieller Dysfunktionen auf.

Vom Standpunkt einer hohen Sicherheitserwartung ist die Anreicherung des behördlichen Wissens durch zusätzliches Fachwissen grundsätzlich wünschenswert. Die Anhörung Betroffener kann zur „Grundform behördlicher Informationsgewinnung" gezählt werden.[401] Die Behörde kann durch die Beteiligung Externer nicht nur fehlendes Tatsachenwissen einholen. Viemehr bietet die Anhörung den Stellungnehmenden die Gelegenheit zur aktiven Mitgestaltung der Entscheidungspraxis. Das Recht wird auf diese Weise nicht nur reflexiv, „sondern responsiv, im Sinne einer intentional vollzogenen Aktivierung der Umwelt, die zu Irritationen des Rechts anregt",[402] erzeugt.

Mit der Einbindung privater Interessenvertreter und der Übernahme externen Wissens, d. h. durch die Externalisierung der Wissensproduktion, wird die NIS-Verwaltung zwar entlastet. Zu einem gewissen Teil gibt sie damit aber Handlungskompetenz an private Akteure ab.[403] Das Beispiel der Beteiligung Privater und Externer an der Implementierung von Sicherheitsstandards macht deutlich, dass die Kooperationsstruktur im IT-Sicherheitsrecht erst im Begriff ist, sich als Modus innovativer Informationsgenerierung zu etablieren.

Ein Mechanismus etwa zur Entscheidung der Frage, welcher Standard bei konkurrierenden Vorschlägen gelten soll, ist in § 8a Abs. 2 BSIG nicht vorgesehen. Die Wissensperspektive darf hier aber nicht zu einer Verengung des Blicks auf die Interessenlage führen. Das fehlende Abstimmungsverfahren birgt die Gefahr ökonomischer Fehlanreize. Die Sicherheit erhöhte sich, wenn die Summe der vorgeschlagenen Maßnahmen als Standard definiert würde. Bestehende ökonomische Anreize können freilich dazu führen, dass der Minimalkonsens als branchenspezifischer Sicherheitsstandard etabliert wird und so durch die Einführung „schwacher" Branchenstandards im Wege der Übernahme verwaltungsexternen Wissens bei den Unternehmen letztlich potenzielle Investitionskosten und Compliance-Vorgaben vermieden werden. Die möglichen Informationsgewinne und damit einhergehenden behördlichen Erleichterungen dürfen, insbesondere bei der Etablierung von Sicherheitsstandards, gerade nicht dazu führen, dass den Eigen-

---

[401] *Gusy*, Die Informationsbeziehung zwischen Staat und Bürger, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. II, 2. Aufl. 2012, § 23 Rn. 69.

[402] *Augsberg*, Informationsverwaltungsrecht, 2014, S. 144.

[403] *Scholl*, Der private Sachverständige im Verwaltungsrecht, 2005, S. 112 f., 147 f.

erklärungen der angehörten Vertreter zu hohes Gewicht eingeräumt wird. Anders als in anderen technischen Sicherheitsbereichen besteht bei der IT-Sicherheit grundsätzlich noch kein dafür hinreichendes Vertrauensniveau.[404]

Bei der wissenschaftlichen Beratung muss bedacht werden, dass die Wissenschaft „die Zahl der Beurteilungsperspektiven und der diskutablen Entscheidungsfolgen vermehrt."[405] Denn die wissenschaftliche Systemrationalität ist stärker auf die Erweiterung der Menge von Wissen und Problemen, zum Beispiel durch die Entwicklung neuer diskutabler Fragestellungen, als auf Problemlösung und Erhöhung der Entscheidungskompetenz ausgerichtet.[406] Gerade für die aufgezeigten Verfahren der wissenschaftlichen Beratung sei das epistemische Problem zu beachten, dass wissenschaftliches Wissen nicht eine Reproduktion der Wirklichkeit darstelle, sondern eine „höchst voraussetzungsreiche, kontextabhängige Konstruktion".[407] Wissensübernahme ist folglich immer auch die Übernahme ausgewerteten Wissens. Die Leistungsfähigkeit der Wissensübernahme stößt dort an die Grenzen, wo die Amtsführung durch die „Internalisierung von Lobbyinteressen" gefährdet wird.[408]

In jedem Falle bedarf es auf Seiten der Verwaltung eines spezifischen Meta-Wissens, um die Koordinierungsfunktion einnehmen zu können und erfolgreich außeradministratives Wissen zu übernehmen.[409] Die Behörde muss in praktischer Hinsicht mit hoch qualifiziertem Personal ausgestattet sein, um die Expertise in der erforderlichen Breite zu entwickeln und eine qualitative Auswahl bezüglich der in Betracht kommenden externen Sachverständigen oder der Vergabe spezifischer amtsbezogener Aufgaben treffen zu können.

---

[404] Vgl. zu den sog. CE-Kennzeichen Verordnung (EG) Nr. 765/2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten.

[405] *Kropp*/*Wagner*, Wissensaustausch in Entscheidungsprozessen: Kommunikation an den Schnittstellen von Wissenschaft und Agrarpolitik, in: Mayntz et al. (Hrsg.), Wissensproduktion und Wissenstransfer, 2008, S. 173 (173).

[406] *Priddat*, Wissen, Recht und Organisation – Perspektiven der Politischen Ökonomie, in: Spiecker gen. Döhmann/Collin (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, 2008, S. 295 (297).

[407] *Augsberg*, Informationsverwaltungsrecht, 2014, S. 138 f.

[408] Vgl. *Groß*, Ressortforschung, Agenturen und Beiräte – zur notwendigen Pluralität der staatlichen Wissensinfrastruktur, in: Röh*l* (Hrsg.), Wissen – Zur kognitiven Dimension des Rechts, Die Verwaltung, Beiheft 9, 2010, S. 135 (140).

[409] Zur Meta-Governance als Modell zum Schutz kritischer Infrastrukturen *Dunn Cavelty*/*Suter*, International Journal of Critical Infrastructure Protection 2009, 179 (183); vgl. auch *Gaycken*, Öffentliches Fachgespräch zum Thema „IT-Sicherheit", A-Drs. 18(24)10, S. 11, der zudem auf das Erfordernis flexibler und industriefähiger Gehälter beim BSI hinweist.

b) Zur Zulässigkeit der Inanspruchnahme Privater bei der Informations- und Wissensgenerierung

Neben der Frage nach den dysfunktionalen Implikationen der Übernahme externen Wissens ist danach zu fragen, ob und wann in der Hinzuziehung Privater zur Informations- und Wissensgenerierung eine unzulässige Inanspruchnahme derselben zu sehen ist.[410] Dies könnte dann der Fall sein, wenn Aufgaben durch Private übernommen werden, für die öffentliche Stellen Anforderungen mit einer höheren Regelungsdichte einzuhalten haben und diese Anforderungen umgangen werden. Ein „Indienstnahmeverbot" wird etwa für die Datenerhebung in Informationsnetzwerken angenommen, in denen Private aktiv (personenbezogene) Daten erheben und an Behörden weiterleiten.[411] Da die NIS-Verwaltung sowohl bei der pflichtenbasierten als auch bei der auf Freiwilligkeit beruhenden Informationsgenerierung auf die Daten bei Privaten zurückgreift, insbesondere bei den Betreibern von Internetinfrastrukturen und -diensten, ist danach zu fragen, ob darin eine unzulässige Form der Indienstnahme von Privaten zu sehen ist.

Die Betreiber von Internetinfrastrukturen und -diensten, die zur Gewährleistung der Netz- und Informationssicherheit verpflichtet werden, sind grundsätzlich nicht als solche Beliehenen zu betrachten, für die spezifische, nur für öffentliche Stellen bestehenden Begrenzungen gelten würden. Sie sind bereits der Struktur nach nicht als Beliehene anzusehen.

Zwar ließe sich mit der Aufgabentheorie annehmen, dass Private schon Beliehene sind, wenn ihnen Staatsaufgaben übertragen sind.[412] Allerdings lässt sich damit eine Abgrenzung zur „Indienstnahme" von Privaten nur schwer vornehmen.[413] Bei der Qualifizierung des Handelns von Beliehenen sollte daher auf die Befugnis- und Rechtsstellung abgestellt werden. Es kommt damit darauf an, ob natürliche oder juristische Personen des Privatrechts Verwaltungsaufgaben erfüllen und ihnen die Befugnis verliehen wurde, diese Aufgaben selbstständig mit den Handlungsformen des öffentlichen Rechts, d. h. ggf. auch zwangsweise, im eigenen Namen wahrzunehmen.[414]

---

[410] Zur Indienstnahme Privater als wichtiges Bauelement im Informationsverwaltungsrecht *Schoch*, Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, in: VVDStRL 57 (1998), S. 158 (209); vgl. *Hoffmann-Riem*, DVBl, 1996, 225 (225 ff.).

[411] *Pitschas*, Datenschutz in Sicherheitspartnerschaften der Polizei mit privaten Sicherheitsdienstleistern, in: Stober (Hrsg.), Public-Private-Partnerships und Sicherheitspartnerschaften, 2000, S. 91 (107).

[412] Insbesondere *Steiner*, Öffentliche Verwaltung durch Private, 1975, S. 46 ff.

[413] *Von Heimburg,* Verwaltungsaufgaben und Private, 1982, S. 33.

[414] BVerwGE 35, 334 (337 ff.); 61, 222 (224 ff.); *Ehlers/Pünder* (Hrsg.), Allgemeines Verwaltungsrecht, 15. Aufl. 2015, § 10 Rn. 24; *Ehlers/Schneider*, in: Schoch/Schneider/Bier (Hrsg.), VwGO, 29. Aufl. 2015, § 40 Rn. 275.

Diese Voraussetzungen erfüllen die Betreiber und Anbieter nicht. Die ihnen auferlegten Pflichten zur Gewährleistung der Netz- und Informationssicherheit (§ 8a BSIG, § 109 TKG, § 13 Abs. 7 TMG bzw. Art. 32 DS-GVO) dienen vorrangig der Sicherheit ihrer eigenen Daten und Systeme und verleihen ihnen noch keine funktionale Behördeneigenschaft. Erst die Bearbeitung der über die Privaten generierten Daten durch die Bundesbehörden und durch die an der NIS-Kooperation angeschlossenen Einrichtungen findet auf der „Ebene der öffentlichen Sicherheit" statt. Einwenden ließe sich, dass gerade der Ausfall oder eine Störung der Informationstechnik in kritischen Infrastrukturen eine Gefahr für die öffentliche Sicherheit darstelle (arg. e. § 2 Abs. 10 S. 1 Nr. 2 BSIG). Hoheitliche Autorität und Gewalt dürfen die Betreiber und Anbieter aber für die ihnen aufgetragenen materiell-rechtlichen Sicherheitspflichten nicht ausüben. Die Telemediendiensteanbieter sind ausdrücklich nach § 7 Abs. 2 TMG nicht allgemein zur Überwachung fremder Informationen,[415] die sie übermitteln oder speichern, und zur Forschung nach Umständen, die auf eine rechtswidrige Tätigkeit hinweisen, verpflichtet. Die Befugnis zu Gefahrenabwehrmaßnahmen bei den Telekommunikationsanbietern und Netzbetreibern ist ebenfalls nicht allgemein, sondern auf den Zweck der Netz- und Informationssicherheit eingegrenzt. Damit kommen sie den Verpflichtungen aus § 109 TKG nach.[416] Die Wahrung der Interessen der öffentlichen Sicherheit bleibt ein Ziel des Regulierungsrechts (§ 2 Abs. 2 Nr. 9 TKG). Bis auf die Befugnis zur Erhebung von Daten und damit zum Eingriff in grundrechtlich geschützte Positionen werden ihnen keine hoheitlichen Rechte und Pflichten im Zusammenhang mit der Netz- und Informationssicherheit übertragen.

Vor allem weil für die Sicherheitsbehörden eigene Erhebungsgrundlagen gelten, kann konstatiert werden, dass die überwiegende Verantwortung für das „Kooperationsergebnis" beim Staat verbleibt.[417] Im Übrigen liegt es vor dem Hintergrund, dass die Infrastrukturbetreiber und Internetanbieter Private sind, in der

---

[415] Die Vorschrift setzt Art. 15 Abs. 1 RL 2000/31/EG (E-Commerce-Richtlinie) um, nach der Mitgliedstaaten Diensteanbietern keine allgemeinen Überwachungspflichten auferlegen.

[416] Vgl. *Greenawalt*, Die Indienstnahme privater Netzbetreiber bei der Telekommunikationsüberwachung in Deutschland, 2009, S. 229, der selbst für die Mitwirkung bei der Telekommunikationsüberwachung mangels Übertragung hoheitlicher Befugnisse nicht von einer Beleihung ausgeht.

[417] Zum Begriff *Ladeur*, Privatisierung öffentlicher Aufgaben und die Notwendigkeit der Entwicklung eines neuen Informationsverwaltungsrechts, in: Hoffmann-Riem/Schmidt-Aßmann (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, 2000, S. 225 ff. (231 f.); allgemein *Voßkuhle*, Beteiligung Privater an der Wahrnehmung öffentlicher Aufgaben und staatliche Verantwortung, in: VVDStRL 62 (2003), S. 266 (266 ff.).

Natur der Sache, dass die Wissensgenerierung nicht einseitig erfolgen kann, sondern in privat-öffentlichen Kommunikationsprozessen stattfinden muss.[418]

E. Besondere Grenzen der Informationsgenerierung

Im Vorangegangenen wurde untersucht, zu welchem Zweck welcher Akteur auf welcher rechtlichen Grundlage Informationen über die Sicherheit von Netzen und Informationssystemen generieren kann. Dabei hat sich gezeigt, dass für die Verwaltung sowohl eine Pflicht als auch ein Recht besteht, Informationen zu erheben. Die staatliche Informationsverantwortung endet jedoch dort, wo die Grenzen der Informationsgewinnung beginnen. Im Folgenden soll festgestellt werden, welche besonderen Grenzen für die Informations- und Wissensgenerierung bestehen. Nachfolgend wird daher untersucht, ob die Erfüllung und Durchsetzung der Meldepflicht davon abhängen, ob in ihnen ein Verstoß gegen das Verbot der Selbstbeschuldigung zu sehen ist (I.) und inwieweit das Datenschutzrecht (II.) und der Unternehmensdatenschutz (III.) die staatliche Informationsgenerierung im Bereich der IT-Sicherheit begrenzen.

I. Meldepflichten und Selbstbelastungsschutz

Die Rechtmäßigkeit von Meldepflichten im Bereich der IT-Sicherheit kann mit Blick auf den grundrechtlichen Schutz vor einer verpflichtenden Selbstbelastung bezweifelt werden. Die Vereinbarkeit einer Meldepflicht mit dem Verbot der Selbstbeschuldigung ist für die Effektivität dieses Instruments zur Generierung von Informationen über die Netz- und Informationssicherheit jedoch von wesentlicher Bedeutung. Der Konflikt tritt insbesondere dann auf, wenn der Grund einer Meldung eine sanktionsbewehrte Handlung oder ein sanktionsbewehrtes Unterlassen darstellt. Die Wissensproduktion könnte dadurch vereitelt werden, dass der Generierung von Informationen der Selbstbelastungsschutz entgegengehalten wird, wenn auf Grundlage von Informationspflichten wie Meldepflichten eine Beweislage geschaffen wird, die sich in einem Ermittlungsverfahren gegen den Meldepflichtigen verwenden ließe.

1. Verbot der Pflicht zur Selbstbelastung

Das Verbot der Pflicht zu Selbstbelastung, aus dem folgt, dass niemand verpflichtet ist, sich selbst und seine Angehörigen zu bezichtigen (*nemo tenetur se ipsum*

[418] *Röhl*, Ausgewählte Verwaltungsverfahren, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. II, 2. Aufl. 2012, § 30, Rn. 35.

accusare), ist unionsrechtlich nicht ausdrücklich normiert. Das in Art. 346 AEUV normierte Auskunftsverweigerungsrecht steht nur Mitgliedstaaten, nicht aber Privaten zu.[419] Der Selbstbelastungsschutz ist jedoch als Ausprägung des durch Art. 6 EMRK gewährten fairen Verfahrens als wesentliches Justizgrundrecht anerkannt.[420] Der EuGH hat zudem die Bedeutung von Verteidigungsgrundrechten, wie sie nunmehr in Art. 48 Abs. 2 GRCh verankert sind, betont.[421]

Das Bundesverfassungsgericht hat den Schutz vor einem Zwang zur Selbstbezichtigung als Teil des allgemeinen Persönlichkeitsrechts, Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG, anerkannt.[422] Der Einzelne solle vom Staat „grundsätzlich nicht in eine Konfliktlage gebracht werden, in der er sich selbst strafbarer Handlungen oder ähnlicher Verfehlungen bezichtigen muss […].“[423]

Problematisch ist insofern, dass die Nichteinhaltung der materiell-rechtlichen Sicherheitspflichten, die ursächlich für das meldepflichtige Ereignis sein kann, sanktionsbewehrt ist. Die Mitgliedstaaten sind nach Art. 21a RL 2009/140/EG bzw. Art. 21 NIS-RL dazu verpflichtet, Vorschriften über Sanktionen für Verstöße gegen die nach den Richtlinien erlassenen nationalen Bestimmungen zu erlassen. Für datenschutzrechtliche Meldepflichten folgt dies aus Art. 83 Abs. 1 und 84 Abs. 1 DS-GVO.[424] Das Spannungsverhältnis wird zudem durch das Zusammenfallen der Funktionen als Meldeadressat und zugleich als Ahnungsbehörde verschärft. Die Aufgabenbündelung präventiver und repressiver Aufgaben bei den zuständigen NIS-Behörden ist in Art. 15 Abs. 2 und 3 bzw. Art. 17 Abs. 2 und 3 NIS-RL angelegt. In Deutschland sind das BSI und die Bundesnetzagentur als Verwaltungsbehörden im Sinne des § 149 Abs. 3 TKG bzw. § 14 Abs. 3 BSIG im Verbindung mit § 36 Abs. 1 Nr. 1 OWiG für die Verfolgung und Ahndung der Ordnungswidrigkeiten zuständig. Auch Art. 83 Abs. 1 DS-GVO geht von der Verhängung von Geldbußen durch die Datenschutzaufsichtsbehörde selbst aus.

Zum Schutz vor der Selbstbezichtigung bestehen zum Teil einfachgesetzliche Regelungen. So besteht mit § 127 Abs. 8 TKG ein Auskunftsverweigerungsrecht und Verwertungsverbot. Das Auskunftsverweigerungsrecht bezieht sich jedoch auf geschäftliche Informationen, das qualifizierte Verwertungsverbot

---

[419] Siehe § 4 C. IV.

[420] EuGH, C-204/00 P, Rn. 64 ff.; C-374/87, Rn. 34; *Hatje*, in: Schwarze/Becker/ders./Schoo, EU-Kommentar, 3. Aufl. 2012, EUV, Art. 6, Rn. 31.

[421] EuGH, C-550/07 P, Rn. 92.

[422] BVerfGE 38, 105 (113 ff.); 55, 144 (150); 56, 37 (43); vgl. *Stohrer*, Informationspflichten Privater gegenüber dem Staat in Zeiten von Privatisierung, Liberalisierung und Deregulierung, 2007, S. 273.

[423] BVerfGE 95, 220 (241).

[424] Sanktionsbewehrt ist auch der Verstoß gegen die Meldepflicht. Es ist gemäß § 149 Abs. 1 Nr. 21a TKG, § 14 Abs. 1 Nr. 4 BSIG, § 43 Abs. 2 Nr. 7 BDSG ordnungswidrig, eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig zu machen.

auf Verfahren im steuerrechtlichen Zusammenhang. Auf Auskünfte und deren Verwendung im sicherheitsrechtlichen Zusammenhang bezieht sich die Norm nicht. Darüber hinaus besteht für die datenschutzrechtliche Meldepflicht ein ausdrückliches Verwendungsverbot in § 42a S. 6 BDSG, das über die Verweisung gleichfalls für die telemediendatenschutzrechtliche und telekommunikationsdatenschutzrechtliche Meldepflicht gilt (§ 15a TMG, § 109a Abs. 1 S. 5 TKG). Allerdings sieht die DS-GVO, anders als § 42a S. 6 BDSG, kein entsprechendes Verwendungsgebot vor. Ein besonderer Schutz fehlt auch in der NIS-Richtlinie und im BSIG.[425]

Damit ist fraglich, wie sich fehlende positiv ausgestaltete Schutzvorkehrungen auf die Erfüllung der Meldepflichten auswirken.

2. Kein absoluter Schutz vor Selbstbelastung

Die genauere Betrachtung der Rechtsprechung macht deutlich, dass der Schutz vor Selbstbelastung nicht absolut ist.

Der Europäische Gerichtshof hat in seiner Rechtsprechung zu kartellrechtlichen Verfahren ein Recht zur Verweigerung der Übermittlung von Informationen aufgrund des *nemo-tenetur*-Grundsatzes abgelehnt. Um die Wirksamkeit wettbewerbsrechtlicher Ermittlungsmaßnahmen zu gewährleisten, seien Unternehmen grundsätzlich verpflichtet, auch belastende Informationen zu übermitteln.[426] Einschränkungen sollten dagegen für die Offenlegung von Tatsachen gelten, für welche die Kommission beweispflichtig wäre.[427]

Auch im nationalen Recht gilt der *nemo-tenetur*-Grundsatz nicht absolut. Dem Selbstbelastungsschutz können im Einzelfall schutzwürdige Belange Dritter oder öffentliche Informationsinteressen gegenüberstehen. Das Bundesverfassungsgericht führte aus, dass die Selbstbezichtigungsfreiheit in Straf- oder ähnlichen Verfahren nicht in gleicher Weise für Personen gilt, „die aus besonderen Gründen rechtsgeschäftlich oder gesetzlich dazu verpflichtet sind, einem anderen oder einer Behörde die für diese notwendigen Informationen zu erteilen“.[428] Bei der Normierung uneingeschränkter Auskunftspflichten „kann“ der Gesetzgeber „berücksichtigen“, dass das Nachkommen der Informationspflicht nicht allein im staatlichen bzw. öffentlichen Interesse, sondern zugleich im In-

---

[425] Lediglich für personenbezogene Daten besteht gemäß § 8b Abs. 7 BSIG eine Beschränkung für die Verwendung in Straf- und Ordnungswidrigkeitsverfahren.

[426] EuGH, Rs. C-301/04, Rn. 41; C-374/87, Rn. 27 ff., 34.

[427] EuGH, C-374/87, Rn. 35; Kritisch mit Blick auf die Abgrenzungsschwierigkeiten *Jaeckel*, in: Grabitz/Hilf/Nettesheim (Hrsg.), AEUV/EUV, 57. Aufl. 2015, AEUV, Art. 337 Rn. 52.

[428] BVerfGE 56, 37 (45).

teresse eines geschädigten Dritten erfolgt.[429] Da Drittinteressen lediglich zu berücksichtigen sind, ist die Rechtfertigung einer uneingeschränkten Informationspflicht allein im öffentlichen Interesse nicht ausgeschlossen.[430]

Die Ausführungen des Gerichts lassen sich auf die sicherheitsrechtlichen Meldepflichten übertragen. Ein öffentliches Interesse besteht dabei insbesondere an Informationen über die Sicherheitslage kritischer Infrastrukturen, also solcher, die für die Gesellschaft von herausragender Bedeutung sind. Im Ergebnis dient die Erkenntnisgewinnung auch den Betreibern selbst, dritten Unternehmen und Nutzern.[431] Ein pauschales Verweigerungsrecht im Rahmen von Informationspflichten würde die effektive Erkenntnisgewinnung nicht nur erschweren, sondern ihr und ihrem Zweck zuwiderlaufen. Die Unternehmen sind strukturell bedingt die einzig verfügbaren Informationsquellen, sodass sie in einer verwaltungsrechtlichen Mitwirkungspflicht in der Sicherheitsgewährleistung stehen. Eine Selbstbezichtigung ist demnach grundrechtlich vertretbar, wenn sie zum Schutz kollidierender Interessen verhältnismäßig erscheint, insbesondere wenn dafür Sorge getragen wird, dass die Aussagen nicht die Voraussetzungen für eine strafgerichtliche Verurteilung oder die Verhängung vergleichbarer Sanktionen liefern.[432]

Für die Wirksamkeit von Melde- und anderen Informationspflichten ist ferner anzuführen, dass das Bundesverfassungsgericht den Schutz vor Selbstbelastung ausdrücklich dem Recht auf informationelle Selbstbestimmung zuordnet.[433] Schutz vor einem Zwang zur Selbstbezichtigung kommt juristischen Personen grundsätzlich nicht zu. Jedenfalls dort, wo der Grundrechtsschutz an Eigenschaften, Äußerungsformen oder Beziehungen anknüpft, die nur natürlichen Personen wesenseigen sind, kommt eine Erstreckung auf juristische Personen als bloßes Zweckgebilde der Rechtsordnung nicht in Betracht. Das ist umso eher der Fall, als der Grundrechtsschutz im Interesse der Menschenwürde gewahrt wird.[434] In diesem Sinne argumentiert auch der Europäische Gerichtshof im Rahmen einer vergleichenden Untersuchung der nationalen Rechtsordnungen.[435]

---

[429] BVerfGE 56, 37 (49 f.).

[430] *Berliner*, Informationsbefugnisse der Bundesnetzagentur im Telekommunikationsrecht, 2012, S. 249.

[431] Siehe zur Informationsdistribution an Private § 5.

[432] BVerfGE 56, 37 (50 ff.); vgl. *Di Fabio*, in: Maunz/Dürig (Hrsg.), GG, Band I, 75. Aufl. 2015, Art. 2 Rn. 188; vgl. aber Sondervotum *Heußner,* BVerfGE 56, 37 (52 ff.).

[433] BVerfGE 65, 1 (46); 96, 171 (181).

[434] BVerfGE 95, 220 (242); vgl. zur Diskussion *Dannecker*, ZStW 127 (2015), 370 (370 ff.); *Roßnagel*, A-Drs. 18(4)284 B, S. 10.

[435] EuGH, C-374/87, Rn. 29.

3. Ausgleich der betroffenen Interessen

Als verfassungsmäßiger Ausgleich der Interessen zum einen an der Generierung sicherheitsrelevanter Informationen und zum anderen an denen zum Schutz vor der Selbstbelastung kommen insbesondere dort, wo ausdrückliche Schutzvorkehrungen nicht getroffen sind, mehrere Lösungen in Betracht.

Zunächst kommt die Begründung eines ungeschriebenen Auskunftsverweigerungsrechts in Betracht.[436] Die Meldepflicht bestünde grundsätzlich fort, ausgenommen wären aber Meldungen über solche Sicherheitsvorfälle, mit denen sich die Meldepflichtigen selbst belasten würden.

Daneben könnten die betreffenden Sanktionsregelungen für unwirksam betrachtet und nicht mehr angewendet werden.[437] Die Meldepflicht bestünde ebenfalls fort, etwaige gemeldete Pflichtverletzungen wären aber nicht mehr bußgeldbewehrt.

Um einen absoluten Schutz für Straf- und ähnliche Verfahren zu gewährleisten, kommt schließlich die Annahme eines ungeschriebenen Verwertungsverbots in Betracht.[438] Die Meldepflicht stünde auch mit diesem Ansatz fort, doch könnten gemeldete Informationen nicht mehr in Straf- und Ordnungswidrigkeitenverfahren gegen den Meldepflichtigen verwendet werden.

Für die Annahme eines Auskunftsverweigerungsrechts spricht im Vergleich zu einem Beweisverwertungsverbot der stärkere Schutz, da insofern von vorneherein keine Meldeinhalte übermittelt werden müssten. Allerdings würde damit der Schutz der Interessen der Meldepflichtigen pauschal höher bewertet als das Interesse der Allgemeinheit und Dritter an den durch die Meldung generierten Informationen. Schutz vor Selbstbezichtigung würde ohne Rücksicht auf weitere schutzwürdige Belange gewährt.

Für die Nichtanwendung der Bußgeldregelungen spricht, dass das Spannungsverhältnis von Meldepflicht und Selbstbelastungsschutz grundsätzlich abgeschwächt wird. Dadurch wird allerdings noch kein rechtssicherer Schutz vor Belastungen in anderen Verfahren bewirkt. Außerdem hat sich der Gesetzgeber nach Kritik an möglichen Durchsetzungsdefiziten ausdrücklich für die Bußgeldregelungen entschieden.[439]

---

[436] Vgl. *Queck*, Die Geltung des nemo-tenetur-Grundsatzes zugunsten von Unternehmen, 2005, S. 44 ff.

[437] Im Rahmen von § 109 Abs. 5 TKG und mit Blick auf Art. 13a Abs. 3 RL 2009/140/EG *Eckhardt*, in: Geppert/Schütz (Hrsg.), BeckTKG, 4. Aufl. 2013, § 109, Rn. 79.

[438] Vgl. *Brink*, in: Wolff/Brink, BeckOK DSR, 19. Ed. 2017, Art. 33, Rn. 42.

[439] Vgl. die Ausführungen von *Roßnagel* im Rahmen der Expertenanhörung zum IT-Sicherheitsgesetz, A-Drs. 18(4)284 B, S. 10. Der später in Kraft getretene Art. 21 S. 2 NIS-RL fordert insbesondere „abschreckende" Sanktionen.

Vorzugswürdig ist die Annahme eines ungeschriebenen Verwertungsverbotes. Dieser Weg berücksichtigt, dass sich die Selbstbelastungsfreiheit letztlich nur auf das Risiko straf-, ordnungswidrigkeiten- oder berufsrechtlicher Verfolgung erstreckt.[440] Im Verwaltungsverfahren kommt somit der *nemo-tenetur*-Grundsatz zum Tragen, indem vor einer Selbstbezichtigung hinsichtlich der genannten Sanktionen ein Schutz besteht. Gesichert bleibt aber, dass Informationen über Sicherheitsvorfälle, deren Eintreten möglicherweise durch pflichtwidriges Verhalten verursacht oder gefördert wurde, generiert werden können. Auch sich an die Meldung anschließende Prüfungen und Anordnungen sind weiterhin zulässig. In diesem Sinne kann auch der Europäische Gerichtshof verstanden werden, der die pauschale Berufung auf den *nemo-tenetur*-Grundsatz ablehnt, gleichwohl aber die Bedeutung der Verteidigungsrechte betont.[441]

Wird vom Vorliegen eines Verwertungsverbotes ausgegangen, stellt sich die wichtige Folgefrage, ob dies auch die Unzulässigkeit der Verwertung solcher Beweismittel einschließt, die mittelbar aus dem ersten Beweismittel gewonnen werden. In der Rechtsprechung wird eine derartige Fernwirkung des Beweisverwertungsverbots regelmäßig mit der Begründung abgelehnt, dass ein solches mit Blick auf das Interesse an einer wirksamen Strafverfolgung nicht ohne Weiteres dazu führen könne, dass das gesamte Strafverfahren lahmgelegt werde und damit die Wahrheitserforschungspflicht des Gerichts, die zu den tragenden Grundsätzen des Strafverfahrens gehöre, ausgehöhlt werde.[442] In einer Gegenposition wird in Anlehnung an die amerikanische Fruit-of-the-Poisonous-Tree-Doktrin eine Fernwirkung bejaht, da andernfalls das Beweisverwertungsverbot leerliefe.[443] Dagegen wiederum kann aber vorgebracht werden, dass die Fernwirkung rechtsstaatlich nicht notwendig ist. Die genannte Doktrin dient vor allem der Disziplinierung der Ermittlungsbehörden, während die Einzelfallabwägung der Frage, ob eine Fernwirkung besteht, auch die Rechtsstaatlichkeit des Verfahrens sichern soll.[444] Für ein Verwertungsverbot mit Fernwirkung sprechen aus informationsverwaltungsrechtlicher Sicht drohende nachteilige Auswirkungen auf die Erfüllung der Meldepflichten. Erst mit einer Fernwirkung

---

[440] *Martini*, in: Paal/Pauly, DS-GVO, 2017, Art. 33, Rn. 27.

[441] EuGH, C-374/87, Rn. 34.

[442] Etwa BGHSt 34, 362 (364); BGHSt 35, 32 (34). Der EGMR hat in einem Fall der Verletzung des Folterverbots aus Art. 3 EMRK eine unbeschränkte Fernwirkung unabhängig von einer Abwägung zuerkannt. Die Frage, ob ein Verfahren insgesamt gegen den *fair-trial*-Grundsatz in Art. 6 EMRK verstößt, beantwortete das Gericht aber nicht, Urteil vom 01.06. 2010, Nr. 22978/05, Rn. 176.

[443] *Lesch*, in: Bockemühl (Hrsg.), Handbuch des Fachanwalts Strafrecht, 6. Aufl. 2015, S. 1291.

[444] Vgl. für die Annahme einer Fernwirkung unter Hinweis auf die jeweils im Einzelfall erforderliche Abwägung OLG Oldenburg, NStZ 1995, 412 (412).

kann der Meldepflichtige sicher sein, dass die Meldung nicht zum Anlass dafür genommen wird, weitere Beweismittel zu erlangen.

Zu betonen ist, dass das Vollzugsmodell von Informationspflicht und Sanktion ohnehin in Regelungskontexten auf Grenzen stößt, in denen der Staat durch strukturelle Informationsasymmetrien auf Kooperation und die Unternehmen auf Vertrauen angewiesen sind. Wegen der „Informationsabhängigkeit" bedarf es „schon aus strategischer Perspektive" einer stärkeren Betonung des kooperativen Elements im Rahmen der Informationsgenerierung seitens der Verwaltung.[445] Auch die Ermittlungsbefugnisse zur Überprüfung, ob bei einem meldepflichtigen Unternehmen überhaupt ein Sachverhalt vorliegt, der die Berufung auf die Selbstbelastungsfreiheit erlaubt, und die Sanktionsmöglichkeiten im Falle der nicht oder nicht vollständigen Meldung sollten primär vor dem Hintergrund betrachtet werden, dass die Verwaltung eine Handhabe haben muss, um Akzeptanz im Meldeverfahren dadurch zu erzeugen, dass ein Ausscheren eines meldepflichtigen Unternehmens durch die Unterlassung von Meldungen verhindert werden kann und bei kooperationswilligen, meldenden Unternehmen nicht die Vermutung hervorgerufen wird, dass ihre Kooperationsbereitschaft zu Wettbewerbsnachteilen führen kann. Bei der Durchsetzung der Meldepflichten haben die NIS-Behörden über das in § 47 OWiG verankerte Opportunitätsprinzip einen gewissen Spielraum bei der Verfolgung von Ordnungswidrigkeiten. Die Intention, ein funktionierendes, auf freiwilligen vollständigen Angaben beruhendes Meldewesens zu gewährleisten, erscheint nicht von vorneherein als unsachlich und kann durchaus hinsichtlich der Frage berücksichtigt werden, ob ein Ordnungswidrigkeitenverfahren eingestellt wird.

Zum Ausgleich der Konfliktsituation, die durch die Pflicht zur Meldung möglicherweise selbstbelastender Umstände bestehen kann, kommt nach allem vorzugsweise die Annahme eines Beweisverwertungsverbots in Betracht. Für die Fernwirkung des Verwertungsverbots kann ins Feld geführt werden, dass dadurch das Funktionieren des Meldewesens abgesichert wird. Zusätzlich sollte die NIS-Verwaltung zur Motivationssteigerung auch in der Ermittlung der Frage, ob eine selbstbelastende Situation überhaupt vorlag und ob eine Meldung hätte übermittelt werden müssen, die strukturelle Angewiesenheit der Verwaltung auf die Informationen berücksichtigen.

---

[445] *Berliner*, Informationsbefugnisse der Bundesnetzagentur im Telekommunikationsrecht, 2012, S. 261; vgl. *Wollenschläger*, Wissensgenerierung im Verfahren, 2009, S. 190 ff.; *Voßkuhle*, Beteiligung Privater an der Wahrnehmung öffentlicher Aufgaben und staatliche Verantwortung, in: VVDStRL 62 (2003), S. 266 (270 ff.); kritisch wohl *Taeger*, NJW 2014, 3759 (3759), der die fehlende Notifizierung von „Heartbleed", einer für die Internetsicherheit kritischen Sicherheitslücke, auf nur rudimentäre Kontrollen der Behörden und nicht ausgesprochene Sanktionen zurückzuführen scheint.

II. Besondere datenschutzrechtliche Grenzen der Informationsgenerierung

Grenzen der Informationsgenerierung können sich insbesondere aus dem Datenschutz ergeben. Verfassungsrechtliche Vorgaben folgen herkömmlich aus dem grundrechtlichen „Recht auf informationelle Selbstbestimmung", welches „die Befugnis des Einzelnen" gewährleistet, „grundsätzlich selbst über die Preisgabe und die Verwendung seiner persönlichen Daten zu bestimmen".[446] Unionsrechtlich ist der Schutz der eigenen personenbezogenen Daten in Art. 8 GRCh sowie in Art. 8 EMRK verankert. Im Zusammenhang mit Telekommunikationsdaten ist auch das in Art. 7 GRCh bzw. Art. 10 GG geschützte Fernmeldegeheimnis zu beachten.[447]

Vor allem in der deutschen Datenschutzdebatte wurde durch die Konstruktion von Staatsraison und Individualschutzinteressen als Gegensätze das Datenschutzrecht als Regulativ in Form eines „kalkulierten Nichtwissens" verstanden.[448] Datenschutzrecht kann insofern auch als Datenverkehrsrecht aufgefasst werden.[449]

Daraus ergeben sich Spannungen, weil der administrativen Informationsgenerierung der Verwaltung verfassungsrechtlich Grenzen gesetzt werden, die mit dem Gebot, „die für rationales und planvolles staatliches Handeln erforderlichen Informationen zu beschaffen"[450], in Einklang zu bringen sind.[451] Der vergleichende Blick auf den US-amerikanischen *Cybersecurity Information Sharing Act* (*CISA*)[452] zeigt, dass auch scheinbar nur technisch anmutende Gesetze zur Cybersicherheit erhebliche datenschutzrechtliche Implikationen aufweisen können. Im Kern verfolgt jenes Gesetz das Ziel, die umfangreiche Datenerhebung der Unternehmen sowie den weitreichenden Austausch der gesammelten Informationen, sog. Cyber Threat Indicators, mit Behörden zu ermöglichen. Aufgrund der überaus weitreichenden Definition der am Austausch teilnehmenden Behörden und der kaum ausgestalteten Datenschutzbestimmungen hat das Ge-

---

446 BVerfGE 65, 1 (43).

447 Dazu *Kujat*, Frühwarnsysteme zur Abwehr von Botnetzen, 2010, S. 20 f.

448 *Pitschas/Aulehner*, NJW 1989, 2353 (2354) mit Verweis auf *Simitis*, KritJ 1988, 32 (46).

449 Dazu *Podlech*, Individualdatenschutz – Systemdatenschutz, in: Brückner (Hrsg.), Beiträge zum Sozialrecht, Festgabe Grüner, 1982, S. 451 ff.; *Pitschas*, Die Verwaltung 33 (2000), 111 (122 ff., 127).

450 BVerfGE 65, 1 (2).

451 *Augsberg*, Informationsverwaltungsrecht, 2014, S. 44; vgl. *Schmidt-Aßmann*, Verwaltungsrecht in der Informationsgesellschaft: Perspektiven der Systembildung, in: Hoffmann-Riem/ders. (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, 2000, S. 405 (425).

452 *Cybersecurity Information Sharing Act* von 2015 (*CISA*), H.R. 2029 – Consolidated Appropriations Act, 2016, Division N.

setz massive Kritik erfahren.[453] Gleichermaßen wurde hinsichtlich der NIS-Richtlinie und des IT-Sicherheitsgesetzes im Gesetzgebungsverfahren bedeutende Kritik geübt. Es ergebe sich aus Datenschutzperspektive bei Einrichtung der für NIS zuständigen, nationalen Zentralbehörden „die Gefahr eines zentralen Datensilos mit entsprechend großem Missbrauchspotential".[454] Das IT-Sicherheitsgesetz genüge den datenschutzrechtlichen Anforderungen nicht.[455]

Zu untersuchen ist also, inwiefern sich für die behördliche Informationsgenerierung aus dem Datenschutz Grenzen ergeben. Dazu ist darauf einzugehen, in welchem Verhältnis die Gewährleistung der Sicherheit von Netzen und Informationssystemen zum Datenschutzrecht steht (1.). Sodann ist zu fragen, inwieweit die Betreiber und Anbieter, bei denen personenbeziehbare Daten generiert werden, ihrerseits entsprechende Daten verarbeiten dürfen (2.). Sodann sind die besonderen für die NIS-Administration aus dem Datenschutz resultierenden Grenzen aufzuzeigen (3.).

1. Datenschutzrechtliche Relevanz der Netz- und Informationssicherheit

Netz- und Informationssicherheit kann zum Datenschutz in einem Spannungsverhältnis stehen,[456] obwohl die Gewährleistung der Netz- und Informationssicherheit nicht nur den Schutzzielen Verfügbarkeit, Vertraulichkeit und Integrität von Daten, sondern letztlich auch dem Datenschutz als Schutz personenbezogener Daten dient. Grundsätzlich beinhaltet die Netz- und Informationssicherheit,

---

[453] *Levine*, Professors' Letter in Opposition to The ‚Cybersecurity Information Sharing Act' (S. 754) vom 26.10.2015, online abrufbar; vgl. auch *Wolff*, Cybersecurity Legislation Is Too Short-Sighted, Slate vom 29.04.2015: „If anything, the primary criticism leveled at them – that the policies allow the sharing of too much data with too many people for too wide a variety of purposes – suggests we need to pare down, rather than expand, the types of information that it covers and their audience and uses."

[454] Siehe *Engeler/Jensen/Obersteller/Deibler/Hansen*, Monitoring durch Informationsfusion und Klassifikation zur Anomalieerkennung, 2014, S. 91; vgl. allgemein zu Risiken informationsverarbeitender Systeme *Steinmüller/Ermer/Schimmel*, Verallgemeinerung für riskante Systeme, in: dies. (Hrsg.), Datenschutz bei riskanten Systemen, 1978, S. 193.

[455] *Hornung*, NJW 2015, 3334 (3337 f.); *Lurz/Scheben/Dolle*, BB 2015, 2755 (2759 ff.); *Spindler*, CR 2016, 297 (301 f.); *Roßnagel*, DVBl. 1216 (1212); zur Kritik im Gesetzgebungsverfahren insbesondere Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) vom 18. und 19.03.2015, IT-Sicherheitsgesetz nicht ohne Datenschutz!, abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/EntschliessungssammlungDSBundLaender/89DSK_ITSicherheitsgesetzNichtOhneDatenschutz.html;jsessionid=609AD2C5C845F6EC00DF5400942EAA53.1_cid319?nn=5217016; Stellungnahme zum Entwurf eines IT-Sicherheitsgesetz des *Unabhängigen Landeszentrums für Datenschutz (ULD) Schleswig Holstein* vom 13.02.2015, online abrufbar.

[456] Vgl. Bericht des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, SH-LT Drs. 18/2730, S. 18.

personenbezogene Daten vor Zugriffen zu schützen. Allerdings kann es für die IT-Sicherheit erforderlich sein, zum Erreichen dieses Zwecks in die Schutzgüter des Datenschutzes einzugreifen.

Datenschutzrechtliche Belange können durch die Datenerhebung der untersuchten Wissens- und Informationsakteure berührt sein (a). Voraussetzung für die Anwendung des Datenschutzrechts ist, dass es sich bei den verarbeiteten Daten um personenbezogene Daten handelt (b).

a) Datensicherheit im Verhältnis zum Datenschutz

Nach den IT-sicherheitsbezogenen Vorschriften müssen Sicherheitsvorkehrungen und -maßnahmen den „Stand der Technik" berücksichtigen oder sollen diesen einhalten.[457]

Schutzmaßnahmen zum Zweck der Sicherheitsgewährleistung nach dem Stand der Technik können es erforderlich machen, dass Daten von Nutzern von Infrastrukturen oder Diensten erhoben, gespeichert, übermittelt und ausgewertet werden. Störungen, Fehlfunktionen und Angriffe auf IT-Systeme können häufig nur durch die automatisierte Analyse von Protokolldaten erkannt werden.[458] Die Effektivität von IT-Sicherheitsmaßnahmen kann umso höher sein, je tiefgreifender sie vorgenommen werden können. Die Abwehr beispielsweise von Botnetzen kann mittels weniger invasiver Maßnahmen wie Schwarzlisten von IP-Adressen, aber auch mittels effektiverer Maßnahmen, welche die invasivere Erhebung und Auswertung von Inhaltsdaten (sog. Deep Packet Inspection) voraussetzen, erfolgen. Technisch ist es möglich, Systeme, Komponenten und Prozesse wie Firewalls, Spamfilter und Intrusion Detection Systems etc. einzusetzen, die für ihre Funktion auf die Protokollierung von Nutzerdaten angewiesen sind, um effektiv vor äußeren Angriffen von Dritten, etwa durch SPAM, Botnetze, Viren, Würmer bzw. Trojaner und Phishing, DDoS-Attacken und vor anderen Klassen von Bedrohungen, zu schützen.[459] Als für besonders wichtig für die Erkennung und Abwehr

---

[457] Vgl. § 8a Abs. 1 S. 2 BSIG bzw. Art. 14 Abs. 1 S. 2 bzw. Art. 16 Abs. 1 S. 2 NIS-RL, § 109 Abs. 2 S. 3 TKG, § 13 Abs. 7 S. 2 TMG bzw. Art. 32 Abs. 1 S. 1 DS-GVO.

[458] BT-Drs. 16/11967, S. 12. Dort auch zur Definition von Protokolldaten: „[Diese] sind in erster Linie die Steuerdaten, die bei jedem Datenpaket mit übertragen werden, um die Kommunikation zwischen Sender und Empfänger technisch zu gewährleisten. Hinzu treten die Daten, die zwar nicht mit übertragen, aber im Rahmen der Protokollierung von dem Server im Übertragungsprotokoll miterfasst werden, insbesondere Datum und Uhrzeit des Protokolleintrags und ggf. Absender und Weiterleitungskennungen."

[459] Vgl. Erklärung der Bundesregierung 2007 zur Notwendigkeit der Protokollierung von IT-Nutzerdaten zum Zwecke der IT-Sicherheit: „Die Speicherung ist insbesondere aus Sicherheitsgründen notwendig: […] Dazu gehört zwingend die Speicherung der IP-Adressen, um Angriffsmuster zu erkennen und Gegenmaßnahmen (z. B. durch die Speicherung bestimmter,

von IT-Angriffen erachtet werden die Kopfdaten (Header) der gängigen Kommunikationsprotokolle (IP, ICMP, TCP, UDP, DNS, http und SMTP).[460] Verschiedene Einzeldaten wie IP-Adressen, URLs, gescannte Portnummern, Routing-Tabellen in Border Gateway Protocol-Routern, Datum, Uhrzeit sind für sich genommen zunächst zwar bloß technische Angaben. Dennoch können diese Daten zugleich auf Nutzer und damit auf natürliche Personen verweisen.[461] Insbesondere wenn (Meta-)Daten aggregiert und verknüpft werden (etwa die IP-Adresse mit der MAC-Adresse), könnten Erkenntnisse über Personen abgeleitet werden.

b) Personenbeziehbarkeit von Maschinendaten

Ob die zu Zwecken der Sicherheit verarbeiteten Maschinendaten als personenbezogene Daten zu qualifizieren sind, ist allerdings im Einzelfall umstritten. Die über die Anwendbarkeit des Datenschutzrechts bestimmende Frage nach dem Personenbezug ist aufgrund des Einflusses und der Bedeutung der Antwort die „Gretchenfrage des Datenschutzes".[462] Bis heute ist ungeklärt, wie der Begriff der Personanbeziehbarkeit auszufüllen ist. Weder auf internationaler[463], auf europäischer[464] noch auf deutscher Ebene[465] besteht ein einheitliches Verständnis des Tatbestandsmerkmals „personenbezogene Daten". Für die Rechtmäßigkeit der Datenverarbeitung zu Zwecken der Netz- und Informationssicherheit resultiert daraus eine rechtliche Unsicherheit.[466]

---

für den Angriff genutzter IP-Adressen) einleiten zu können. Ohne diese Daten ist eine Abwendung der kontinuierlichen Angriffe nicht möglich.", BT-Drs. 16/6938, Antwort auf Frage 11.

[460] *Buchberger*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, BSIG, § 3 Rn. 10.

[461] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Stellungnahme zum IT-Sicherheitsgesetz, 20.10.2014, S. 2.

[462] Vgl. *Haase*, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 3; *von Lewinski*, Die Matrix des Datenschutzes, 2014, S. 1; *Saeltzer*, DuD 2004, 218 (218 f.).

[463] *Schwartz*/*Solove*, Cal. Law Rev. 2014, Vol. 102, 877 (900).

[464] *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", angenommen am 20. 06.2007, WP 136, S. 3.

[465] Siehe *Gerlach*, CR 2013, 478 ff.; *Brink*/*Eckhardt*, ZD 2015, 205 ff.; *Pohle*/*Nink*, MMR 2015, 563 ff.

[466] In einer Studie hat die ENISA bereits darauf hingewiesen, die Rahmenbedingungen für CERTs zu verbessern. Dazu wurde unter anderem die Empfehlung ausgesprochen „B.1 Address legal uncertainty concerning requests, B.2 Designate national/governmental CERTs on a specific regulatory footing, B.5 Articulate why CERTs need to process personal data to Article 29 Working Party", siehe ENISA, A flair for sharing – encouraging information exchange between CERTs, 2011, S. 67 ff.; ferner *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*, Stellungnahme zum IT-Sicherheitsgesetz, 13.02.2015, das irritiert über die Aussage in der Begründung eines Gesetzesentwurfes zum IT-Sicherheitsgesetz war, die nach § 8b BSIG-E übermittelnden Daten seien „üblicherweise rein technischer Natur", BR-

Exemplifizieren lässt sich das Spannungsfeld von Sicherheitsgewährleistung und Datenschutz am Beispiel von IP-Adressen, da diese typischerweise zur Bearbeitung von Missbräuchen von IT-Infrastruktur (Abuse Handling) und Netzwerk-Monitoring benötigt werden (aa).[467] Die IP-Adresse steht stellvertretend für Einzeldaten, die grundsätzlich neben anderen Datensätzen bei Maßnahmen zur Gewährleistung der Netz- und Informationssicherheit von den Infrastrukturbetreibern, Diensteanbietern, aber auch den öffentlichen CSIRTs und Behörden erhoben werden könnten (bb).[468]

aa) Beispiel der IP-Adresse

Die das Internet bildenden Server und Computer werden durch standardisierte Datenaustauschprotokolle[469] zu einem Netzwerk verbunden. Der Transport der Bitströme erfolgt gemäß dem Internet Protocol (IP).[470] Die IP-Adresse dient der Identifizierung aller am Internet angeschlossenen Rechner[471] und kann als „Telefonnummer" eines Computers verstanden werden.[472] Zu unterscheiden sind statische und dynamische IP-Adressen. Statische IP-Adressen sind bestimmten Netzwerkschnittstellen fest zugewiesen. Dynamische IP-Adressen werden bei jeder neuen Netzwerkverbindungsaufnahme neu zugewiesen. Erstere werden

---

Drs. 643/14. Dabei handelte es sich um eine relativierte Aussage; der Vorgängerentwurf ging davon aus, dass „üblicherweise kein Personenbezug" bestehe. Diese Formulierung ist nicht in die abschließende Gesetzesbegründung übernommen worden. Einen „rechtlichen Graubereich" identifizierend *Einzinger*/*Skopik*/*Fiedler*, DuD 2015, 723 (724).

[467] Technische Ausführungen zum Abuse-Verfahren der Deutschen Telekom finden sich bei OLG Frankfurt a. M., ZUM-RD 2013, 596 (605); vgl. zu diesem Verfahren auch OLG Frankfurt a. M., ZUM-RD 2011, 173.

[468] *Engeler/Jensen/Obersteller/Deibler/Hansen*, Monitoring durch Informationsfusion und Klassifikation zur Anomalieerkennung, 2014, S. 23 nennt als potenziell personenbezogene Daten je nach Abwehrmechanismus (Botnetzabwehr, Routing-Anomalien, Netzwerk-Monitoring) noch E-Mail-Header, Zeitpunkte der Versendung und Markierung als Spam, URLs, IP-Bereich in Routing-Tabellen autonomer Systeme, AS-Nummern, IP-Adressen, die durch Traceroutes adressiert werden, Zeitpunkte der Ereignisse, IP-Adressen von unternehmensinternen und externen Rechnern, Portnummern, Daten aus dem genutzten Protokoll. Zu nennen sind außerdem Cookies, Unternehmenskennziffern und besondere Webtracking-Funktionen.

[469] Eine Legaldefinition von Protokolldaten findet sich in § 2 Abs. 8 BSIG, die ein Verständnis auch über das BSIG hinaus erlaubt. Darunter sind Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung zu verstehen, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind.

[470] RFC 791 (Internet Protocol).

[471] RFC 2050 (Internet Registry IP Allocation Guidelines).

[472] Siehe auch die Ausführungen in BVerfGE 130, 151 (162 ff.).

häufig von wenigen Geschäftskunden eingesetzt, Letztere häufig von Access-Providern genutzt, um Internetverbindungen über Wählleitungen anzubieten.

Die Funktionen von IP-Adressen lassen sich verwenden, um bestimmte internetbasierte IT-Sicherheitsvorfälle zu detektieren, abzuwehren oder zu verfolgen. Da die IP-Adresse die Identifizierung einzelner Rechner ermöglicht, können so auch von diesen Rechnern ausgehende Angriffe erfasst werden. Sie wird beispielsweise gebraucht, um Angriffe von Botnetzen abzuwehren. Im Kontext der IT-Sicherheit wird unter einem Botnetz ein Verbund von infizierten (Bot-) Rechnern verstanden, die miteinander kommunizieren und zumeist über einen zentralen Server kontrolliert und ferngesteuert werden.[473] Hauptsächlich werden diese zu Distributed-Denial-of-Service-(DdoS-)Angriffen (auf Internetdiensteanbieter angewendet, um durch das Versenden großer Datenmengen die attackierten Server mit dem Ziel der Sabotage zu überlasten. Darüber hinaus gibt es eine Vielzahl weiterer Angriffsmodi und Ziele.[474] Die IP-Adresse kann in den Varianten der Botnetzangriffe zur Identifikation dienen und wird in Anomalieerkennungssystemen eingesetzt, bei denen Kennzahlen des normalen Datenverkehrs aufgezeichnet werden, um Abweichungen als mögliche Angriffe einzustufen. Um in der Rückschau Anomalien erkennen zu können, werden IP-Adressen über einen gewissen Zeitraum gesichert und ausgewertet.[475]

bb) Personenbeziehbarkeit von IP-Adressen

Die Einordnung der IP-Adresse in datenschutzrechtliche Kategorien hat in der Literatur und Rechtsprechung in diversen Konstellationen zu einer umfangreichen Diskussion geführt.[476] Im Kern geht es um die Frage, ob IP-Adressen personenbezogene Daten im Sinne von Art. 2 lit. a und Art. 7 lit. f der RL 95/46/EG bzw. von Art. 4 Abs. 1 DS-GVO und § 3 Abs. 1 BDSG sind.

Personenbezogene Daten sind gemäß Art. 4 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologi-

---

[473] *Eckert*, IT-Sicherheit, 2000, S. 72 f.

[474] Dazu Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2016, 2016, S. 18 ff.

[475] Zur Zulässigkeit der siebentägigen Speicherung dynamischer IP-Adressen zur Störungserkennung auf Grundlage von § 100 TKG siehe BGH, NJW 2014, 2500.

[476] Siehe Nachweise bei *Haase*, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 373 (Fn. 202 und 203); *Schmidt-Holtmann*, Der Schutz der IP-Adresse im deutschen und europäischen Datenschutzrecht, 2014, passim.

schen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Aus IP-Adressdaten lässt sich grundsätzlich unmittelbar noch kein Rückschluss auf die Identität der eine IP-Adresse nutzenden Person schließen.[477] Eine IP-Adresse, zumal wenn sie dynamisch vergeben wird, bezeichnet damit keine Einzelangabe über eine „bestimmte Person". Klärungsbedürftig ist damit, ob eine natürliche Person aus einer IP-Adresse „identifizierbar" ist.

Zunächst ist zwischen statischen und dynamischen IP-Adressen zu unterscheiden. Die festen, statischen IP-Adressen geben Aufschluss über benutzte Rechner und den Zeitpunkt der Nutzung und können als Einzelangaben über Personen eingeordnet werden.[478] Mittlerweile ist weitgehend anerkannt, dass bei statische IP-Adressen eine Person zuordenbar oder bestimmbar ist, weil die Identität des jeweiligen Nutzers über mehrere Zwischenschritte mit weiteren Angaben objektiv und ohne unverhältnismäßigen Aufwand über die Internet Service Provider ermittelbar ist.[479]

Rechtsunsicherheit besteht daher dagegen vor allem bezüglich der dynamischen IP-Adresse. Die Einzelangaben aus der IP-Adresse, etwa über bestimmte Zeitpunkte und Serverabrufe, erlauben für sich noch keinen Schluss auf die Identität des Nutzers. Umstritten ist daher bei der Bestimmbarkeit, ob ein objektiver oder ein relativer Maßstab anzulegen ist.

Nach objektiver Auffassung ist der Personenbezug dann gegeben, wenn ein Dritter in der Lage ist, die Identität festzustellen. Auf die individuellen Verhältnisse der datenverantwortlichen Stelle komme es aufgrund der mannigfaltigen Möglichkeiten der Datenzusammenführung und Korrelationstechniken[480] und der fehlenden Unterscheidbarkeit von statischen und dynamischen IP-Adressen (Infizierung) nicht an.[481] Der subjektive Ansatz geht davon aus, dass von einem Personenbezug dann keine Rede sein kann, wenn für die verantwortliche Stelle die Bestimmung des Betroffenen mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft verbunden ist und so das Risiko einer Identifizie-

---

[477] Vgl. Erwägungsgrund 30 DS-GVO.

[478] Vgl. *Dammann*, in: Simitis (Hrsg.), BDSG, 8. Aufl. 2014, § 3 Rn. 10.

[479] Zur Zuordenbarkeit BGH, Urteil v. 13.01.2011, Az. III ZR 146/10. Vgl. auch BGH, Urteil v. 03.07.2014, Az. III ZR 391/13.; *Weichert*, in: Däubler/Klebe/Wedde/ders. (Hrsg.), BDSG, 5. Aufl. 2016, § 3 Rn. 13; differenzierend nach der Art der Registrierung bei der RIPE NCC-Datenbank oder bei einem Zugangsanbieter *Gerlach*, CR 2013, 478 (481).

[480] Zum Personenbezug im Zusammenhang mit Datenkorrelation und -fusion *Engeler/Jensen/Obersteller/Deibler/Hansen*, Monitoring durch Informationsfusion und Klassifikation zur Anomalieerkennung, 2014, S. 22; kritisch *Krüger/Maucher*, MMR 2011, 433 ff.

[481] *Schaar*, Datenschutz im Internet, 2002, Kap. 3 Rn. 153, 174 f.; *Heidrich/Wegener*, DuD 2010, 172 (172); *Pahlen-Brandt*, K&R 2008, 286 (289): *Karg*, MMR 2011, 345 (346).

rung praktisch vernachlässigt werden kann.[482] Diese Ansicht zieht eine Erwägung in der Datenschutzrichtlinie heran, nach der bei der Beurteilung der Bestimmbarkeit alle Mittel berücksichtigt werden sollten, die „vernünftigerweise" eingesetzt werden könnten, um die betreffende Person zu bestimmen.[483] Aus letzterer Ansicht folgt, dass dieselben Daten für unterschiedliche Stellen einen Personenbezug aufweisen können oder auch nicht. Aufgrund je unterschiedlicher Erlaubnistatbestände, Kenntnisse, Mittel und Möglichkeiten können Daten für einen Zugangsanbieter personenbezogen sein,[484] nicht aber etwa für einen Anbieter von Telemediendiensten.[485]

Die Datenschutzaufsichtsbehörden tendieren dazu, IP-Adressen grundsätzlich als personenbeziehbar zu behandeln. Dies sei bei Internetzugangsanbietern und Diensteanbietern der Fall, die Protokolle bzw. Logfiles speichern und die Internetnutzer identifizieren könnten. Der Personenbezug sei umso mehr gegeben, je eher der Zweck der Verarbeitung in der Identifizierung von Personen liege.[486] Der europäische Datenschutzbeauftragte geht in seiner Stellungnahme zum Entwurf der NIS-RL ausdrücklich davon aus, dass die zwischen den NIS-Behörden ausgetauschten IP-Adressen, die indirekt auf Angreifer oder von diesen betroffene Einzelne verweisen, personenbezogene Daten darstellen.[487]

Im Ergebnis bemisst sich die Bestimmbarkeit des Personenbezugs durch die verantwortliche Stelle, der die Daten vorliegen, nach dem Zusatzwissen, den Möglichkeiten, dem Aufwand an Zeit, den Kosten sowie der Arbeitskraft, die zur Identifizierung einer verantwortlichen Stelle in der entsprechenden Situa-

---

[482] *Dammann*, in: Simitis (Hrsg.), BDSG, 8. Aufl. 2014, § 3 Rn. 23, 196; *Mantz*, ZD 2013, 625 ff.

[483] RL 96/46/EG, Erwägungsgrund 26. Siehe auch Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", 20.06.2007, WP 136, S. 15.

[484] Vgl. EuGH, RS- C-70/10, Rn. 51.

[485] *Härting*, Internetrecht, 5. Aufl. 2014, Kap. B Rn. 276; *Specht/Müller-Riemenschneider*, ZD 2014, 71 ff.

[486] *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", angenommen am 20.06.2007, WP 136, S. 21; vgl. *Düsseldorfer Kreis*, Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 26./27.11.2009, 2009, S. 2.

[487] *European Data Protection Supervisor*, Opinion on the Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy on a ‚Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace', and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union, 2013, Rn. 58. Der Europäische Datenschutzbeauftragte wird nach Art. 28 Abs. 2 VO (EG) Nr. 1/2001 konsultiert, wenn ein europäisches Gesetzgebungsverfahren die Datenschutzgrundrechte betrifft.

tion zur Verfügung stehen bzw. von ihr erbracht werden müssen.[488] Die Bestimmbarkeit lässt sich – vorbehaltlich der Bewertung im Einzelfall – nach allgemeinen Kriterien bemessen.

Die Datenschutzrichtlinie 95/46/EG hatte im Erwägungsgrund 23 die heranziehbaren Mittel und Stellen konkretisiert. Dessen Satz 2 besagt, dass bei der Entscheidung, ob eine Person bestimmbar ist, alle Mittel berücksichtigt werden sollten, die „vernünftigerweise" entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betroffene Person zu bestimmen. Tendenziell wird damit ein objektiver Ansatz zur Bestimmung verfolgt. Erwägungsgrund 30 der DS-GVO erweitert den Kreis der Mittel. Es sollten „alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden". Bei der Bestimmung dieser Wahrscheinlichkeit kann nach teilweise vertretener Auffassung die Überlegung berücksichtigt werden, dass das Datenschutzrecht auch als Vorfeldschutz fungiert. Für den Anwendungsbereich seien Gefährdungspotenziale unabhängig davon mit einzubeziehen, ob die Gefahr später eintritt oder in der Vergangenheit eingetreten ist.[489] In dieser Lesart kann die frühe Feststellung des Bundesverfassungsgerichts verstanden werden, dass es unter den Bedingungen der automatischen Datenverarbeitung kein „belangloses Datum mehr [gibt]".[490] Bei einer Gefährdungsprognose wäre zu beachten, dass das BSI die Polizeien, die Strafverfolgungsbehörden und die Nachrichtendienste nach § 3 Abs. 1 S. 2 Nr. 13 BSIG unterstützt. Dabei kann es zu einem Datenaustausch kommen. Ein solcher Datenaustausch mit Landes- und Bundesbehörden findet hinsichtlich der kritischen Infrastrukturen notwendigerweise statt (§ 8b Abs. 2 Nr. 4 BSIG). Dieser kann wiederum an Eingriffsgrundlagen (allgemein §§ 161, 163 StPO, ggf. in Verbindung mit §§ 112, 113 TKG, § 109 Abs. 9 UrhG) geknüpft sein. Die Prognose darf aber nicht auf die Erwartung rechtskonformen Verhaltens reduziert werden, sondern hat auch mögliche Begehrlichkeiten in Bezug auf Informationen in die Wertung mit einzubeziehen.[491]

Mit den Wertungen der DS-GVO wird der sachliche Anwendungsbereich des Datenschutzes sogar tendenziell erweitert. Nach Art. 4 Nr. 1 DS-GVO wird eine Person als identifizierbar angesehen, „die direkt oder indirekt identifiziert werden kann, insbesondere mittels Zuordnung […] zu einer Kennung, […], wie eine Kennnummer, […], zu einer Online-Kennung oder zu einem oder mehreren be-

---

[488] *Haase*, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 319; für die pauschale Behandlung von Daten, die durch Netzverhalten anfallen, *Giesen*, RDV 2010, 266 (269).

[489] *Haase*, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 151.

[490] BVerfGE 65, 1 (45).

[491] *Haase*, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 394.

sonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Personen sind", identifiziert werden kann. Zu den Online-Kennungen zählt Erwägungsgrund 30 der DS-GVO neben Cookie-Kennungen oder Protokollen Maschinendaten wie IP-Adressen.[492] Die Zuordnung „kann Spuren hinterlassen, die insbesondere in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können", natürliche Personen zu identifizieren. Es kommt dem Wortlaut nach nicht ausdrücklich darauf an, ob die verantwortliche Stelle selbst die betroffene Person identifizieren kann, sondern es sind auch die Möglichkeiten Dritter zu berücksichtigen.

In einem vom Europäischen Gerichtshof zu entscheidenden Vorabentscheidungsersuchen ging es um die Frage, ob Daten (dort IP-Adressen) personenbezogen sind, wenn zwar nicht die speichernde Stelle, aber ein Dritter (dort der Access-Provider) den Personenbezug herstellen kann.[493] Der Europäische Gerichtshof entschied, dass eine dynamische Internetprotokoll-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine Website, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, für den Anbieter ein personenbezogenes Datum darstellt, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen.[494] Bei privaten Diensteanbietern genügt als rechtliches Mittel grundsätzlich die gemäß § 406e Abs. 1 S. 1 StPO mögliche Akteneinsicht, über die die vom Dritten an die Staatsanwaltschaft preisgegebene Identität des Täters herausgefunden gefunden werden kann.[495] In seiner Abgrenzung der Vorlagefrage hat der Generalstaatsanwalt jedoch in seinen Schlussanträgen klargestellt, dass es in dem Verfahren nicht um die Frage geht, ob IP-Adressen immer und unter allen Umständen personenbezogene Daten im Sinne des Datenschutzrechts sind und ob IP-Adressen unvermeidlich als personenbezogene Daten zu qualifizieren sind, sobald ein Dritter, wer dies auch sei, in der Lage ist, sie zur Identifizierung von Internetnutzern zu verwenden.[496] Eine abschließende Entscheidung über die Frage des Personenbezugs bei IP-Adressen ist daher auch mit der Entscheidung des Europäischen Gerichtshofs, die nicht auf Grundlage der DS-GVO erging, nicht getroffen worden.

---

[492] Dazu *Härting*, Jan Philipp Albrecht setzt sich durch: Datenschutzrecht soll ausnahmslos für Maschinendaten gelten, CR online Blog vom 09.12.2015, online abrufbar.

[493] BGH, Beschluss vom 28.10.2014 – VI ZR 135/13, NJW 2015, 368.

[494] EuGH, C-582/14, Rn. 49.

[495] Vgl. Anmerkung von *Moos*, MMR 2016, 842 (846).

[496] GA *Sánchoz-Bordona*, Schlussanträge, C-582/14, Rn. 50.

In jedem Fall wird in diesem Zusammenhang zukünftig die technische Entwicklung zu beachten sein. Neben der Unterscheidung der statischen von den dynamischen IP-Adressen sind Internetprotokolladressen der Version 4 (IPv4) vom Internetprotokoll der Version 6 (IPv6) zu differenzieren. IPv6-Adressen werden seit einigen Jahren und in Zukunft zunehmend als feste Adressen vergeben.[497] Das weltweite Anwachsen der Anzahl der Internetteilnehmer und internetfähigen Endgeräte hat dazu geführt, dass alle zur Verfügung stehenden IPv4-Adressen verteilt sind und Knappheit in diesem Adressraum die Umstellung auf ein neues Internetprotokoll erforderlich macht. Mit der Einführung von IPv6 als neuen Standard werden zukünftig 340 Sextillionen ($3{,}4 \times 10^{38}$) IPv6-Adressen zuteilbar sein.[498] Der damit verbundene neue Adressaufbau führt dazu, dass allen Rechnern (z. B. allen am Internet der Dinge beteiligten und mit einer Netzwerkschnittstelle ausgestatteten Geräte) eine oder mehrere IP-Adressen statisch zugeordnet werden können. Die durch IPv4 noch in Teilen mögliche Form der Anonymität wird durch die dann nicht mehr erforderliche dynamische Vergabe von Adressen grundsätzlich nicht mehr vorhanden sein. Die Internetadresse ist dann weltweit eindeutig.[499] Das Bundesverfassungsgericht stellt in diesem Zusammenhang fest, dass den Gesetzgeber in Bezug auf § 112 TKG eine Beobachtungs- und ggf. Nachbesserungspflicht treffe, da § 112 TKG ein erheblich größeres Eingriffsgewicht auf Basis des Internetprotokolls Version 6 und des damit verbundenen erhöhten Informationspotenzials abgefragter statischer IP-Adressen erhalten könne.[500]

Die Frage nach dem datenschutzrechtlichen Personenbezug von Maschinendaten ist nicht abschließend zu beantworten. Sie ist Ergebnis einer Wertung und zukünftig von technischen Umständen abhängig. Für die hier übergeordnete Untersuchung der Grenzen der Informationsgenerierung öffentlicher Stellen zu Zwecken der Gewährleistung der Netz- und Informationssicherheit kommt es darauf an, ob überhaupt und welche Daten im Einzelnen verarbeitet werden. Der Blick auf europäische Regulierungspraktiken macht deutlich, dass die Datenverarbeitung von dem jeweils gewählten Regulierungsansatz und dem Design des Datenaustausches von NIS-Behörden und Unternehmen abhängt. Die Ansätze sind mitunter disparat.[501] Dass eine Behörde wie das BSI oder die CSIRTs tatsächlich etwaige Maschinendaten Daten verarbeiten können, ergibt sich im Übrigen aus Anhang I Abs. 2 lit. a 2. Spiegelstrich NIS-RL bzw. § 7

---

497 Zur Spezifikation RFC 2460; *Wegener*/*Heidrich*, CR 2011, 479 ff.

498 Siehe *Hagen*, IPv6, 2. Aufl. 2009, S. 43 ff.

499 *Hoeren*, ZRP 2010, 251 (252 f.).

500 BVerfGE 130, 151 (199).

501 Vgl. *ENISA*, Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches, 2015, S. 20, 34.

BSIG.[502] Die Information und Warnung von Nutzern vor Sicherheitslücken, Schadprogrammen und Störungen, zu deren Durchführung Dritte mit einbezogen werden können, kann die Kenntnis der IP-Adresse oder anderer (personenbezogene) Daten voraussetzen.[503]

2. Zur Rechtfertigung der Datenverarbeitung zum Zwecke der Netz- und Informationssicherheit

Die Verarbeitung personenbeziehbarer Daten durch die NIS-Verwaltung setzt in tatsächlicher wie rechtlicher Hinsicht eine zulässige Datenverarbeitung durch die Betreiber kritischer Infrastrukturen und Anbieter von Telekommunikations- und Telemedien voraus. Nur wenn die Infrastrukturbetreiber und Dienstanbieter ihrerseits rechtmäßig Daten zur Gefahrenabwehr verarbeiten dürfen (a), kann untersucht werden, nach Maßgabe welcher Kriterien die Datenverarbeitung der zentralen NIS-Behörden gerechtfertigt werden kann (b).

a) Datenverarbeitung durch Diensteanbieter und Infrastrukturbetreiber

Eine die Datenverarbeitung rechtfertigende Einwilligung (vgl. § 3 Abs. 1 BDSG, § 13 Abs. 2 TMG bzw. Art. 6 Abs. 1 lit. a. DS-GVO, § 94 TKG[504]) durch alle von der Datenverarbeitung Betroffenen wird regelmäßig nicht vorliegen, obwohl diese erforderlich ist, weil für das Einwilligungserfordernis nicht danach differenziert werden kann, ob ein rechtmäßiger Nutzer oder ein externer Angreifer auf Netze, IT-Systeme und Telemedien zugreift. Schon strukturell und aus Gründen der Praktikabilität scheidet das Einholen einer bewussten und eindeutigen Einwilligung aus. Demnach muss die Datenverarbeitung der Diensteanbieter und Infrastrukturbetreiber zum Zweck der Abwehr von Gefahren für die Netze und Informationssysteme auf eine gesetzliche Grundlage gestützt sein.

---

[502] Vgl. auch § 8d Abs. 2 S. 2 BSIG.

[503] Vgl. *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*, Stellungnahme zum IT-Sicherheitsgesetz, 20.10.2014, S. 2. Das BSI hat 2014 eine Datenbank mit 16 Millionen kompromittierten Benutzerkonten aufgesetzt, mit der Nutzer ihre Daten mit Daten aus Botnetzen abgleichen konnten. Die Benutzerkonten bestanden regelmäßig aus Benutzernamen in Form einer E-Mail-Adresse und Passwörtern, dazu *BSI*, Millionenfacher Identitätsdiebstahl: BSI bietet Sicherheitstest für E-Mail-Adressen, Pressemitteilung vom 21.01.2014; *Horchert*, E-Mail-Check beim BSI: Verunsicherte Bürger legen Behördenseite lahm, Spiegel Online, 21.01.2014, online abrufbar.

[504] Vgl. Erwägungsgrund 17 und Art. 2 UAbs. 2 lit. f RL 2002/58/EG in der Fassung der TL 2009/136/EG.

aa) Verarbeitung datenschutzrechtlich geschützter Daten zur Gefahrenabwehr im Telekommunikationsrecht

Eine Rechtsgrundlage für Anbieter von Telekommunikationsdiensten zur Verarbeitung von Daten zu Zwecken der Abwehr von Cybergefahren für die Netz- und Informationssicherheit stellt § 100 Abs. 1 TKG dar. Auf Grundlage dieser Vorschrift können Bestands- und Verkehrsdaten zum Erkennen, Eingrenzen und Beseitigen von Störungen und Fehlern an Telekommunikationsanlagen erhoben und verwendet werden.[505] Im europäischen Datenschutz ist eine solche Vorschrift nicht vorgegeben, die Mitgliedstaaten sind aber nach Art. 6 Abs. 5 RL 2002/58/EG dazu befugt, sie zu schaffen.[506]

Verkehrsdaten sind gemäß § 3 Nr. 30 TKG „Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden". Erfasst sind in dieser Definition demnach sämtliche Daten, die mit der Erbringung des Dienstes in Zusammenhang stehen, einschließlich also der in den technischen Übermittlungs- und Abrechnungssystemen erhobenen oder anfallenden Daten für den Telekommunikationsvorgang.[507] Verkehrsdaten sind nicht nur (dynamische) IP-Adressen, sondern auch Kopfdaten (Header), die anfallen, wenn die Datenübertragung einen Telekommunikationsvorgang darstellt[508], oder Logfiles.[509] Die eigentlichen Kommunikationsinhalte sind demnach nicht Bestandteil der Protokolldaten.

Der Begriff der Störung war lange Zeit umstritten. Das Begriffsverständnis ist von erheblicher Bedeutung, weil davon abhängt, gegen welche Angriffsarten sich die Telekommunikations-Anbieter schützen können. Somit hat die Vorschrift eine indirekte Funktion für die Netz- und Informationssicherheit. Der Störungsbegriff des § 100 Abs. 1 TKG entspricht dem aus § 8b Abs. 4 BSIG und ist demnach funktional zu verstehen.[510] Dieses umfassende Verständnis ermöglicht es, gegen spezifische Missbräuche des Internets vorzugehen. So können der Empfang von

---

[505] Zu den Verkehrsdaten gehört auch hier die IP-Adresse, Begründung der Bundesregierung des Entwurfs eines Telekommunikationsgesetzes, BT-Drs. 15/2316, S. 90; *Wittern*, in: Geppert/Schütz (Hrsg.), BeckTKG, 4. Aufl. 2013, § 100 Rn. 3.

[506] Vgl. auch Art. 15 und Erwägungsgrund 29.

[507] Vgl. TK-Datenschutzrichtlinie 2002/58/EG, Erwägungsgrund 15; *Heun*, in: Auernhammer, 4. Aufl. 2014, TKG, Vor. zu § 88 Rn. 101.

[508] Siehe § 3 Abs. 8 S. 2 BSIG.

[509] § 96 Abs. 1 TKG ist nicht abschließend, sodass der Begriff für jede Verbindungsart, hier: Datenverbindungen, spezifiziert werden muss. Siehe *Büttgen*, in: Scheurle/Mayen (Hrsg.), TKG, 2. Aufl. 2008, § 96, Rn. 3; a. A. *Braun*, in: Geppert/Schütz (Hrsg.), BeckTKG, 4. Aufl. 2013, § 96 Rn. 6.

[510] Siehe bereits § 3 D. I. 2. (3); kritisch etwa *Mantz*, CR 2012, S. 605 (606); *Braun*, in: Geppert/Schütz (Hrsg.), BeckTKG, 4. Aufl. 2013, § 100 Rn. 11; siehe dagegen BGH, NJW 2014, 2500 (2502).

Spam-Mails und Schad- oder Spionageprogrammen sowie Denial-of-Service-Attacken und dergleichen durch Abuse Handling abgewehrt werden.[511] Dabei handelt es sich vor allem um Angriffe, die auch die Verfügbarkeit der Netze beeinträchtigen können. Letztlich ist darin die gesetzliche Neuregelung von § 100 Abs. 1 S. 2 TKG durch das IT-Sicherheitsgesetz begründet.[512] Die Datenverarbeitung ist zu Zwecken der Bekämpfung solcher Störungen erlaubt, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf die TK- und Datenverarbeitungssysteme der Nutzer führen können. Die Diensteanbieter dürfen folglich ihren Netzwerkverkehr prüfen, indem sie sog. Honeypots oder Spamtraps einsetzen.[513]

Ein weiteres Problem bei der Frage, ob Anbieter von Telekommunikationsdiensten zur Gefahrenabwehr personenbezogene Daten verarbeiten dürfen, ist die zulässige Speicherdauer der erhobenen Daten, die nicht ausdrücklich aus den drei in der Vorschrift genannten Verarbeitungsstufen Erkennen, Eingrenzen und Beseitigen hervorgeht.[514] Das Speichern von IP-Adressen und Session-Daten kann erforderlich sein, um Störungen und Fehler aus der Analyse der Daten durch Musterbildung und Anomaliediagnose zu erkennen und prospektiv einzugrenzen oder zu beseitigen.[515] Insofern könnte das Tatbestandsmerkmal „Erkennen" das Speichern beinhalten, weil für eine Erkennung Anhaltspunkte bestehen müssen, die sich erst aus der retrospektiven Betrachtung gespeicherter Daten ergeben.

Zulässig ist die Datenspeicherung allenfalls, wenn sie geeignet, erforderlich und im engen Sinne verhältnismäßig ist, um abstrakten Gefahren entgegenzuwirken. Der BGH erlaubt eine auf sieben Tage begrenzte Speicherung von Verkehrsdaten, wenn die präventive Erhebung und Speicherung diesem Zweck

---

[511] Dies aber bestritt der Kläger in OLG Frankfurt a. M., ZUM-RD 2013, 596, da etwa Spam-E-Mails nur Kapazitätsprobleme darstellen, nicht aber die Funktionsfähigkeit beeinträchtigten. Die Infrastruktur sei durch etwaige Angriffsarten nicht bedroht.

[512] *Leisterer/Schneider*, CR 2014, 574 (578).

[513] BR-Drs. 643/14, S. 52. Dabei handelt es sich um Fallen für Schadprogramme im Netz bzw. damit ist das Blockieren und Versenden von Schadprogrammen gemeint.

[514] Die DS-GVO löst das Spannungsverhältnis solange nicht auf, wie das Verhältnis zu den Richtlinien-Regelungen im Bereich der Telekommunikation besteht. Art. 95 DS-GVO ordnet an, dass den Betreibern von TK-Diensten durch die DS-GVO keine zusätzlichen Pflichten auferlegt werden, soweit die Pflichten in der RL 2002/58/EG dasselbe Ziel verfolgen.

[515] Der Kläger blieb in einem Streit darüber vor dem LG Darmstadt, Urteil v. 06.06.2007 – Az. 10 O 562/03, abrufbar unter: http://tlmd.in/u/1008, und vor dem OLG Frankfurt a. M., MMR 2010, 645 und ZD 2013, 614 erfolglos. Das OLG Frankfurt a. M. stellte nach Einholung eines Gutachtens fest, dass zur Speicherung der Logdaten keine Alternative bestehe, um Störungen und Fehler zu bekämpfen, und andernfalls die Gefährdung der Kommunikationsinfrastruktur zu befürchten sei.

dient und technisch erforderlich ist.[516] Diese Rechtsprechung dürfte auch nach der Novellierung des TKG durch das IT-Sicherheitsgesetz gelten, da die in § 100 Abs. 1 TKG genannten Verarbeitungsstufen nicht geändert wurden.[517]

Die Speicherung darf anlasslos erfolgen, solange die Verhältnismäßigkeit der Speicherung gewahrt bleibt.[518] Mit Blick auf die materielle Gewährleistungspflicht in § 109 TKG ist dies angemessen. Nicht zuletzt § 88 Abs. 3 S. 1 TKG, auf Grundlage dessen die Analyse von Inhaltsdaten, etwa im Rahmen des Einsatzes von Deep-Packet-Inspection-Systemen, gerechtfertigt werden kann,[519] streitet für die Rechtmäßigkeit der Erhebung, Speicherung und Verwendung personenbezogener Daten zum Zwecke der Gefahrenabwehr. Im Übrigen würde eine Speicherung nur dann gegen Unionsrecht, d. h. Art. 15 Abs. 1 und Art. 6 I RL 2002/58/EG, nach denen eine verhältnismäßige Speicherung zur Abwehr eines unzulässigen Gebrauchs der Kommunikationssysteme erlaubt ist, verstoßen, wenn der den Mitgliedstaaten eröffnete Beurteilungsspielraum zur Interessenabwägung offensichtlich[520] unverhältnismäßig[521] ausgefüllt wird. Dies ist bei § 100 Abs. 1 TKG nicht der Fall.

Anbieter von Telekommunikationsdiensten können demnach zur Abwehr von Gefahren für die Netz- und Informationssicherheit personenbezogene Daten verarbeiten.

bb) Verarbeitung datenschutzrechtlich geschützter Daten zur Gefahrenabwehr im Telemedienrecht und allgemeinen Datenschutzrecht

Die Grundsätze zum Umgang mit personenbezogenen Daten im Bereich der Telemediendienste legt § 12 TMG fest. Der Diensteanbieter darf personenbezogene Daten zur Bereitstellung von Telemedien gemäß § 12 Abs. 1 TMG nur erheben und verwenden, soweit das TMG oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat. Das allgemeine Datenschutzrecht ist gemäß § 12 Abs. 3 TMG subsidiär anzuwenden.

Als Rechtsgrundlage kommt § 15 Abs. 1 S. 1 TMG in Betracht, der das Erheben und Verwenden von Nutzungsdaten ermöglicht, um die Inanspruchnahme von Telemedien „zu ermöglichen und abzurechnen", ohne dass ein Vertragsverhältnis zwischen Anbieter und Nutzer bestehen muss.[522] Nutzungsdaten sind

[516] BGH, NJW 2011, 1509 (1511 ff.). In dem betreffenden Fall ging es um IP-Adressen.
[517] Kritisch *Rath/Kuss/Bach*, K&R 2015, 437 (440).
[518] Vgl. *Eckhardt*, CR 2003, S. 805 (809).
[519] *Heun*, in: Auernhammer, 4. Aufl. 2014, TKG, § 88 Rn. 34.
[520] Zum Acte-clair-Kriterium BGHZ 174, 273 (287).
[521] Zu diesem Kriterium EuGH, NJW 2008, 743 (746).
[522] *Spindler/Nink*, in: ders./Schuster (Hrsg.), Recht der elektronischen Medien, 3. Aufl.

solche personenbezogenen Daten, die bei der Nutzung entstehen und erforderlich sind, um die Inanspruchnahme des Telemediums zu ermöglichen oder abzurechnen. Wann es Nutzungsdaten für die konkrete Nutzung bedarf und welcher Art diese sein müssen, ist abhängig von der Art und dem Zweck des Dienstes.[523] Die Erhebung und Verwendung von Daten wie die IP-Adresse wird regelmäßig erforderlich sein, um dem Nutzer den Zugriff auf den Host-Server des Telemediums zu ermöglichen.

Im Kontext der Gefahrenabwehr ist die Norm in mehreren Aspekten problematisch. Dem Wortlaut nach erlaubt die Norm nicht die Datenverarbeitung zum Zwecke der Gefahrenabwehr. Zwar können durch den Wortlaut „Inanspruchnahme […] zu ermöglichen" wohl noch Angriffe auf das Schutzziel der Verfügbarkeit wie durch Distributed-Denial-of-Service-Attacken subsumiert werden, weil solche Angriffsarten die Inanspruchnahme des Dienstes unmöglich machen können.[524] Wie bei Anbietern von Telekommunikationsdiensten setzen die Abwehrmaßnahmen aber nicht nur das Loggen von Daten voraus, sondern auch deren Speicherung, ohne die keine effektive Auswertung der Daten möglich wäre. Eine Speicherung von Logdaten über den konkreten Nutzungsvorgang hinaus ist allerdings nur über § 15 Abs. 4 S. 1 TMG für Abrechnungsdaten erlaubt. Im Ergebnis sind dem Wortlaut nach Schutzmaßnahmen wie Intrusion-Detection-Systeme erlaubt, eine Speicherung ist jedoch nach der Konzeption der Vorschrift nicht ohne Weiteres möglich.[525]

Denkbar erscheint es, die Datenverarbeitung der Telemediendiensteanbieter durch eine entsprechende Anwendung von § 100 Abs. 1 TKG zu rechtfertigen. Eine direkte Anwendung scheidet aus, weil die datenschutzrechtlichen Bestimmungen der §§ 91 ff. TKG nur für geschäftsmäßige Telekommunikationsdienste gelten (§ 3 Nr. 24 in Verbindung mit § 3 Nr. 6 TKG und § 1 S. 1 TMG). Das Interesse der Telemedienanbieter daran, ihre Informationssysteme vor Angriffen zu schützen, ist aber nicht weniger legitim als das der Telekommunikations-

---

2015, TMG, § 15 Rn. 2. Da zwischen dem Anbieter und Angreifer typischerweise kein Vertragsverhältnis besteht, stellt § 14 TMG keine taugliche Rechtsgrundlage zur Cyberabwehr dar, zumal IP-Adressen und andere Logdaten keine Bestandsdaten im Sinne der Norm sind. Vgl. Müller-Broich, Telemediengesetz, 2012, § 14 Rn. 2; zur möglichen Überschneidung mit Nutzungsdaten Jandt/Laue, K&R 2006, 316 (320); zur Behandlung der dynamischen IP-Adresse als Bestandsdatum im Strafprozessrecht BT-Drs. 16/5846, S. 26 f., 86 f.

[523] BT-Drs. 13/7385, S. 24; *Spindler/Nink*, in: ders./Schuster (Hrsg.), Recht der elektronischen Medien, 3. Aufl. 2015, TMG, § 15 Rn. 7.

[524] *Meyerdierks/Gendelev,* ZD 2013, 626 (627).

[525] Für eine Unzulässigkeit auch der Erhebung und Verwendung zur Störungserkennung *Hornung*, Stellungnahme zum Entwurf eines IT-Sicherheitsgesetzes vom 18.04.2015, A-Drs. 18(4)284 G, S. 19; ferner auch Stellungnahme des FIfF zum IT-Sicherheitsgesetz vom 17.12.2014, A-Drs. 18(4)252, S. 4 f., online abrufbar.

diensteanbieter. Ohnehin sind mit der durch das IT-Sicherheitsgesetz eingeführten materiell-rechtlichen Sicherheitspflicht des § 13 Abs. 7 TMG die Anbieter zur Gewährleistung der IT-Sicherheit verpflichtet.[526] Der vergleichbare Verarbeitungszweck spricht ebenfalls für eine analoge Anwendung der weitreichenden Norm.

Dem Argument einer Regelungslücke aber steht zum einen der Wortlaut („nur […], um“) und zum anderen die Genese der Vorschrift entgegen. Der an § 100 TKG angelehnte § 15 Abs. 9 TMG-E wurde bewusst nicht eingeführt.[527] Eine Vorlage des Bundesgerichtshofs beim Europäischen Gerichtshof der Frage, ob § 15 Abs. 1 TMG als Rechtsgrundlage zur Abwehr von IT-Angriffen herangezogen werden kann,[528] ergibt im Umkehrschluss, dass § 100 TKG nicht in Betracht kommt, denn andernfalls wäre die Vorlagefrage nicht entscheidungserheblich gewesen.[529]

Wird die Datenverarbeitung zur Gefahrenabwehr grundsätzlich als zulässig angesehen, besteht ein Spannungsverhältnis zu § 13 Abs. 6 TMG.[530] Danach hat der Diensteanbieter grundsätzlich eine anonyme oder pseudonyme Nutzung zu ermöglichen. Der BGH hat jedoch anerkannt, dass eine Pseudonymisierung erfasster IP-Adressen untunlich und unzumutbar ist.[531] Im Rahmen der summarischen Prüfung der Interessen würden die Güter und Interessen des Betroffenen im Übrigen nicht überwiegen.[532] Demnach besteht das Gebot der Anonymität einer auf Datenverarbeitung basierenden Schutzmaßnahme, wenn die Eingriffsintensität, die sich aus der Art der erfassten Daten und der Speicherdauer ergeben kann, verhältnismäßig ist. Grundsätzlich ist die Eingriffstiefe der Maßnahmen technisch skalierbar und sie lässt sich an dem Kriterium der Erforderlichkeit ausrichten.[533]

---

[526] Zu den Rechtsfragen des neuen Tatbestands *Gerlach*, CR 2015, 581 ff.

[527] Ursprünglich sah ein Entwurf zum IT-Sicherheitsgesetz einen § 15 Abs. 9 TMG-E vor, der an § 100 TKG angelehnt war und der es erlaubt hätte, Logdaten zur Abwehr von Cybergefahren im Internet zu speichern. Dieser eindeutige Erlaubnistatbestand wurde nicht in die Beschlussfassung übernommen. Siehe Referentenentwurf eines IT-Sicherheitsgesetzes, Art. 2 Nr. 3, Stand 18.08.2014, abrufbar unter: http://www.computerundrecht.de/Entwurd_IT-Sicherheitsgesetz_1808.pdf.

[528] BGH, CR 2015, 109 (Vorlagebeschluss an EuGH – Rs. C-582/14).

[529] *Bergt*, BGH bestätigt: Webserver-Logfiles nicht nach § 100 Abs. 1 TKG erlaubt, CRonline vom 28.10.2014, online abrufbar.

[530] Vgl. Art. 25 Abs. 1, Art. 32 Abs. 1 lit. a DS-GVO.

[531] BGH, Urteil vom 03. Juli 2014 – III ZR 391/13 –, juris, Rn. 8.

[532] Insbesondere sind dies solche aus den Art. 5, 10, 13 sowie dem Art. 2 (in Verbindung mit Art. 1) GG mit den entwickelten Ausprägungen. Siehe für das IT-Grundrecht und das Verhältnis zum Datenschutz *Roßnagel/Schnabel*, NJW 2008, 3534 (3538).

[533] Zum Maßstab und zur Abwägungsmethodologie *Kramer*, in: Auernhammer 4. Aufl. 2014, BDSG, § 28 Rn. 70 ff.

Schließlich stehen der Zulässigkeit der Datenverarbeitung unionsrechtlichen Bedenken nicht entgegen. Vor der Verabschiedung der DS-GVO konnte noch vertreten werden, dass § 15 Abs. 1 TMG eine Konkretisierung der unionrechtlichen Grundnorm Art. 7 lit. f RL 95/46/EG (Datenschutz-Richtlinie) sei. Maßgebliches Rechtmäßigkeitskriterium ist dort die zugunsten des Datenverarbeitenden ausfallende Interessenabwägung. Da § 15 Abs. 1 TMG keinen Spielraum für eine Abwägung der grundrechtlich geschützten Interessen lässt, stand die Vorschrift mit den unionsrechtlichen Vorgaben im Widerspruch.[534] Eine unionsrechtskonforme Auslegung des Tatbestandsmerkmals „Ermöglichen" wäre aufgrund des eindeutigen Wortlauts („Der Diensteanbieter darf […] nur erheben und verwenden") eine solche *contra legem* gewesen. Dazu ist der Rechtsanwender nicht verpflichtet.[535] Gegen den Widerspruch konnte eingewandt werden, dass nach Art. 288 Abs. 2 und 3 AEUV die Datenschutz-Richtlinie die Mitgliedstaaten nur hinsichtlich des Ziels zur Umsetzung verpflichtet werden und demnach im nationalen Recht Erlaubnistatbestände einführen können, die bereits eine abstrakt-generelle Abwägung vornehmen. Dagegen sprach die Rechtsprechung des Europäischen Gerichtshofs, der, obgleich die Mitgliedstaaten im Rahmen ihres Ermessens Leitlinien für die geforderte Abwägung aufstellen können,[536] im Ansatz von einer Vollharmonisierung der nationalen Rechtsvorschriften durch die Datenschutz-Richtlinie ausging.[537] Die Richtlinie gebe den Mitgliedstaaten sowohl Mindeststandards als auch eine Beschränkung hinsichtlich der Erhöhung des Datenschutzniveaus auf.[538]

Mit der Anwendung der DS-GVO ist der Normkonflikt entschärft. Nach der Aufhebung der Datenschutzrichtlinie durch Art. 99 DS-GVO führt Art. 6 lit. f DS-GVO, der Art. 7 lit. f RL 95/46/EG entspricht, zum Abwägungsprinzip.[539] Die Erwägungen zur DS-GVO zeichnen das Abwägungsergebnis zum Teil vor. Die Datenverarbeitung, unter der gemäß Art. 4 Abs. 3 DS-GVO auch die Speicherung zu verstehen ist, stelle in dem Maße ein berechtigtes Interesse dar, wie sie für die Gewährleistung der Netz- und Informationssicherheit notwendig und verhältnismäßig ist.[540] Im Übrigen werden damit die telemediendatenschutzrechtlichen Vorschriften in den §§ 11 TMG nicht mehr anwendbar sein, da die Normen des TMG nicht das Telekommunikationsdatenschutzrecht (RL 2002/58/

---

534 Auf Grundlage der RL 95/46/EG EuGH, C-582/14, Rn. 64.
535 EuGH (Große Kammer), NJW 2012, 509 (510).
536 EuGH, C-486/10, C-469/10, CR 2012, 29 (31).
537 Vgl. EuGH, C-101/01, CR 2004, 286 (290); kritisch *Masing,* NJW 2012, 2305 (2311).
538 EuGH, C-486/10, C-469/10, CR 2012, 29 (30).
539 KOM(2012) 11 endg., Erläuterungen zu Kapitel 2 – Grundsätze, 3.4.2.
540 Erwägungsgrund 49 DS-GVO.

EG in Verbindung mit 89 DS-GVO) umsetzen.[541] Die Datenschutzgrundverordnung ist in allen ihren Teilen verbindlich und gilt in jedem Mitgliedstaat unmittelbar (Art. 288 Abs. 2 S. 2 AEUV). Der unionsrechtliche Anwendungsvorrang vor dem nationalen Recht reicht so weit, wie der Anwendungsbereich definiert ist.[542] Damit genießt die DS-GVO gegenüber den datenschutzrechtlichen Regelungen im TMG Vorrang. Sofern kritische Infrastrukturen keine Anbieter von Telekommunikationsdiensten und -netzen oder Telemediendiensten sind, können sie ihre Datenverarbeitung zu Zwecken der Cybersicherheit ebenso auf Art. 6 lit. f DS-GVO stützen.

b) Datenverarbeitung durch NIS-Verwaltung

Nachdem nun die Zulässigkeit der Datenverarbeitung der privaten Internetinfrastrukturbetreiber und Diensteanbieter untersucht wurde, ist zu fragen, wie die Verarbeitung personenbezogener Daten im Rahmen der administrativen Informationsgenerierung gerechtfertigt werden kann. Die Frage der Rechtfertigung stellt sich für das BSI, die Bundesnetzagentur und die CSIRTs insbesondere im Zuge der durch das IT-Sicherheitsgesetz eingeführten Meldepflichten (aa). Sofern das allgemeine Datenschutzrecht in den Mitgliedstaaten Anwendung findet,[543] bedingt dies nicht nur das Erfordernis einer Rechtsgrundlage, sondern auch die Beachtung weiterer datenschutzrechtlicher Prinzipien, die Einfluss auf die Effektivität der Generierung von Informationen zur Sicherheitsgewährleistung haben. Von hervorzuhebender Bedeutung für Informationsgenerierung und Produktion von Wissen über die Sicherheit von Netzen und Informationssystemen sind die Prinzipien der Datenminimierung und der Grundsatz der Zweckbindung. Hinzu kommt daher die Frage, welche Begrenzungswirkung auf die Informationsgenerierung die datenschutzrechtlichen Grundsätzen der Datenminimierung (bb) und der Zweckbindung (cc) entfalten.

aa) Zur Rechtfertigung der Datenverarbeitung

Bei Bestehen eines Personenbezugs ist grundsätzlich das Datenschutzrecht zu beachten. Art. 2 NIS-RL stellt für die Datenverarbeitung „gemäß dieser Richtlinie" klar, dass sie nach Maßgabe der Datenschutzrichtlinie respektive der Datenschutz-Grundverordnung zu erfolgen hat. Erwägungsgrund 72 der NIS-RL geht davon aus, dass „der Austausch von Informationen über Risiken und Vorfälle […] und die Einhaltung der Verpflichtung zur Meldung von Sicherheitsvor-

[541] *Keppeler*, MMR 2015, 779 (781).

[542] Vgl. *Ruffert*, in: Calliess/ders. (Hrsg.), EUV/AEUV, 4. Aufl. 2011, AEUV Art. 288 Rn. 20, Art. 1 Rn. 16 ff.

[543] Zur nachrichtendienstlichen Datenerhebung siehe § 3 D. II. 3.

fällen“ die Verarbeitung personenbezogener Daten erfordern könnten. Ebenfalls geht die deutsche Regelung für die Meldepflicht von Betreibern kritischer Infrastrukturen in § 8b Abs. 7 BSIG von der datenschutzrelevanten Verarbeitung aus.

Die Verarbeitung personenbezogener Daten im Rahmen der NIS-Richtlinie erfolgt nach deren Art. 2 nach Maßgabe der Richtlinie 95/46/EG. Diese Datenschutzrichtlinie wird gemäß Art. 94 DS-GVO mit Inkrafttreten der Datenschutz--Grundverordnung aufgehoben. Verweise auf die aufgehobene Richtlinie gelten als Verweise auf die Verordnung. Mit Art. 2 DS-GVO wird prinzipiell der Ansatz verfolgt, das gesamte Datenschutzrecht allumfassend zu regeln und sämtliche nationale Normen zu verdrängen.[544] Öffnungsklauseln in der DS-GVO ermöglichen indes den Mitgliedstaaten spezifische Anforderungen sowie sonstige Maßnahmen für eine rechtmäßige Datenverarbeitung präziser zu bestimmen. So können die Mitgliedstaaten gemäß Art. 6 Abs. 2 DS-GVO insbesondere die Bestimmungen zur Datenverarbeitung, die zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe dienen, beibehalten oder neu einführen.

Als spezifische Grundlage für die Datenverarbeitung des BSI im Rahmen der Meldepflicht kommt § 8b Abs. 2 BSIG in Betracht, da der Absatz im systematischen Zusammenhang mit der Festlegung des BSI als zentrale Meldestelle steht und nachdem das BSI zu dieser Aufgabe „die […] wesentlichen Informationen […] sammeln und auszuwerten“ hat. Allerdings kann darin eine rechtliche Verpflichtung im Sinne des Art. 6 Abs. 1 UAbs. 1 lit. c, Abs. 3 DS-GVO (vgl. § 4 BDSG) zu sehen sein, wenn sie zusätzliche Voraussetzungen erfüllt. Verlangt wird eine Norm, welche die Verarbeitung personenbezogener Daten eindeutig für zulässig erklärt.[545] Jedenfalls aber reicht eine die Datenverarbeitung voraussetzende bloße Aufgabenbeschreibung nicht aus.[546] Etwas anderes ergibt sich nicht aus § 8b Abs. 7 S. 1 BSIG. Danach soll eine über die § 8b BSIG hinausgehende Verarbeitung und Nutzung zu anderen Zwecken unzulässig sein. Daraus folgt aber im Umkehrschluss lediglich die Konkretisierung der Zweckbestimmung. Im Übrigen sind nach § 8b Abs. 7 S. 3 BSIG die Regelungen des BDSG und somit das allgemeine Datenschutzrecht anzuwenden. Für die Daten-

---

[544] *Keppeler*, MMR 2015, 779 (781).

[545] *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl. 2015, § 4 Rn. 8; schwächer *Bäcker*, in: Wolff/Brink (Hrsg.), Datenschutzrecht, 2013, BDSG, § 4 Rn. 6, dem zufolge es ausreiche, dass sich etwa die Art der Daten und der Zweck der Verarbeitung durch Auslegung ermitteln lasse.

[546] *Sokol*, in: Simitis (Hrsg.), BDSG, 8. Aufl. 2014, § 4 Rn. 15; *Weichert*, in: Däubler/Klebe/Wedde/ders. (Hrsg.), BDSG, 5. Aufl. 2016, § 4 Rn. 3; letztlich auch *Bäcker*, in: Wolff/Brink (Hrsg.), Datenschutzrecht, 2013, BDSG, § 4 Rn. 6.

verarbeitung der Bundesnetzagentur im Rahmen der Meldepflicht scheidet aus den gleichen Gründen § 109 Abs. 5 TKG als besondere Rechtsgrundlage aus.

Somit kommt wegen des Verweises in § 8b BSIG auf das allgemeine Datenschutzrecht, sofern die Mitgliedstaaten nicht von ihrer Abweichungskompetenz Gebrauch machen, als zentrale Rechtsgrundlage Art. 6 DS-GVO für die Datenverarbeitung der NIS-Verwaltung in Betracht, insbesondere Art. 6 Abs. 1 UAbs. 1 lit. e DS-GVO stellt auf die Erfüllung einer im öffentlichen Interesse liegenden Aufgabe ab.[547] Ein pauschaler Rückgriff auf das „öffentliche Interesse" ist für sich noch nicht geeignet, die Datenverarbeitung der Verwaltung zu Zwecken der Gewährleistung von Netzen und Informationssystemen zu rechtfertigen[548] Das öffentliche Interesse ist kein isoliertes Rechtsgut, sodass stets eine spezifische Abwägung zwischen der im öffentlichen Interesse stehenden Aufgabe und den Interessen und Rechten der betroffenen Personen stattzufinden hat.[549] Überwiegen letztere Interessen, ist die Datenverarbeitung nicht rechtmäßig.[550]

Die Rechtfertigung richtet sich folglich nach der festzustellenden Eingriffsqualität und -tiefe.

Die gegenläufigen Interessen des öffentlichen Interesses und die Belange des Datenschutzes auf Regelungsebene einer sekundärrechtlichen Verordnung oder eines Bundesgesetzes auszugleichen, ist aufgrund der erforderlichen Abstraktion kaum möglich. Die Abwägung richtet sich nämlich nach der konkreten Art und Weise der Datenverarbeitung durch öffentliche Stellen. Die Anwendungsszenarien der Datenverarbeitung sind dabei entwicklungsoffen und dynamisch.[551] Für die Frage nach dem Eingriffsgewicht ist letztlich auf den Anlass und den Umfang der Speicherung, den Zweck der Verwendung und die Art und Weise der Abfrage (offen oder heimlich) abzustellen.[552]

---

[547] Vgl. *EDPS*, Opinion of the European Data Protection Supervisor on the Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy on a ‚Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace', and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union, 2013, S. 19 Rn. 61.

[548] *Engeler/Jensen/Obersteller/Deibler/Hansen*, Monitoring durch Informationsfusion und Klassifikation zur Anomalieerkennung, 2014, S. 88.

[549] *Dammann*/*Simitis*, in: EG-Datenschutzrichtlinie, 1997, Art. 7 Rn. 11; vgl. *Frenzel*, in: Paal/Pauly, DS-GVO, 2017, Art. 6 Rn. 23.

[550] Vgl. Erwägungsgrund 47 DS-GVO bzw. 30 RL 95/46/EG.

[551] Siehe *Roos*/*Schumacher*, Monitoring durch Informationsfusion und Klassifikation zur Anomalieerkennung, 2014, S. 151 mit Überlegungen eines verpflichtenden kooperativen und datenintensivem Monitorings zwischen privaten und öffentlichen Stellen.

[552] Zur Rechtfertigung der Datenverarbeitung von CSIRTs *Cormack*, Incident Response

bb) Grundsatz der Datenminimierung

Zu den Grundsätzen der Verarbeitung gehört die Datenminimierung. Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (vgl. Art. 5 Abs. 1 lit. c DS-GVO). Der Grundsatz ist ein Aspekt des Systemdatenschutzes und stellt eher einen Programmsatz denn eine zwangsbewährte Zielvorgabe dar.[553] Das Telos der Norm schließt ein, Gefahren eines Missbrauchs von Daten präventiv durch Datenvermeidung zu begegnen. Dem Schutz vor einer übermäßigen Datengenerierung dient prinzipiell auch der Grundsatz der Erforderlichkeit. Eine Datenerhebung muss zur Aufgabenerfüllung der verantwortlichen Stelle stets erforderlich sein (vgl. Art. 6 Abs. 1 lit. b bis f DS-GVO).[554] Eine Datenerhebung ist nicht notwendig, wenn die Interessen auch ohne personenbezogene Informationen gewahrt werden können. Der Grundsatz ist jedoch nicht so auszulegen, dass eine Verarbeitung personenbezogener Daten absolut zwingend notwendig sein muss.[555] Jedenfalls aber folgt aus dem Kriterium der „Erforderlichkeit", dass personenbezogene Daten nicht auf Vorrat erhoben werden können. Die Erheblichkeit des Grundrechtseingriffs bemisst sich ferner danach, ob die Daten unverzüglich gelöscht werden.[556] Maßgebliche Leitlinien zur Reichweite staatlicher Datenverarbeitung gerade im Umgang mit Verkehrsdaten ergeben sich aus den strengen Vorgaben des Europäischen Gerichtshofs[557] und des Bundesverfassungsgerichts[558] zur sog. Vorratsdatenspeicherung. Der Europäische Gerichtshof hatte die maßgebliche Richtlinie[559] für ungültig erklärt, weil sie die Grundrechte aus den Artikeln 7 und 8 GRCh in unverhältnismäßigem Umfang einschränke.[560] Beide Gerichte hielten allerdings eine solche anlasslose

---

and Data Protection, Version 2.0, 2011, S. 3 ff.; vgl. *ENISA*, A flair for sharing – encouraging information exchange between CERTs, 2011, S. 12 f.

553 Vgl. zur Datensparsamkeit *Roßnagel*, DuD 1999, 253 ff.

554 *Gallwas*, Zum Prinzip der Erforderlichkeit im Datenschutzrecht, in: Haft/Hassemer/Neumann/Schild/Schroth (Hrsg.), Strafgerechtigkeit, Festschrift für A. Kaufmann, 1993, S. 819 f.

555 Vgl. *Gola*/*Schomerus*, in: dies. (Hrsg.), BDSG, 12. Aufl. 2015, § 28, Rn. 15.

556 BVerfGE 120, 378 (399).

557 EuGH, verbundene Rechtssachen C – 293/12 und C – 594/12, EuZW 2014, 459.

558 BVerfGE 125, 260.

559 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (ABl. L 105 vom 13.04. 2006, S. 54).

560 Zu unterscheiden ist diese Entscheidung vom Beschluss des BVerfG vom 24. Januar 2012 – 1 BvR 1299/05. Gegenstand der Verfassungsbeschwerde waren hier insbesondere die

Massenspeicherung der Daten nicht *per se* für rechtswidrig. Es müssen allerdings stets eng definierte Voraussetzungen zur Gewährleistung der Grundrechte und der Verhältnismäßigkeit geregelt sein. Für die Rechtmäßigkeit der Datenverarbeitung im großen Umfang kommt es darauf an, ob sie insgesamt nachteilig in der „Überwachungs-Gesamtrechnung" ist.[561] Ausgeschlossen ist danach eine Gesetzgebung zur Speicherung von Telekommunikationsverkehrsdaten, die auf eine möglichst flächendeckende vorsorgliche Speicherung für die Gefahrenprävention nützlicher Daten zielte. Der Gesetzgeber ist bei der Erwägung von Speicherungspflichten oder -berechtigungen im Hinblick auf „die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen zu größerer Zurückhaltung" gezwungen. Die Freiheitswahrnehmung der Bürger dürfe „nicht total erfasst oder registriert" werden.[562] Ausgeschlossen ist eine demnach Datensammlung, auch wenn sie ausschließlich für Zwecke der Netz- und Informationssicherheit vorgesehen wäre und nicht etwa auch für die Strafverfolgung, die im „Zusammenspiel mit anderen vorhandenen Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger" führte. Das Bundesverfassungsgericht zählt dieses Freiheitskriterium zur „verfassungsrechtlichen Identität der Bundesrepublik Deutschland". Insofern sei auch der Spielraum für „weitere anlasslose Datensammlungen über den Weg der Europäischen Union erheblich geringer".

Das Zurückhaltungsgebot für staatliche Datensammlungen, die telekommunikationsrechtliche Verkehrsdaten umfassen, gilt vorrangig für die Vorratsdatenspeicherung. Die in § 113b TKG nach den Urteilen des Europäischen Gerichtshofs und des Bundesverfassungsgerichts wieder eingeführte Vorratsdatenspeicherung ist von der Datenverarbeitung zur Gewährleistung der Sicherheit abzugrenzen. Die im Rahmen der Vorratsdatenspeicherung gespeicherten Daten unterliegen einer Verwendungsbestimmung, die es grundsätzlich ausschließt, dass die Daten systematisch von den Netz- und Informationssicherheitsbehörden eingesetzt werden. Die Verwendungsbestimmung für die gespeicherten Verkehrsdaten aus § 113c Abs. 1 TKG lässt nur zu, dass die Daten an eine Strafverfolgungsbehörde oder an eine Gefahrenabwehrbehörde der Länder übermit-

---

Verfassungsmäßigkeit der Regelungen über die Verpflichtung geschäftsmäßiger Anbieter von Telekommunikationsdiensten zur Speicherung bestimmter (Bestands-)Daten (§ 111 TKG) sowie zur Beauskunftung dieser Daten im Wege des automatisierten oder manuellen Auskunftsverfahrens (§§ 112, 113 TKG). Die Entscheidung führte zur Neuregelung der Bestandsdatenauskunft mit dem Gesetz zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft vom 20. Juni 2013, BGBl. 2013, Teil I Nr. 30, S. 1602.

[561] *Roßnagel*, NJW 2010, 1238 (1240 ff.).

[562] BVerfG, NJW 2010, 833 (839, Rn. 218).

telt werden oder durch den Erbringer öffentlich zugänglicher Telekommunikationsdienste für das manuelle Auskunftsverfahren nach § 113 TKG verwendet werden. Das manuelle Auskunftsverfahren wiederum dient der Verfolgung von Straftaten und Ordnungswidrigkeiten, der Gefahrenabwehr und der Erfüllung nachrichtendienstlicher Aufgaben. Eine Berechtigung zum Zugriff auf diese Daten ist aber nach § 113 Abs. 2 S. 1 TKG nur gegeben, wenn eine gesetzliche Bestimmung auf § 113 Abs. 1 TKG Bezug nimmt und dieser Stelle die Erhebung der Daten erlaubt.[563]

Den NIS-Behörden ist der Zugriff auf gespeicherte Vorratsdaten nicht erlaubt. Sie werden auch nicht primär zu Zwecken der Strafverfolgung aktiv. Die Datenspeicherung bei den Unternehmen, bei denen die NIS-Behörden Daten generieren, ist obligatorisch. Soweit dort auf Grundlage der Gefahrabwehrbefugnisse eine begrenzte Speicherung stattfindet, handelt es sich auch nicht um eine „weitreichende Vorratsdatenspeicherung“,[564] zumal auch dort der Zugriff von Polizeien und Strafverfolgungsbehörden nicht vorgesehen ist.[565] Den materiell-rechtlichen Sicherheitspflichten ist keine ausdrückliche Pflicht zur vollautomatisierten, anlasslosen und einzelfallunabhängigen Datenerhebung zu entnehmen. Auch wenn den Betreibern und Anbietern die Pflicht zur Netz- und Informationssicherheit nach dem Stand der Technik aufgegeben ist (§ 8a BSIG, § 109 TKG und § 13 Abs. 7 TMG), bieten die datenschutzrechtlichen Eingriffsgrundlagen (§ 100 TKG „darf“, § 15 Abs. 1 TMG „darf“) den Privaten einen Abwägungsspielraum. Die auf Grundlage dieser Vorschriften zulässige Datenspeicherung ist primär für eigene Interessen zulässig. Die Telemediendienste- und Telekommunikationsdiensteanbieter dürfen kurzfristig Nutzungs- bzw. Verkehrsdaten zur Abwehr von Gefahren für die eigene Infrastruktur speichern. Eine Vorratsdatenspeicherung ist gesetzlich nicht für diese Zwecke vorgesehen.

Bedenken unter der Leitfrage der Informationsgenerierung und Wissensproduktion sind schließlich nicht gegen die rechtliche Ausgestaltung der Datenvermeidung vorzubringen, sondern gegen das Prinzip als solches. Ungeachtet vorgebrachter Zweifel, ob Datenminimierung überhaupt ein realistisch erreichbares Ziel moderner Regulierung sein kann,[566] stellt sich die Kontrollfrage nach

---

[563] Z. B. § 22 BKAG; *Graf*, in: ders. (Hrsg.), BeckOK StPO, 23. Ed. 2015, TKG, § 113 Rn. 13; zur Erkennung anderer rechtswidriger Nutzungen und von Missbräuchen wie Leistungserschleichung durch sog. Fraud-Detection-Systeme bedarf es der Erlaubnistatbestände im Sinne des § 100 Abs. 3 und 4 TKG. Siehe dazu *Schuster*/*Sassenberg*, CR 2011, 15 (17 f.).

[564] So aber Empfehlungen der Ausschüsse im Bundesrat zum Entwurf eines IT-Sicherheitsgesetzes, BR-Drs. 643/1/14, S. 11.

[565] Vgl. *Lutz*, in: Arndt/Fetzer/Scherer/Graulich (Hrsg.), TKG, 2. Aufl. 2015, § 100 Rn. 32.

[566] *Härting*, Datenschutz im 21. Jahrhundert, in: ders., Internetrecht, 2014, Annex, Rn. 44; vgl. *Simitis*, in: ders. (Hrsg.), BDSG, 8. Aufl. 2014, § 4 Rn. 23.

den epistemischen Implikationen dieses datenschutzrechtlichen Prinzips. Die Datenminimierung führt zu einer Informationsminimierung und potenziell zu einer Wissensminimierung. Die Reduzierung von Datenmengen kann erkenntnishemmend wirken, da der Überraschungswert, der sich aus der Informationsverarbeitung ergibt, grundsätzlich geringer als bei großen Datenmengen ist. Informationswerte, die über das bereits Bekannte hinausgehen, sind bei der Auswertung von kleinen Datenmengen geringer als bei großen Datenmengen.[567] Kleinere Datenmengen erfordern mehr Wissen darüber, was gesucht wird, d. h. der Fund muss besser antizipiert werden. Aus Datenmengen, die eine größere Anzahl an Verknüpfungsmöglichkeiten zulassen, können grundsätzlich eher Mehrwerte, die durch nicht vorhersehbare Korrelationen entstehen, generiert werden, als aus solchen mit einer geringeren Daten- und Informationsdichte und damit weniger Verknüpfungsmöglichkeiten. Wissensgenerierungsprozesse sind aber auf eine hohe (maschinelle) Assoziationsfähigkeit angewiesen.[568] Sollen die Gefahren ungewünschter, den Einzelnen in seinen Persönlichkeitsrechten treffender Profilbildungen vermieden werden, müssen die Verwaltung wie die Unternehmen Anonymisierungs- und Pseudonymisierungstechniken einsetzen, die einen möglichst schonenden Ausgleich der epistemischen Bedürfnisse der NIS-Verwaltung mit den Belangen des Datenschutzes begünstigen.

cc) Zweckbindung und Regelungstiefe

Aus dem allgemeinen Datenschutzrecht ergibt sich zunächst für die Datenverarbeitung der allgemeine Grundsatz der Zweckbindung. Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden (vgl. Art. 5 Abs. 1 lit. b DS-GVO).[569] Die Zweckbindung soll sicherstellen, dass die Daten nur für den Zweck verarbeitet werden, für den sie erhoben worden sind (sog. Zweckidentität).[570] Erforderlich ist für die Datenerhebung demnach eine erkennbare Zielsetzung. Aufgrund fehlender bereichsspezifischer Datenschutzregelungen in der NIS-RL als auch in den einfachgesetzli-

---

[567] Vgl. *Tene*/*Polonetsky*, Big Data for All: Privacy and User Control in the Age of Analytics, 11 Nw. J. Tech. & Intell. Prop. 239 (2013), 239 (259 ff.).

[568] Vgl. *Ladeur*, Die Kommunikationsinfrastruktur der Verwaltung, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. II, 2. Aufl. 2012, § 24, Rn. 41.

[569] Vgl. BVerfGE 95, 1 (45): „Die Verwendung der Daten ist auf den gesetzlich bestimmten Zweck begrenzt."

[570] *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl. 2015, § 14 Rn. 9.

chen Rechtsgrundlagen für die behördliche Datenerhebung im BSIG, TKG oder im TMG, mangelt es an einer expliziten, präzisen Zweckbestimmung.[571]

Das Gebot der präzisen Festlegung der Verwendungszwecke schließt aber eine weite Fassung der Zweckbestimmung nicht aus. Bereits das Volkszählungsgesetz, das Gegenstand des Volkszählungsurteils des Bundesverfassungsgerichts war, fasste den Zweck der Datenerhebung notwendig weit, da mit dem Gesetz eine Datenerhebung zu statistischen Zwecken beabsichtigt war. Es gehört zum Wesen der Statistik, dass die Daten nicht für eine *a priori* festgelegte Aufgabe verwendet werden.[572] Ähnlich verhält sich die Datenverarbeitung zu wissenschaftlichen Zwecken, die sich ob der möglichst offenen Forschungsergebnisse nicht vorab durch enge Zwecke binden lässt. Das Bundesverfassungsgericht erkannte deshalb sogar das Bedürfnis nach der Vorratsdatenspeicherung an.[573] Lediglich eine zweckfreie Datenverarbeitung wäre von vorneherein verfassungsrechtlich unzulässig. Hingegen dürfte es unschädlich sein, wenn der (eindeutige) Zweck indirekt ermittelbar ist. Das Bundesverfassungsgericht lässt zumindest für die Anforderung an die Normenklarheit genügen, dass der Gesetzeszweck in Verbindung mit den Gesetzgebungsmaterialien deutlich wird, wobei es ausreicht, dass sich der Gesetzeszweck aus dem Zusammenhang ergibt, „in dem der Text des Gesetzes zu dem zu regelnden Lebensbereich steht".[574]

Die Datenschutz-Grundverordnung macht nunmehr in Art. 6 Abs. 3 UAbs. 2 S. 1, wenn auch sprachlich unglücklich, deutlich, dass der Zweck für Datenverarbeitungen, die auf Art. 6 Abs. 1 UAbs. 1 lit. c und e gestützt werden, nicht notwendig festgelegt sein muss, sondern dass er sich aus dem Kontext der betimmten Aufgabe ergeben kann, die erfüllt wird.[575]

Die Ermittlung des Zwecks der Datenverarbeitung erfordert mithin eine Gesamtbetrachtung des europäischen und nationalen NIS-Rechts. Der Zweck der etwaigen Verarbeitung personenbezogener Daten lässt sich den in der NIS-RL zugewiesenen Aufgaben der NIS-Akteure entnehmen. Zwar verpflichtet Art. 8 NIS-RL die Mitgliedstaaten lediglich dazu, die „für die Sicherheit von Netz- und Informationssystemen zuständige nationale Behörden" zu benennen. Gemäß Art. 8 Abs. 2 überwachen sie die Anwendung der Richtlinie auf nationaler Ebene. Aus den weiteren in der NIS-RL statuierten Aufgabenzuweisungen in Art. 15 und 17 NIS-RL ergibt sich jedoch, dass die NIS-Behörden die Sicherheit

---

[571] Vgl. aber im Rahmen des Schutzes des Fernmeldegeheimnisses die Begrenzung des § 88 Abs. 3 S. 2 TKG.

[572] *Härting*, NJW 2015, 3284 (3284 f.).

[573] BVerfGE 65, 1 (46, Rn. 166).

[574] BVerfGE 65, 1 (53).

[575] *Frenzel*, in: Paal/Pauly, DS-GVO, 2017, Art. 6 Rn. 41.

der Netz- und Informationssysteme bewerten und beurteilen. Diese Aufgabe ist an die spezifische Definition der Schutzziele der Sicherheit von Netzen und Informationssystemen gebunden.[576] Die Datenverarbeitung ist damit auf die Beurteilung der Gefahr der Verfügbarkeit, Vertraulichkeit und Integrität von Netzen und Informationssystemen begrenzt. Ebenso lässt sich für die CSIRTs der Zweck einer Verarbeitung personenbezogener Daten ermitteln. Diese sind für die „Bewältigung von Risiken und Vorfällen" zuständig. Das Aufgabenprofil wird unter Punkt 2 des Anhangs I der NIS-RL näher spezifiziert. Im Schwerpunkt hat ein CSIRT die Sicherheitsvorfälle auf nationaler Ebene zu überwachen und zu analysieren, Frühwarnungen auszugeben und Informationen über Risiken und Vorfälle zu verbreiten und bekanntzugeben sowie auf Risiken zu analysieren. Die Anknüpfungspunkte Sicherheitsvorfall und Risiko sind durch die Definition in Art. 4 Nr. 7 und Nr. 9 NIS-RL ebenfalls rechtlich begrenzt. Daraus lässt sich ableiten, dass das CSIRT Erkenntnisse über Umstände und Ereignisse zu generieren hat, um nachteilige Auswirkungen für die Sicherheit zu ermitteln. Die Erhebung personenbezogener Daten führt über keine Aufgabenzuweisung zu einer operativen Befugnis der genannten NIS-Akteure. Die Datenverarbeitung zum Zwecke der Netz- und Informationssicherheit ist nicht auf Repression oder Verhaltenssteuerung angelegt. Soweit den Akteuren die Aufgabe eines Informationsaustausches in der Kooperationsgruppe (Art. 11 NIS-RL) oder dem CSIRTs-Netzwerk (Art. 12 NIS-RL) zugewiesen ist, stellt der Datenaustausch mit anderen Behörden und Stellen eine selbstständige Verarbeitungsstufe dar, weshalb sich die datenschutzrechtliche Rechtmäßigkeit dort nach der Zulässigkeit einer Zweckänderung bemisst.[577]

Problematisch ist hingegen, wie sich die gemäß Art. 8 Abs. 6 NIS-RL mögliche Zusammenarbeit mit nationalen Strafverfolgungsbehörden zur Zweckermittlung verhält. Gemäß Art. 8 Abs. 6 NIS-RL „konsultieren" die NIS-Behörden mit den zuständigen nationalen Strafverfolgungsbehörden. Aus Erwägungsgrund 62 der NIS-RL ergibt sich, dass die Zusammenarbeit der NIS-Behörden mit den Strafverfolgungsbehörden dazu dient, strafrechtlich relevante Handlungen, die zu Sicherheitsvorfällen geführt haben, zu ermitteln, aufzuklären und zu verfolgen. Allerdings ergibt sich aus Art. 8 Abs. 6 NIS-RL unmittelbar, dass die zuständigen NIS-Behörden „nach Maßgabe des nationalen Rechts" mit den Strafverfolgungsbehörden zusammenarbeiten.

Nach deutschem Datenschutzrecht ist eine Übermittlung personenbezogener Daten nicht unzulässig. Gemäß § 15 Abs. 1 Nr. 1 BDSG ist die Übermittlung

---

[576] Siehe § 2 A.

[577] Siehe zu den datenschutzrechtlichen Grenzen für den Transfer von Informationen über die Sicherheit von Netzen und Informationssystemen § 4 D. I.

durch öffentliche Stellen zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten, an den die Daten übermittelt werden, liegenden Aufgaben erforderlich ist. Keine andere Wertung ergibt sich aus Art. 6 Abs. 3 DS-GVO. Den NIS-Behörden ist keine originäre Aufgabe zur Strafverfolgung zugewiesen. Insofern ist die Übermittlung von Daten daran gebunden, dass die empfangende Stelle eine öffentliche Aufgabe wahrnimmt. Diese ist separat zu ermitteln und bedarf einer eigenen Zweckprüfung. Eine Gefahr der Umgehung des formalisierten Strafprozessrechts ist demnach nicht zu befürchten. Das BSI unterstützt Strafverfolgungsbehörden gemäß § 3 Abs. 1 S. 2 Nr. 13 BSI auch nur auf Anforderung. Sollten in diesem Rahmen personenbezogene Daten übermittelt werden, wären die Voraussetzungen einer eigenständigen Verarbeitungsphase zu prüfen.

Es kann damit festgehalten werden, dass sich aus dem NIS-Recht der Zweck einer etwaigen Verarbeitung personenbezogener Daten ermitteln lässt und ein Schutz vor Zweckentfremdung grundsätzlich besteht. Die etwaig verarbeiteten personenbezogenen Daten dürfen zum technisch-analytischen Zwecke der Netz- und Informationssicherheit verwertet werden.

Mit Blick auf die Ausnahmen von der Anwendung der Datenschutz-Grundverordnung und der den Mitgliedstaaten eröffneten Möglichkeit, die Datenverarbeitung im öffentlichen Interesse oder durch öffentliche Stellen mittels spezifischerer Regelungen auszugestalten (Art. 6 Abs. 2 DS-GVO), stellt sich die Frage nach weitergehenden Datenschutzregelungen für den Bereich der Netz- und Informationssicherheit für die nationale Ebene. Bereichsspezifischer Regelungen bedürfte es insbesondere bei besonderen verfassungsrechtlichen Anforderungen an die Regelungstiefe des Datenschutzes.

Das Bedürfnis nach einem Datenschutz im Bereich der Netz- und Informationssicherheit mit einer besonderen Regelungsdichte könnte aus der hohen Eingriffsintensität folgen, die sich bei sicherheitsrechtlichen Maßnahmen wie Vorratsdatenspeicherung, Rasterfahndungen[578] oder automatisiertrn Kennzeichenerfassung[579] durch die Verdachtslosigkeit und die damit erhöhte Streubreite erfasster Daten ergibt. Die Datenverarbeitung zur Gewährleistung der Netz- und Informationssicherheit ist grundsätzlich nicht an Verdachtsstufen gebunden.

Aus dem Sicherheitsrecht ist für das Verhältnis von Generalbefugnis zur Spezialermächtigung das Regelungsprinzip bekannt, nach dem sich die Anforderungen an die Bestimmtheit und Klarheit der Eingriffsgrundlage nach dem Schweregrad des möglichen Grundrechtseingriffs bestimmen.[580] Das Erfordernis spe-

[578] BVerfGE 115, 320 (354).

[579] BVerfGE 120, 378 (398 f.).

[580] *Gola*/*Klug*/*Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl. 2015, § 13 Rn. 2; vgl. BVerfG, NVwZ 2007, 688 (690).

zialgesetzlicher Regelungen könnte aus dem qualifizierten Parlamentsvorbehalt im Datenschutz folgen. Im Volkszählungsurteil des Bundesverfassungsgerichts war mit dem Erfordernis einer formell-gesetzlichen Rechtsgrundlage[581] die Idee verbunden, den informationellen Datenumgang des Staates unter Rechtfertigungszwang zu setzen. Der qualifiziertere Gesetzesvorbehalt erfordert nicht nur eine Regelung des bloßen „Ob", sondern auch des „Wie" der Datenverarbeitung. Die Normierungspflicht betrifft sowohl die Frage, „ob ein bestimmter Gegenstand überhaupt gesetzlich geregelt sein muss, als auch, wie weit diese Regelungen im Einzelnen zu gehen haben".[582] Der Grad der Bestimmtheit bemisst sich nach dem zu schützenden Rechtsgut und der Art und Schwere seiner Gefährdung. Die Bestimmtheit einer Norm ist Bezugspunkt für die Eignung, Erforderlichkeit und Angemessenheit der Ermächtigung.[583] Neben der Einhaltung des Gebots der Normbestimmheit verlangt das Gericht das Einhalten des Gebots der Normenklarheit.[584] Normenklarheit zielt darauf, dass der Gehalt einer Regelung erkennbar, nachvollziehbar und verständlich und somit anwendungsfreundlich ist. Der Normadressat muss die Rechtslage anhand der Regelung so erfassen können, dass er sein Verhalten an ihr auszurichten vermag.[585] Das Gebot der Normenbestimmtheit zielt darauf, dass der Gesetzgeber dafür Sorge trägt, „dass das Notwendige geschieht".[586] Umgekehrt steigen aber die Anforderungen an die Regelungsdichte mit der Intensität des Grundrechtseingriffs, sodass gleichzeitig die Handlungsspielräume der Exekutive abnehmen. Die Anforderungen an die Normenbestimmtheit sind insbesondere im Sicherheitsrecht konkretisiert worden. Dem Europäischen Gerichtshof lässt sich in seiner Rechtsprechung zur Vorratsdatenspeicherungsrichtlinie die Forderung nach Verrechtlichung entnehmen. Im Sinne eines unionsrechtlichen Parlamentsvorbehalts und der grundrechtlichen Wesentlichkeitslehre des Bundesverfassungsgerichts[587] ist die Forderung zu verstehen, dass der europäische Gesetzgeber „klare und präzise Regeln" aufstellt, sodass die Personen „über ausreichend Garantien verfügen", die einen wirksamen Schutz vor Missbrauchsrisiken ermöglichen.[588]

Die Besinnung auf den Kontext, aus dem der datenschutzrechtliche Parlamentsvorbehalt stammt, macht indessen deutlich, dass allgemeine datenschutz-

---

[581] BVerfGE 64, 1 (43 f.).

[582] BVerfGE 101, 1 (34).

[583] BVerfGE 120, S. 378 (408).

[584] BVerfGE 65, 1 (43, 46).

[585] BVerfGE 110, 33 (64).

[586] BVerfGE 65, 1 (59).

[587] BVerfGE 61, 260 (275); *Pieroth/Schlink/Kingreen/Poscher*, Grundrechte, Staatsrecht II, 31. Aufl. 2015, Rn. 271 ff.

[588] EuGH, verb. Rs. C-293/12 u. C-594/12, Rn. 54.; dazu *Kühling* NVwZ 2014, 681 (684).

rechtliche Schutzbestimmungen das Gebot der Normenbestimmtheit erfüllen können. Das Bundesverfassungsgericht hatte im Volkszählungsurteil über die Erhebung von Daten zu entscheiden, die staatliche, statistisch-planerische Steuerungszwecke erfüllen sollten. Die gesetzliche Konkretisierung ist hier Ausprägung des Verhältnismäßigkeitsprinzips und bezieht sich spezifisch auf einen legislativen Zweckschutz. Bestimmt werden soll demnach vor allem der „bereichsspezifische" Verwendungszweck. Es soll ein Schutz vor Zweckentfremdungen bestehen.[589] Eine weiter gehende bereichsspezifische Regelung war nicht geboten.

Ein ausdifferenzierter Grundrechtsschutz durch Verfahren mittels Informations-, Auskunfts- und Löschpflichten und ein organisatorisch-institutioneller Schutz durch eine unabhängige Datenschutzbeauftragte genügen dem legislativen Erfordernis.[590] Letzte Anforderungen werden mit der Anwendung des allgemeinen Datenschutzrechts in der NIS-Verwaltung erfüllt. Außerdem entsteht Rechtsklarheit gerade auch dann, wenn die Normen nicht übermäßig komplex formuliert und in der Konstruktion wenig verschachtelt sind sowie wenige Verweisungen enthalten.

Im Übrigen ist eine Verdichtung der datenschutzrechtlichen Bestimmungen ungeachtet der zahlreichen Öffnungsklauseln in der DS-GVO für den Bereich der Gewährleistung der Netz- und Informationssicherheit auch nicht notwendig sinnvoll. Die Entwicklung in Referenzgebieten, in denen bereichsspezifische Sonderregelungen zum Datenschutz eingeführt wurden, weist darauf hin, dass es aufgrund hypertropher Überregulierung zu einem Vollzugsdefizit kommen kann und dem Datenschutz letztlich nicht gedient ist.[591] Diese Beobachtung bettet sich ein in die allgemein für das klassische Ordnungsrecht zu konstatierende Tendenz, die Steuerungsfähigkeit durch allzu dichte Regeln zu reduzieren.[592] Diese „Verrechtlichungsfalle" kann auch im Datenschutzrecht drohen, zumal die Zentrifugaltendenzen im Datenschutzrecht durch zahlreiche Öffnungsklauseln nicht gänzlich eingehegt sind.

Soweit ein Verfassungsauftrag für einen sektorspezifischen Umgang mit personenbeziehbaren Daten außerhalb der Datenverarbeitung zur Gefahrenabwehr und Strafverfolgung aus dem Gefährdungsgrad und der Sensibilität abgeleitet wird,[593] ist für die NIS-Verwaltung entgegenzuhalten, dass die Sensibilität der

---

[589] BVerfGE 65, 1 (46).

[590] Vgl. *Petersen*, Grenzen des Verrechtlichungsgebotes im Datenschutz, 2000, S. 113.

[591] *Kingreen/Kühling*, JZ 2015, 213 (214) mit einer Problemskizze am Beispiel des Gesundheitsdatenschutzrechts; am Beispiel des Telemediengesetzes *Kühling/Sivridis/Schuchow/Burghardt*, DuD 2009, 335 ff.

[592] *Voßkuhle*, Neue Verwaltungsrechtswissenschaft, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band I, 2. Aufl. 2012, § 1 Rn. 10.

[593] BSGE 102, 134 (144 f.) mit Blick auf §§ 284 ff. SGB V und der Folgerung, dass auf-

Daten im Rahmen der allgemeinen Regelungen angemessen berücksichtigt werden kann. Den bereichsspezifischen Risiken der Datenverarbeitung kann mit einer präzisen Anwendung des Verhältnismäßigkeitsgrundsatzes begegnet werden.[594] Die Informationsverarbeitung der NIS-Behörden ist zuletzt nicht mit sicherheitsrechtlichen Maßnahmen wie Vorratsdatenspeicherung, Rasterfahndungen oder der automatisierten Kennzeichenerfassung zu vergleichen. So knüpft etwa die IT-Meldepflicht wie die genannten Maßnahmen nicht an ein vorwerfbares Verhalten des Einzelnen an, sondern an bestimmte, bei privaten Unternehmen detektierte Anomalien und Störungen. Die Informationen fließen den Behörden anlassbezogen und infolge konkreter Situationen zu. Es ist ein Unterschied, ob Logdateien aus Systemen und Netzwerken gesammelt und ausgewertet werden oder ob personenbezogene Daten systematisch (mit anderen personenbezogenen Daten) abgeglichen werden. Ein solches Screening,[595] Data Mining[596] oder Einrichten eines Data Warehouse[597] ist nicht Zweck der Informationsgenerierung der zuständigen NIS-Behörden.[598]

Datenschutzrechtliche Spezialregelungen sind nach allem für den ermittelten Zweck der Datenverarbeitung weder erforderlich noch hilfreich, wenn es um die Begrenzung der administrativen Informationsgenerierung geht.

III. Besondere Grenzen der Informationsgenerierung zum Schutz von Unternehmensgeheimnissen

Unternehmen haben grundsätzlich Interesse am Schutz sicherheitssensibler Unternehmensinformationen (1.). Betriebs- und Geschäftsgeheimnisse können grundrechtlich geschützt sein. Für Betreiber kritischer Infrastrukturen besteht im Rahmen der Meldepflicht durch das abgestufte Meldeverfahren ein besonderer Schutz (2.). Der Eingriff in geschützte Geheimnisse wird insbesondere durch den Schutz des Verwaltungsgeheimnisses gerechtfertigt (3.).

---

grund bestehender punktueller Regelungen zur Datenweitergabe ausschließlich Spezialregelungen anzuwenden sind und sich ein Rückgriff auf die allgemeinen Regelungen verbiete.

[594] Vgl. zum Erfordernis bereichsspezifischer Reglungen bei überdurchschnittlichen Eingriffen und zur „Schwellentheorie" *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, S. 55 (Fn. 163).

[595] Solche Screenings werden in Unternehmen zur Prävention von Korruption und Compliance-Verletzungen sowie repressiv zur Straftatenverfolgung eingesetzt. Dazu *Brink/Schmidt*, MMR 2010, 592 (592).

[596] *Heinson*, BB 2010, 3084 (3084).

[597] *Dammann*, in: Simitis (Hrsg.), BDSG, 8. Aufl. 2014, § 3 Rn. 72.

[598] Zur Datenverarbeitung der Nachrichtendienste außerhalb des Anwendungsbereichs der NIS-Richtlinie § 3 D. II. 3.

1. Schutzbedarf von Unternehmensinformationen

Die Informationsgewinnung durch öffentliche Stellen steht mit schutzwürdigen und zu berücksichtigenden Unternehmensgeheimnissen in einem Spannungsverhältnis. Da Gegenstand datenschutzrechtlicher Diskussionen häufig personenbezogene Daten sind, wurde der Schutz unternehmensbezogener Daten dagegen „bisher kaum diskutiert oder gar rechtlich durchdrungen".[599] Während dem Schutz personenbezogener Daten eine menschenrechtliche Bedeutung zukommt, weil das Recht auf informationelle Selbstbestimmung in den Persönlichkeitsrechten des Einzelnen verwurzelt ist, folgt das Spannungsverhältnis von Informationsgewinnung und Unternehmensinformationen aus der wirtschaftlichen Bedeutung von Daten. Auch wenn für Unternehmen kein Persönlichkeitsrecht anerkannt wird,[600] können sie dennoch ein schutzbedürftiges Geheimhaltungsinteresse haben.[601] Der Umgang mit solchen Daten hat für Unternehmen sowohl großen direkten Wert (Daten sind Gegenstand von Geschäften oder immaterielle Vermögenswerte und ihr Wert lässt sich bemessen) als auch indirekten Wert (Daten und Informationen können wettbewerbsrelevant sein und dem Unternehmen Vorsprünge verschaffen). Das Schutzbedürfnis von Unternehmen folgt aus der Befürchtung, ein Wettbewerber könnte unbotmäßig Kenntnis von einem Umstand erlangen. Das Bedürfnis nach informationellem Schutz ist nicht von vorneherein dadurch aufgehoben, dass es sich bei der Sicherheitsverwaltung um eine Datenverarbeitung öffentlicher Stellen handelt.

2. Der öffentlich-rechtliche Schutz von Unternehmensinformationen bei Bestehen von Informationspflichten in der NIS-Verwaltung

Die Feststellung, dass Betreiber von Netzinfrastrukturen und Anbieter von Internetdiensten ein Geheimhaltungsinteresse an den ihre Netz- und Informationssicherheit betreffenden Informationen haben und dass Informationen daher grundsätzlich öffentlich-rechtlich geschützte Unternehmensgeheimnisse darstellen, impliziert noch nicht, dass die Informationsgenerierung öffentlicher Stellen diese Geheimnisse gefährdet. Da die Verwaltung grundsätzlich nicht im

---

[599] So *Stancke*, BB 2013, 1418 (1418).

[600] Im Ergebnis offengelassen durch BVerfG, NJW 2010, 3501 (3502). Zum Unternehmenspersönlichkeitsrecht und der geschützten „Unternehmensehre" siehe BGH, NJW 2008, 2110 (2111).

[601] *Holznagel*, Informationsbeziehungen in und zwischen Behörden, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band II, 2. Aufl. 2012, § 24 Rn. 69; vgl. für die durch das IT-Sicherheitsgesetz eingeführte Meldepflicht *Böcking*, Geplante Meldepflicht: Firmen verweigern direkte Auskunft über Cyberangriffe, Spiegel Online vom 19.08.2014, online abrufbar.

Wettbewerb mit Unternehmen steht, kann argumentiert werden, dass eine Gefährdung erst mit der Weitergabe von geschützten Informationen an die Öffentlichkeit oder andere öffentliche Stellen oder an andere Unternehmen besteht. Zu untersuchen ist daher die Ausgestaltung des Schutzes von Informationen in der NIS-Verwaltung. Dabei zeigt sich, dass das Datenschutzrecht nicht anwendbar ist und damit ein im Vergleich zu personenbezogenen Daten weniger ausdifferenziertes Schutzregime besteht (a). Gleichwohl besteht ein grundrechtlich gewährleisteter Schutz von Betriebs- und Geschäftsgeheimnissen, wobei die aufgrund von Meldepflichten gemeldeten Daten grundsätzlich keine geschützten Geheimnisse darstellen. Dennoch bestehen besondere Schutzmechanismen für die Meldungen von Betreibern kritischer Infrastrukturen (b). Die Angemessenheit des etwaigen Eingriffs durch administrative Informationsgenerierung wird insbesondere durch das Verwaltungsgeheimnis gewahrt (c).

a) Keine Anwendbarkeit des Datenschutzrechts auf juristische Personen

Juristische Personen des Privatrechts sind Träger von europäischen und deutschen Grundrechten. Die Dogmatik hinsichtlich der in Betracht kommenden Grundrechte entspricht grundsätzlich dem im deutschen Recht angewendeten Prinzip. Grundrechtlicher Schutz kommt juristischen Personen zu, soweit das Grundrecht dem Wesen nach anwendbar ist. In Betracht kommt daher, dass das natürliche Personen schützende Datenschutzrecht auch auf juristische Personen Anwendung findet.

Gemäß Art. 8 Abs. 1 GRCh hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Dem Wortlaut nach differenziert das Grundrecht nicht zwischen natürlichen und juristischen Personen („jede Person“).[602] Da der Rechtsbegriff der Person nicht weiter eingeschränkt ist, ist die Schlussfolgerung, den Schutzbereich auf juristische Personen zu erstrecken, keinesfalls fernliegend.[603]

Für die Erstreckung des Datenschutzrechts auf Daten juristischer Personen spricht, dass sich auch juristische Personen auf Art. 8 Abs. 1 EMRK berufen können. Dort erstreckt sich der Schutz auf berufliche und geschäftliche Tätigkeiten.[604] Über Art. 52 Abs. 3 GRCh wird kein Grundrecht verdrängt, da das Grundrecht in Art. 8 Abs. 1 EMRK insoweit bereichsspezifische Aussagen über

---

[602] Anders hingegen in Art. 42 und 44 GRCh.

[603] *Kingreen*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, 4. Aufl. 2011, GRCh, Art. 8 Rn. 11; dafür *Streinz*, in: ders. (Hrsg.), EUV/AEUV, 2. Aufl. 2012, GRCh, Art. 8 Rn. 7; vgl. *Heußner*, Informationssysteme im Europäischen Verwaltungsverbund, 2007, S. 320 ff.

[604] Vgl. EGMR, Urteil vom 16.12.1992, Serie A, Nr. 251-B, §§ 29 bis 31; Urteil vom 16. April 2002, Reports of Judgements and Decisions 2002-III, § 41 und Urteil vom 28. Januar 2003, Reports of Judgements and Decisions 2003-I, Nr. 44647/98, § 57.

den Datenschutz und grenzüberschreitende Datenflüsse enthält.[605] Daher bietet Art. 8 EMRK wichtige Anhaltspunkte für die konkretisierende Auslegung von Art. 8 GRCh.[606] In binnensystematischer Sicht ist das Datenschutzgrundrecht bei den die „Freiheit" schützenden Grundrechten zu verorten und nicht in Art. 1 bis 6 GRCh, die den „Menschen" schützen.[607] Eine Beschränkung des Datenschutzes auf natürliche Person schreibt die RL 95/46/EG nicht vor, im Gegenteil lässt sie in diesem Bereich einen Umsetzungsspielraum, von dem einige Mitgliedstaaten sogar Gebrauch gemacht haben.[608]

Der Vergleich von Art. 8 GRCh mit der gleichlaufenden Gewährleistung in Art. 16 AEUV weist hingegen auf eine Beschränkung des personalen Schutzbereichs auf natürliche Personen hin. Die Gesetzgebungskompetenz in Art. 16 Abs. 2 AEUV erkennt einen unternehmens- bzw. organisationsbezogenen Datenschutz nicht an.

Die gerichtliche Auslegung des Datenschutzrechts hält an der herkömmlichen, auf natürliche Personen beschränkten Konzeption im Grundsatz fest. In den vom Europäischen Gerichtshof entschiedenen Fällen wiesen die verfahrensgegenständlichen Geschäftsinformationen zwar jeweils einen konkreten Bezug zu natürlichen Personen auf, aber auch sonst ist die Rechtsprechung des Gerichts restriktiv im Vergleich zur expansiven Rechtsprechung über die sonstigen europäischen Datenschutzbestimmungen.[609] Juristische Personen können sich nach der Rechtsprechung auf Art. 7 und 8 GRCh nur berufen, „soweit der Name der juristischen Person eine oder mehrere natürliche Personen bestimmt".[610] Die Verletzung des Rechts auf Schutz personenbezogener Daten habe nämlich bei juristischen Personen ein anderes Gewicht als bei natürlichen Personen.[611] Die Begründung stützt sich jedoch nicht auf das deutliche Spannungsverhältnis von Art. 8 GRCh zu Art. 16 Abs. 2 AEUV. Das Gericht zieht als Beurteilungsmaßstab die Trennung von natürlichen und juristischen Personen heran, obwohl eine

---

[605] *Meyer*, in: ders. (Hrsg.), Charta der Grundrechte der Europäischen Union, 4. Aufl. 2014, Art. 8 Rn. 19.

[606] Vgl. *Britz*, EuGRZ 2009, 1 (6).

[607] *Guckelberger*, EuZW 2011, 126 (128).

[608] Vgl. für Österreich § 4 Nr. 3, für Dänemark Kap. 2 Nr. 4 und für Luxemburg Art. 2 d) der jeweiligen Datenschutzgesetze. Siehe auch *Guckelberger*, EuZW 2011, 126 (128); *Gola*/*Klug*/*Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl. 2015, § 3 Rn. 11; siehe aber Art. 1 Abs. 2 DS-GVO.

[609] Dazu *Schneider*, Die Verwaltung 44 (2011), 499 (507).

[610] EuGH, Urteil vom 09.11.2010, C-92/09 u. a., Rn. 53. Regelungen einer Agrarfondsverordnung sahen aus Transparenzgründen die namentliche Veröffentlichung von Zuwendungsempfängern und zugewendeten Summen vor, ohne Datenschutzinteressen natürlicher oder juristischer Personen zu unterscheiden.

[611] EuGH, C-92/09 u. a., Rn. 87.

konkrete Betrachtung des Schutzgutes geboten wäre. Eine Graduierung des Schutzniveaus und die dogmatische Verknüpfung mit der Menschenwürde ist durch die soziale Relevanz von auf Personen bezogenen Daten naheliegend. Den personalen Schutzbedarf hätte das Gericht aber ebenso im Rahmen der Rechtfertigung berücksichtigen können. Das Datenschutzrecht betrifft also lediglich den Schutz personenbezogener Daten und ist auf unternehmensbezogene Daten nicht anwendbar.

Im Ergebnis führt dies zu einem strukturell abgeschwächten Schutz für Unternehmensgeheimnisse. Der Schutz personenbezogener Daten wird ungeachtet dessen gewährleistet, ob sie geheim und vertraulich sind. Dagegen sind geschäftliche Informationen außerhalb der Geheimhaltung nicht Gegenstand eines Schutzregimes. Der Geheimnisschutz stellt nicht auf die Dichotomie von personen- und nicht personenbezogenen Daten ab, sondern auf das berechtigt schützenswerte Geheimnis. Personenbezogene Daten können durch beide Schutzrechte erfasst werden. Als speziellere Regelung geht im Falle dieser doppelt geschützten Schnittmenge der Datenschutz vor.[612]

b) Schutz von Betriebs- und Geschäftsgeheimnissen

Da das Datenschutzrecht nicht für juristische Personen Anwendung findet, besteht kein umfassend kodifizierter Schutz für unternehmensbezogene Daten.[613] Dem Schutzbedürfnis wird in rechtlicher Hinsicht gleichwohl für die Beziehung von Unternehmen zueinander als auch im Verhältnis der Unternehmen zum Staat Rechnung getragen. Unter zivilrechtlichen Gesichtspunkten geht es um den Schutz von Betriebs- und Geschäftsgeheimnissen. Im Öffentlichen Recht kann geheimen Informationen eine subjektiv-rechtlich geschützte Rechtsposition zukommen. Hier geht es um die Abwehr von Eingriffen und den Schutz vor der Offenbarung, also der Weitergabe an Dritte, folglich um Geheimnisschutz bzw. Geheimhaltung.[614]

aa) Herleitung des Schutzes

Die dogmatische Verortung und die Reichweite des Schutzbereichs des Unternehmensdatenschutzes sind nicht eindeutig geklärt. Für die Begründung des Geheimnisschutzes kommen verschiedene Begründungsansätze in Betracht.

In Betracht kommt, den Schutz unternehmensbezogener Daten mit der Eigentumsgarantie aus Art. 17 GRCh bzw. Art. 14 Abs. 1 GG oder der Berufsfreiheit

---

612 *Kloepfer*, Informationsrecht, 2002, § 9 Rn. 5.

613 Dazu *Stancke*, BB 2013, 1418 (1419).

614 *Von Lewinski*, Die Matrix des Datenschutzes, 2014, S. 11 f.

aus Art. 15 GRCh bzw. 12 Abs. 1 GG zu verbinden.[615] Die Anwendung der Grundrechte auf juristische Personen ist anerkannt.

Der Europäische Gerichtshof zitiert Art. 15, 16 und 17 GRCh in einem Zusammenhang und stellt zusätzlich fest, dass der Schutz von Geschäftsgeheimnissen ein allgemeiner Grundsatz des Unionsrechts ist.[616] Demnach ist der Geheimnisbegriff für die Reichweite des Schutzes von besonderer Bedeutung.[617] Das Europäische Gericht leitet aus der „Natur von Geschäftsgeheimnissen" die Voraussetzung ab, dass diese oder vertrauliche Informationen nur einer beschränkten Zahl von Personen bekannt sind, dass es sich um Informationen handelt, durch deren Offenlegung dem Offenbarenden oder Dritten ein ernsthafter Nachteil entstehen kann, und schließlich, dass die Interessen, die durch die Offenlegung der Information verletzt werden können, schützenswert sind.[618] Bei der Beurteilung der Vertraulichkeit einer Information sollen die berechtigten individuellen Interessen, die mit ihrer Offenlegung in Konflikt stehen, und das entgegenstehende Interesse zum Ausgleich gebracht werden.[619]

Das Bundesverfassungsgericht sieht den Schutz der Betriebs- und Geschäftsgeheimnisse über Art. 12 GG gewährleistet.[620] Betriebs- und Geschäftsgeheimnisse sind nach der Rechtsprechung des Bundesverfassungsgerichts „alle auf ein Unternehmen bezogene Tatsachen, Umstände und Vorgänge […], die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Nichtverbreitung der Rechtsträger ein berechtigtes Interesse hat. Betriebsgeheimnisse umfassen im Wesentlichen technisches Wissen im weitesten Sinne; Geschäftsgeheimnisse betreffen vornehmlich kaufmännisches Wissen. Zu derartigen Geheimnissen werden etwa Umsätze, Ertragslagen, Geschäftsbücher, Kundenlisten, Bezugsquellen, Konditionen, Marktstrategien, Unterlagen zur Kreditwürdigkeit, Kalkulationsunterlagen, Patentanmeldungen und sonstige Entwicklungs- und Forschungsprojekte gezählt, durch welche die wirtschaftlichen Verhältnisse eines Betriebs maßgeblich bestimmt werden können."[621]

---

[615] *Heußner*, Informationssysteme im Europäischen Verwaltungsverbund, 2007, S. 320 ff.; vgl. *Frank*, Der Schutz von Unternehmensgeheimnissen im öffentlichen Recht, 2008, S. 68 ff.

[616] EuGH, C-1/11, Rn. 43; vgl. EuGH, C-450/06, Rn. 49; zur häufig fehlenden Differenzierung des EuGH *Siebert*, Geheimnisschutz und Auskunftsansprüche im Recht des Geistigen Eigentums, 2011, S. 260.

[617] Der Begriff der Betriebs- und Geschäftsgeheimnisse wird ebenso in Art. 41 Abs. 2 lit. b GRCh im Zusammenhang mit dem Informationszugangsanspruch verwendet, allerdings nicht abstrakt definiert.

[618] EuG, T-474/04, Rn. 65.

[619] EuG, T-474/04, Rn. 65, das sich in diesem Zusammenhang auf die Veröffentlichung der Information bezieht.

[620] BVerfGE 115, 205 (229).

[621] BVerfGE 115, 205 (230 f.), NVwZ 2006, 1041 (1042).

In sekundär- oder einfachgesetzlichen Ausgestaltungen werden die Begrifflichkeiten nicht einheitlich verwendet.[622] Hinsichtlich des Inhalts besteht jedoch im Gegensatz zur Verwendung des Begriffs weitgehend Einigkeit.[623] Aus der Gesamtschau der Definitionen europäischer und deutscher Rechtsprechung ergibt sich, dass eine Information schützenswert ist, wenn sie erstens einen Unternehmensbezug aufweist, zweitens nur einem begrenzten Personenkreis bekannt ist, drittens ein Geheimhaltungswille und viertens ein berechtigtes Geheimhaltungsinteresse bestehen.[624]

bb) Beispiel der Sicherheitslücke

Inwiefern die Voraussetzungen auf sicherheitstechnische Informationen appliziert werden können, soll am Beispiel von Sicherheitslücken aufgezeigt werden.

Dass Sicherheitslücken und Schwachstellen ein grundlegendes und strukturelles Problem für die IT-Sicherheit darstellen, ist zwar eine banale, aber keine triviale Erkenntnis. Es ist ein zentrales Anliegen in der Sicherheitsgewährleistung, Wissen über Sicherheitslücken, deren prinzipielle Ursachen und deren Natur zu generieren. Das Wissen über Sicherheitslücken wird zum Teil als „sehr gering" bezeichnet.[625] Das daraus entstehende Bedürfnis nach Kenntnissen über Sicherheitslücken verdeutlicht zugleich die Schutzbedürftigkeit der Unternehmen.

(1) Begriff der Sicherheitslücke

Technisch betrachtet sind Sicherheitslücken Zustände in einem Computersystem oder in Systemen, die es ermöglichen, dass Befehle ohne Berechtigung ausgeführt werden können, ein Dritter unberechtigten Zugriff auf Daten erhält, dem System eine falsche Identität vorgegeben werden ein Angreifer Deni-

---

[622] Vgl. Art. 118 Abs. 2 VO (EG) Nr. 1907/2006; § 67 Abs. 1 S. 2 SGB X; § 17 UWG.

[623] Die weitergehende Unterscheidung von Betriebs- und Geschäftsgeheimnissen kann hier entfallen, da der rechtliche Schutz als Rechtsfolge übereinstimmt, siehe *Siebert*, Geheimnisschutz und Auskunftsansprüche im Recht des Geistigen Eigentums, 2011, S. 240 f. Geschäftsgeheimnisse können dem kaufmännischen Bereich eines Unternehmens zugeordnet werden, während Betriebsgeheimnisse dem technischen Bereich zugewiesen werden können. Als Oberbegriff wird der Begriff Unternehmensgeheimnis verwendet. Siehe *Zech*, Information als Schutzgegenstand, 2012, S. 230 ff.

[624] Vgl. Art. 2 Abs. 1 RL (EU) 2016/943; ebenso *Roßnagel*, Verfassungsrechtliche Grenzen gesetzlicher Pflichten zur Offenlegung von Arbeits- und Beschäftigungsbedingungen, 2016, S. 37.

[625] *Brodowski/Freiling*, Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, 2011, S. 26.

al-of-Service-Attacken ausführen kann.[626] Sicherheitslücken sind Resultat von Komplexität. Es ist im Grunde nicht möglich, eine Software zu schreiben, die keine Fehler enthält. Die zunehmende Funktionsvielfalt führt zu einer insgesamt unendlichen Anzahl an Schwachstellen. Gewöhnliche Programme führen in der Regel Millionen Zeilen von Codes aus, also Sätze und Computerbefehle. Je nach Programmqualität liegt die Fehlerquote zwischen 5 und 0,0001 Prozent.[627] Die Anzahl an Sicherheitslücken, die für einen Hack ausgenutzt werden können, liegt ebenfalls bei ungefähr 5 Prozent.[628] Bei anspruchsvolleren Programmen mit mehreren hundert Millionen Zeilen Code kann dies zu einer beträchtlichen Quantität an Angriffswegen führen. Hinzu kommt, dass es nicht nur neue Wege gibt, Sicherheitslücken zu produzieren, sondern auch Techniken dafür, Sicherheitslücken auszunutzen (sog. Exploits).

Auf europäischer Ebene findet sich keine Begriffsbestimmung. Eine rechtliche Ausgangsdefinition des Begriffs der Sicherheitslücke findet sich in § 2 Abs. 6 BSIG. Sicherheitslücken im Sinne des BSIG sind demnach Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung sich Dritte gegen den Willen des Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen Systeme beeinflussen können. Letztlich können Sicherheitslücken damit auch rechtlich als Fehler von Programmen beschrieben werden.[629]

(2) Schutzvoraussetzungen

Für die in Betracht kommende Qualifizierung als Betriebs- und Geschäftsgeheimnis muss die Information zunächst einen tatsächlichen Unternehmensbezug aufweisen. Die Information muss in Abgrenzung zu Einschätzungen, Bewertungen, Ansichten und Meinungen „Tatsachen, Umstände und Vorgänge" erfassen, die in einem unternehmerischen Zusammenhang stehen.[630] Der Unter-

[626] Definition von „Vulnerability" nach Common Vulnerabilities and Exposures (CVE), abrufbar unter: https://cve.mitre.org/about/terminology.html. CVE ist ein Industriestandard mit dem Ziel, eine einheitliche Namenskonvention für Sicherheitslücken einzuführen.

[627] *Gaycken*, Cybersicherheit in der Wissensgesellschaft, in: Daase/Engbert/Junk (Hrsg.), Verunsicherte Gesellschaft – Überforderter Staat, 2013, S. 109 (121).

[628] *Gaycken*/*Lindner*, Zero Day Governance – A(n Inexpensive) Solution to the Cyber Security Problem, in: Harvard – MIT Cyber Dialogue: What is Stewardship in Cyberspace, 2012, S. 13, online abrufbar.

[629] *Buchberger*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, BSIG, § 2 Rn. 8.

[630] *Frank*, Der Schutz von Unternehmensgeheimnissen im öffentlichen Recht, 2008, S. 46; *Roßnagel*, Verfassungsrechtliche Grenzen gesetzlicher Pflichten zur Offenlegung von Arbeits- und Beschäftigungsbedingungen, 2016, S. 39.

nehmensbezug besteht grundsätzlich dann, wenn die Information derart in einen Betrieb eingebracht wird, dass sie zum räumlichen oder persönlichen Herrschaftsbereich des Unternehmens gehört und nicht etwa ein Privatgeheimnis darstellt. Eine IT-Sicherheitslücke ist ein wirklicher, nachweisbarer Sachverhalt und fällt, wenn sie zu den Netz- und Informationssystemen gehört, in den Herrschaftsbereich des betreffenden Unternehmens.

Des Weiteren muss die Information nichtoffenkundig sein, d. h. nur einem eng begrenzten Personenkreis bekannt sein. Offenkundig ist eine Information dann, wenn sie in den Kreisen, die üblicherweise mit Informationen dieser Art befasst sind, allgemein bekannt oder leicht zugänglich ist.[631] Damit hängt die Erfüllung dieses Kriteriums vom Einzelfall ab. Für die Bestimmung der Zugänglichkeit können Kriterien wie die Verbreitung des Programms und die Qualität der Sicherheitslücke herangezogen werden. Differenzierungsmerkmale könnten auch die Natur der Sicherheitslücke und das Verfahren ihrer Aufdeckung sein. Der Geheimnischarakter von Exploits, also Computerprogrammen, die Vulnerabilitäten tatsächlich systematisch ausnutzen, soll erst mit einer gewissen Verbreitung der Kenntnis über sie entfallen.[632] Der Geheimnischarakter kann entfallen, ohne dass es der Untersuchung des Quellcodes bedarf, wenn wie bei DDoS-Exploits strukturelle Serverschwächen ausgenutzt werden, die in der „Community" gemeinhin bekannt sind.

Der Geheimhaltungswille als subjektives Element dürfte typischerweise zu unterstellen sein. Dieser Wille soll das Geheimnis von bloßen unbekannten Tatsachen unterscheiden.[633] Soweit jedenfalls eine IT-Sicherheitslücke entdeckt wurde und ihre Offenbarung zu Reputationsverlusten des Unternehmens führt, kann ein solcher Geheimhaltungswille angenommen werden. Das Geheimhaltungsinteresse soll sicherstellen, dass die Geheimhaltung nicht beliebig verlangt wird, ohne dass dafür ein im Ansatz begründetes Interesse gegeben ist.[634] Ein wirtschaftliches Interesse vermag die Erfüllung dieses Kriteriums zu indizieren. Das Interesse muss sich nicht auf konkrete Vermögenswerte beziehen,[635] sondern kann auch die Stellung im Wettbewerb betreffen, sodass auch hier die Angst vor einem Reputationsverlust auf ein bestehendes Interesse schließen lässt.

Zuletzt muss ein berechtigtes objektives Geheimhaltungsinteresse vorliegen. Das Merkmal soll eine willkürliche Vorenthaltung von Informationen und da-

---

631 *Kloepfer*, Informationsfreiheitsgesetz und Schutz von Betriebs- und Geschäftsgeheimnissen, 2011, S. 23; BGH GRUR 58, 297 (299); *Ohly,* in: ders./Sosnitza (Hrsg.), UWG, 6. Aufl. 2014, § 17 Rn. 7; vgl. § 39 Abs. 2 TRIPS.

632 Vgl. BayOLG, GRUR 91, 694 (696) zu illegalen Auswertungsprogrammen.

633 *Harte-Bavendamm*, in: ders./Henning-Bodewig (Hrsg.), UWG, 3. Aufl. 2013, § 17 Rn. 5.

634 *Harte-Bavendamm*, in: ders./Henning-Bodewig (Hrsg.), UWG, 3. Aufl. 2013, § 17 Rn. 6.

635 BGH GRUR 06, 1044, Rn. 19.

mit die Ausuferung des Geheimnisschutzes verhindern.[636] Das Interesse muss wirtschaftlicher Natur sein und ist immer dann anzunehmen, wenn das Bekanntwerden der Information geeignet ist, die Stellung des Betriebs im Wettbewerb zu verschlechtern oder ihm wirtschaftlichen Schaden zuzufügen.[637] Da das Bekanntwerden einer Sicherheitslücke Rückschlüsse auf die interne IT-Infrastruktur zulässt und Reputationsschäden denkbar sind, die zu wirtschaftlichen Schäden führen können, ist die Annahme eines berechtigten Geheimhaltungsinteresses grundsätzlich zu bejahen. Überdies kann das Bekanntwerden dazu führen, dass unbefugte Dritte die Informationen in Schädigungsabsicht missbrauchen. So kann die Meldung einer Sicherheitslücke den Anlass dafür bilden, dass diese von einem Angreifer ausgenutzt wird, bevor sie geschlossen werden kann.

Es ist demnach nicht völlig ausgeschlossen, eine IT-Sicherheitslücke als rechtlich geschütztes Geheimnis zu qualifizieren. Die Definition des geschützten Unternehmensgeheimnisses ließe sich auf andere Informationen im Kontext der Netz- und Informationssicherheit übertragen. Denkbar sind etwa Informationen über erfolgte Angriffe auf Unternehmen oder Informationen über Sicherheitsverschlüsselungen und sonstige Algorithmen.

c) Besonderer Schutz für Betreiber kritischer Infrastrukturen im Rahmen von Meldepflichten

Mit Blick auf die Meldepflichten ist allerdings fraglich, ob hinsichtlich der betreffenden Informationen ein berechtigtes Geheimhaltungsinteresse besteht. Gegen den Geheimnisschutz bei Bestehen von Meldepflichten spricht, dass das Unternehmen die meldepflichtigen Informationen gerade offenbaren muss und insofern den Geheimnischarakter der Information nicht beherrschen kann. In der Meldepflicht könnte die gesetzgeberische Wertung liegen, dass diese Informationen aus dem Kreis der Betriebs- und Geschäftsgeheimnisse herausgenommen sind.[638] Gegen den Schutz spricht darüber hinaus, dass nicht nur schutzbe-

[636] *Kloepfer*/*Grewe*, NVwZ 2011, 577 (582).

[637] *Kloepfer*, Informationsfreiheitsgesetz und Schutz von Betriebs- und Geschäftsgeheimnissen, 2011, S. 28; *Roßnagel*, Verfassungsrechtliche Grenzen gesetzlicher Pflichten zur Offenlegung von Arbeits- und Beschäftigungsbedingungen, 2016, S. 41 f.

[638] *Roßnagel*, Verfassungsrechtliche Grenzen gesetzlicher Pflichten zur Offenlegung von Arbeits- und Beschäftigungsbedingungen, 2016, S. 72: „Diese Informationen können keine Betriebs- und Geschäftsgeheimnisse sein, weil der Unternehmer sie veröffentlichen muss und daher ihren Geheimnischarakter nicht beherrschen kann. Auch wenn es Informationen sind, die das Unternehmen betreffen [sic] und er einen Geheimhaltungswillen kundgetan hat und ohne die Veröffentlichungspflicht ein berechtigtes Interesse an der Geheimhaltung gelten machen könnte, fallen sie nicht unter die Betriebs- und Geschäftsgeheimnisse, weil der Gesetzgeber die Publikation der Information für die Öffentlichkeit höher gewichtet hat als das Geheimhaltungsinteresse des Unternehmers." Vgl. auch *Breuer*, NVwZ 1986, 171 (173).

dürftige, sondern auch nur schutzwürdige Interessen erfasst sein sollen. Beziehen sich die Informationen auf rechtswidrige Geschäftspraktiken oder die Missachtung von IT-Sicherheitspflichten, kann an dem zuzumessenden Schutz durchaus gezweifelt werden.[639] Im Interesse der größtmöglichen Reichweite des Grundrechtsschutzes spricht aber vieles dafür, die möglichen Wertungen auf Ebene der Rechtfertigung in Einklang zu bringen.

Unabhängig von der Bewertung in Einzelfall wird im Rahmen der Meldepflichten dem Schutzbedürfnis der Betreiber kritischer Infrastrukturen durch ein besonderes abgestuftes Meldesystem Rechnung getragen.

Die Meldepflicht für Betreiber kritischer Infrastrukturen ist zweistufig ausgestaltet. Für Störungen der Sicherheit, die nicht zu einem tatsächlichen Ausfall oder einer Beeinträchtigung führen, ist die namentliche Nennung des Betreibers nicht erforderlich (§ 8b Abs. 4 S. 1 BSIG). Die Meldung muss nicht direkt an das BSI gerichtet sein, sondern kann über eine Kontaktstelle erfolgen (§ 8b Abs. 3 BSIG). Die Nennung des Betreibers ist hingegen geboten, wenn die Störung zu einem tatsächlichen Ausfall oder zu einer Beeinträchtigung der Funktionsfähigkeit kritischer Infrastrukturen geführt hat (§ 8b Abs. 4 S. 3 BSIG). Durch die NIS-Richtlinie wird diese Differenzierung nicht vorgesehen, aber auch nicht ausgeschlossen.

Durch das gestufte Verfahren sollen gerade vor dem Hintergrund der Sensibilität der Meldungen wirtschaftliche Auswirkungen durch ein etwaiges Bekanntwerden von Vorfällen verhindert werden.[640] Erst im konkreten Schadensfall soll das BSI ohne Umwege eine Informationsbeziehung mit den Betreibern aufnehmen können, sodass erst dann das Interesse der Unternehmen an der Nichtpreisgabe der Identität hinter die Eilbedürftigkeit zurücktritt. Die Offenlegung des konkreten Betreibers gegenüber dem BSI ist dann wegen des übergeordneten Interesses an der Abwehr der unmittelbaren Gefährdung der Versorgungssicherheit gerechtfertigt.[641]

Die fehlende Pflicht zur Nennung des Infrastrukturbetreibers führt indes nicht zu einer Anonymität des Betreibers. Die Meldung an die Kontaktstelle führt lediglich zu einer Pseudonymisierung. Im datenschutzrechtlichen Kontext bedeutet Pseudonymisierung, dass – im Gegensatz zur Anonymisierung – das

---

[639] Vgl. § 2 S. 1 Nr. 2 c) VIG; *Wollenschläger*, VerwArch 112 (2011), 20 (36); *Heußner*, Informationssysteme im Europäischen Verwaltungsverbund, 2007, S. 321.

[640] BT-Drs. 18/4096, S. 47.

[641] *Hornung*, Stellungnahme zum Entwurf eines IT-Sicherheitsgesetzes vom 18.04.2015, A-Drs. 18(4)284 G, S. 3; vgl. aber *Roßnagel*, A-Drs. 18(4)284 B, S. 11, der darauf hinweist, dass eine Aufdeckungsregel wie etwa § 16 DeMailG im BSIG eben nicht enthalten ist und zumindest aus dem datenschutzrechtlichen Zweckbindungsgrundsatz eine Offenlegung untersagt ist.

Herstellen des Zusammenhangs zum Betroffenen noch möglich ist.[642] Da zu den Angaben einer Meldung die Nennung der eingesetzten Technik sowie der Branche gehört, ist eine Zuordnung durch Wettbewerber nicht von vorneherein ausgeschlossen. Die Herkunft einer Meldung kann gerade in Branchen mit nur wenigen meldepflichtigen Betreibern durch eine nachträgliche Zuordnung anhand der gemeldeten Daten feststellbar sein.[643] Dem BSI soll gerade die Möglichkeit erhalten bleiben, auf meldende Betreiber zurückzukommen, ohne dass eine Offenlegung des Klarnamens erforderlich wäre.[644]

Bemerkenswert ist allerdings, dass eine Regelung für Infrastrukturbetreiber im Energiesektor wie in § 11 Abs. 1c S. 5 EnWG besteht, nach der sowohl das BSI als auch die Bundesnetzagentur sicherzustellen haben, dass die unbefugte Offenbarung der durch die Meldepflicht zur Kenntnis gelangten Angaben ausgeschlossen ist. Dies verwundert umso mehr, als sowohl diese Regelung als auch das abgestufte Meldeverfahren mit den Novellierungen durch das IT-Sicherheitsgesetz eingeführt wurden. Der Unterschied in der Regulierung lässt auf eine Differenzierung der Interessen der Meldeverpflichteten an der Schutzbedürftigkeit der Informationen schließen. Zwar lässt sich nicht bezweifeln, dass die Daten über die IT-Sicherheit im Energiesektor hochsensibel sind. Versorgungssysteme sind eine Infrastruktur für andere Infrastrukturen, mithin eine Meta-Infrastruktur, ohne die auf sie aufbauende Sekundärinfrastrukturen nicht würden funktionieren können. Nicht weniger sensibel dürften regelmäßig aber die gemeldeten Daten der sonstigen meldeverpflichteten Betreiber kritischer Infrastrukturen sein.[645]

Das abgestufte Meldeverfahren über eine Kontaktstelle gilt nicht für die Betreiber von Telekommunikationsnetzen und Anbieter von Telekommunikationsdiensten. Deren Meldungen sind direkt der Bundesnetzagentur zu übermitteln. Die Effektivität der Meldepflicht kann beeinträchtigt werden, wenn ein Unternehmen die mit einer offengelegten Identität verbundenen Risiken nicht eingeht und stattdessen das Risiko eines Ordnungsgeldes nach § 149 Abs. 1 Nr. 21a TKG in Kauf nimmt. Die Friktion im System der Meldepflichten lässt sich damit rechtfertigen, dass gerade die telekommunikationsrechtlichen Meldungen einen erheblichen Teil der Informationen über die Internetsicherheit generieren. Die bilaterale Kommunikation der Behörden mit den Unternehmen muss daher

---

642 Vgl. § 3 Abs. 6, 6a BDSG.

643 *Bräutigam*/*Wilmer*, ZRP 2015, 38 (41).

644 BT-Drs. 18/4096, S. 47.

645 Zur Folgenanalyse ausgewählter Sektoren kritischer Infrastrukturen, insbesondere zur Stromabhängigkeit und zu den Interdependenzen der Sektoren *Petermann*/*Bradke*/*Lüllmann*/*Poetzsch*/*Riehm*, Was bei einem Blackout geschieht, Studien des Büros für Technikfolgenabschätzung des Deutschen Bundestages, 2011, S. 77.

im Zweifel ohne Verzögerung stattfinden können. Der Weg über eine Kontaktstelle würde durch einen anschließenden Identifikationsprozess zu unbotmäßigen Verzögerungen führen. Das für die Betreiber von kritischen Infrastrukturen bestehende Meldeverfahren ist anders als das für Telekommunikationsunternehmen im besonderen Maße auf den Aufbau einer vertrauensvollen Kooperation angewiesen. Die telekommunikationsrechtlichen Meldepflichten bestanden schon vor der Einführung der Meldepflicht für Sicherheitsvorfälle bei den Betreibern kritischer Infrastrukturen. Insofern dient die Möglichkeit, Meldungen pseudonym abzugeben, zugleich als Anreiz, den Pflichten überhaupt nachzukommen.

Nach allem ergibt sich aus dem besonderen Meldeverfahren für Betreiber kritischer Infrastrukturen ein indirekter Schutz für Unternehmensinformationen. Eine Reduzierung der meldepflichtigen Angaben und damit ein Erkenntnisverlust sind grundsätzlich nicht zu befürchten. Vielmehr dient das abgestufte Meldeverfahren den Betreibern und Anbietern als zusätzlicher Anreiz, die Meldepflichten zu erfüllen.

3. Schutz vor unbefugter Offenlegung durch das Verwaltungsgeheimnis

Zur Rechtfertigung von Eingriffen in geschützte Betriebs- und Geschäftsgeheimnisse kommt es maßgeblich auf die Verhältnismäßigkeit an (a). Für die Verhältnismäßigkeit streitet insbesondere der Schutz der generierten Informationen durch das Verwaltungsgeheimnis (b).

a) Beachtung der Verhältnismäßigkeit

Das direkte Erheben von geschützten Geheimnissen beeinträchtigt grundsätzlich die grundrechtlich geschützte Rechtsposition.

Die durch Art. 15 GRCh geschützte Berufsfreiheit gewährt, trotz aller Einzelausprägungen, ein einheitliches Grundrecht, das sowohl das Recht auf Berufswahl als auch auf die Berufsausübung umfasst.[646] Die durch Art. 16 GRCh geschützte unternehmerische Tätigkeit umfasst die Ausübung der Wirtschafts- und Geschäftstätigkeit, die Vertragsfreiheit, die Handelsfreiheit, die Werbe- sowie die Wettbewerbsfreiheit.[647] Eingriffe in diese Grundrechte sind nach Art. 52 Abs. 1 S. 1 GRCh nur aufgrund eines Gesetzes zulässig, wenn sie den Wesensgehalt beachten. Einschränkungen dürfen gemäß Art. 52 Abs. 1 S. 2 GRCh nur unter Wahrung des Grundsatzes der Verhältnismäßigkeit vorgenommen wer-

[646] *Schwarze*, in: ders./Becker/Hatje/Schoo (Hrsg.), EU-Kommentar, 3. Aufl. 2012, GRCh, Art. 15, Rn. 12.

[647] *Schwarze*, in: ders./Becker/Hatje/Schoo (Hrsg.), EU-Kommentar, 3. Aufl. 2012, GRCh, Art. 16, Rn. 3.

den, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

Vergleichbare Anforderungen an die Rechtfertigung sind auch im Rahmen von Art. 12 GG zu stellen. Eine staatliche Maßnahme, die auf die Offenlegung bestimmter Geschäfts- und Betriebsgeheimnisse gerichtet ist, stellt einen Eingriff in den Schutzbereich von Art. 12 Abs. 1 GG dar und ist an der vom Bundesverfassungsgericht aufgestellten Drei-Stufen-Theorie zu messen.[648] Die Offenlegung von Geschäfts- und Betriebsgeheimnissen kann als Berufsausübungsregelung qualifiziert werden, da sie weder an subjektive Voraussetzungen anknüpft, noch die Berufswahl betrifft. Zulässig ist eine Berufsausübungsregelung, wenn vernünftige Erwägungen des Allgemeinwohls dieselbe zweckmäßig erscheinen lassen.[649]

Der Schutzgegenstand des in Art. 17 GRCh gewährleisteten Eigentumsrechts ist nicht abstrakt definierbar, da er normativ durch den Gesetzgeber ausgefüllt wird.[650] Das Eigentum wird nach Art. 345 AEUV vor allem durch die nationalen Rechtsordnungen bestimmt. Unter den Schutzbereich des Eigentums fallen daher die im nationalen Recht geschützten Rechtspositionen.[651] Allerdings wird die Kompetenz des Europäischen Gerichtshofs, Inhalt und Grenzen des Eigentums unionrechtlich festzulegen, durch Art. 345 AEUV nicht ausgeschlossen. Der Gesetzgeber kann nach Art. 17 Abs. 1 S. 3 GRCh die Nutzung des Eigentums regeln, soweit dies für das Wohl der Allgemeinheit erforderlich ist. Rechtmäßig sind bloße Nutzungsbeschränkungen, wenn sie tatsächlich dem Gemeinwohl dienenden Zielen der Union entsprechen und nicht einen im Hinblick auf die verfolgten Ziele „unverhältnismäßigen, nicht tragbaren Eingriff darstellen, der die so gewährleisteten Rechte in ihrem Wesensgehalt antastet."[652]

Das Eigentumsrecht, das nach Art. 14 GG geschützt wird, ist gleichfalls normgeprägt.[653] Der Geheimnisschutz wird teilweise im davon erfassten Recht am eingerichteten und ausgeübten Gewerbebetrieb verortet, da Geheimnisse maßgebliche wertbildende Faktoren seien.[654] Das Bundesverfassungsgericht lässt die Frage offen, ob ein Unternehmen in seiner tatsächlichen Zusammen-

---

[648] BVerfGE 115, 205 (230); zur Drei-Stufen-Theorie BVerfGE 7, 377 (398 ff.).

[649] BVerfGE 7, 377 (407).

[650] Vgl. *Streinz*, in: ders. (Hrsg.), EUV/AEUV, 2. Aufl. 2012, GRCh, Art. 17 Rn. 18.

[651] *Siebert*, Geheimnisschutz und Auskunftsansprüche im Recht des Geistigen Eigentums, 2011, S. 260.

[652] EuGH, C-368/96, Rn. 79.

[653] *Papier*, in: Maunz/Dürig (Hrsg.), GG, Band II, 75. Aufl. 2015, Art. 14 Rn. 315 ff.

[654] *Michalski*/*Funke*, in: Michalski (Hrsg.), GmbHG, Band 1, 2. Aufl. 2010, § 13 Rn. 56.

fassung vor Eingriffen geschützt ist.[655] Zum Teil wird angenommen, dass eine Offenlegungspflicht eine Information gerade aus dem Geheimnisschutz herausnimmt.[656] Andere nehmen an, dass durch den hoheitlichen Umgang mit einer geheimen Information die Nutzung des Eigentums dergestalt beschränkt wird, dass das betreffende Unternehmen in der alleinigen Verfügungsgewalt beschnitten wird, da das Recht auch umfasst, darüber zu bestimmen, wer von Informationen Kenntnis nehmen darf und wer nicht.[657]

Der Unternehmensdatenschutz kann bei Informationseingriffen demnach über einen eigentumsähnlichen Zuweisungsgehalt oder über die freie Berufsausübung gewährleistet werden.[658] Es ähnelt dem Recht der informationellen Selbstbestimmung insoweit, als das Grundrecht auf Geheimsphäre grundsätzlich vor unbefugter Erhebung, Offenlegung und Weitergabe schützt.[659] Das Kriterium der „sozialen" Relevanz im Datenschutz findet seine Entsprechung in der Stellung eines Unternehmens im Wettbewerb.[660]

Die hohe Normprägung der Grundrechte gibt dem Gesetzgeber grundsätzlich einen großen Auswahl- und Gestaltungsspielraum. Aus allen Grundrechten folgt letztlich, dass die gesetzgeberischen Maßnahmen und die behördliche Anwendung der informationsverwaltungsrechtlichen Rechtsgrundlagen im Einzelfall verhältnismäßig sein müssen.

b) Schutz durch das Verwaltungsgeheimnis

Im Rahmen der Angemessenheit ist besonders zu berücksichtigen, dass dem Geheimhaltungsinteresse der Unternehmen durch das Verwaltungsgeheimnis Rechnung getragen wird, das vor unbefugter Offenbarung durch die Behörde schützt.[661]

Spezielle Schutzvorschriften für das BSI finden sich im BSIG hinsichtlich des Schutzes von Unternehmensgeheimnissen nicht. Das Gleiche gilt für die Bundesnetzagentur. Das Telekommunikationsrecht gewährt zwar einen speziellen Schutz unternehmensbezogener Daten,[662] der sich auf Daten juristischer Perso-

---

[655] BVerfGE 105, 252 (278).

[656] *Breuer*, NVwZ 1986, 171 (173).

[657] *Wettner*, Die Amtshilfe im europäischen Verwaltungsrecht, 2005, S. 329; *Heußner*, Informationssysteme im Europäischen Verwaltungsverbund, 2007, S. 324.

[658] Zum kumulierten Schutz in Idealkonkurrenz *Kloepfer*, Informationsfreiheitsgesetz und Schutz von Betriebs- und Geschäftsgeheimnissen, 2011, S. 9.

[659] *Stancke*, BB 2013, 1418 (1420).

[660] Zur Bedeutung des grenzüberschreitenden, interadministrativen Informationstransfers siehe unter § 4 E.

[661] Vgl. *Meyer-Sebastian*, in: Geppert/Schütz (Hrsg.), BeckTKG, 4. Aufl. 2013, § 127, Rn. 16.

[662] Anforderungen an den Schutz von Betriebs- und Geschäftsgeheimnissen finden sich in

nen während des Telekommunikationsvorgangs oder Betriebs- und Geschäftsgeheimnisse in Beschlussverfahren der Bundesnetzagentur bezieht. Eine spezielle Regelung des Geheimnisschutzes mit Bezug auf die jeweiligen Informationserhebungsbefugnisse findet sich im TKG jedoch nicht.

Damit kann auf das Verwaltungsgeheimnis in § 30 VwVfG zurückgegriffen werden.[663] Nach § 30 VwVfG haben die Beteiligten Anspruch darauf, dass ihre Geheimnisse, insbesondere Betriebs- und Geschäftsgeheimnisse, von der Behörde nicht unbefugt offenbart werden. Die Anwendung des § 30 VwVfG steht unter dem allgemeinen Subsidiaritätsvorbehalt des § 1 VwVfG. Inhaltsgleiche und entgegenstehende Bestimmungen des Bundes gehen § 30 VwVfG vor.

Nach dem Wortlaut („Beteiligte“) und der systematischen Stellung im VwVfG bezieht sich die Vorschrift auf Verwaltungsverfahren im Sinne des § 9 VwVfG. Diese sind auf den Erlass des Verwaltungsaktes gerichtet. Dem Schutz durch § 30 VwVfG könnte also entgegenstehen, dass einige Verfahren zur Informationsgenerierung keine Verwaltungsverfahren darstellen. So stellen die Meldepflichten bei Sicherheitsvorfällen selbstbeständige Informationsbeibringungspflichten dar, die einen Verwaltungsakt als Rechtsgrundlage nicht voraussetzen und von der Behörde keine Sachauseinandersetzung erfordern.

Eine genaue Charakterisierung der Verfahren ist gleichwohl nicht geboten. Gute Gründe sprechen dafür, der Regelung einen allgemeinen Charakter zuzusprechen.[664] Zum einen sprechen rechtsstaatliche Erwägungen dafür, den Schutz nicht nur im Rahmen eines laufenden Verfahrens zu gewähren. „Beteiligte“ sind nach weiterer Auslegung des Tatbestandsmerkmals auch solche eines bereits durchgeführten Verwaltungsverfahrens und sonstiger einzelfallbezogener Behördenverfahren.[665] Zum anderen ist § 30 VwVfG Ausdruck eines allgemeinen, verfassungsrechtlich abgeleiteten Rechtsgrundsatzes, der auch außerhalb des durch §§ 1, 2 und 9 VwVfG markierten Anwendungsbereichs Anwendung findet.[666] Dadurch gilt der Grundsatz bei jeder öffentlich-rechtlichen Verwaltungstätigkeit.[667]

Für den Umgang staatlicher Stellen mit sensiblen, unternehmensbezogenen Angaben gilt damit für die hier relevanten Sicherheitsbehörden die Grundregel

---

§ 77a Abs. 3 S. 3 TKG, § 82 Abs. 4 S. 2 TKG, § 87 Abs. 3 TKG, § 121 Abs. 2 S. 3 TKG, § 123b Abs. 3, § 135 Abs. 3 S. 2 TKG und § 126 TKG.

663 *Kallerhoff*, in: Stelkens/Bonk/Sachs (Hrsg.), VwVfG, 8. Aufl. 2014, § 30 Rn. 3.

664 Vgl. auch Begründung zu § 26 des Entwurfs des VwVfg 1973, BT-Drs. 7/910, S. 54; *Kallerhoff*, in: Stelkens/Bonk/Sachs (Hrsg.), VwVfG, 8. Aufl. 2014, § 30 Rn. 5.

665 *Kopp*/*Ramsauer* (Hrsg.), VwVfG, 16. Aufl. 2015, § 30 Rn. 2; *Kallerhoff*, in: Stelkens/Bonk/Sachs (Hrsg.), VwVfG, 8. Aufl. 2014, § 30 Rn. 5.

666 Vgl. *Sydow*, Die Verwaltung 38 (2005), 35 ff.

667 *Kallerhoff*, in: Stelkens/Bonk/Sachs (Hrsg.), VwVfG, 8. Aufl. 2014, § 30 Rn. 6.

des § 30 VwVfG. In der Rechtsfolge schützt § 30 VwVfG vor dem unbefugten Offenbaren von Unternehmensgeheimnissen, d. h., für die Weitergabe der betreffenden Unternehmensinformation bedarf es einer gesonderten Befugnis.[668]

Da bei Anwendung des Verwaltungsgeheimnisses geschützte Informationen vor dem unbefugten Offenbaren zu schützen sind, wird teilweise angenommen, dass für die behördliche Informationsgenerierung keine rechtliche Grenze bestehe. Ein rechtfertigungsbedürftiger Eingriff sei erst in der interbehördlichen Weitergabe oder in der Offenbarung von Informationen gegenüber privaten Dritten zu sehen.[669] Dafür lässt sich in der Tat anführen, dass durch die behördliche Generierung von geheimen Informationen grundsätzlich keine berufs- oder wettbewerbsbezogene Beeinträchtigung im Sinne der rechtlichen Zuordnung des Geheimnisses herbeigeführt wird. Ein Geheimnis ist für Wettbewerber gerade nicht besser erreichbar, da die Behörde das Geheimnis gemäß § 30 VwVfG nicht ohne Weiteres offenbaren darf. Im Übrigen schützen die sonstigen, das rechtsstaatliche Verfahren absichernden Vorschriften des Dienstrechts zur Amtsverschwiegenheit[670] und der strafrechtliche Geheimnisschutz[671] vor einer unbefugten Veröffentlichung eines Unternehmensgeheimnisses.

Für die Annahme eines Eingriffs in geschützte Unternehmensgeheimnisse durch behördliche Informationsgenerierung trotz Anwendbarkeit des Verwaltungsgeheimnisses spricht, dass die NIS-Behörden Teil einer institutionalisierten Kooperation sind, die darauf angelegt ist, einen Informationsaustausch zu ermöglichen. Die Informationsgenerierung ist Voraussetzung und Vorstufe einer späteren Weitergabe von Informationen und folglich einer späteren Gefährdung. Diese erhöhte Gefährdung spricht dafür, den Schutzbereich für Unternehmensgeheimnisse bereits früher als eröffnet anzusehen.[672] Zudem besteht bei behördlichen Informationssammlungen die tatsächliche Gefahr, dass diese angegriffen werden und so geschützte Informationen ungewollt an die Öffentlichkeit gelangen. Gegen starke Angreifer kann grundsätzlich kein Informationssystem als sicher gelten.[673] Demnach besteht für Unternehmensgeheimnisse allein durch die Speicherung bei der NIS-Verwaltung eine abstrakte Gefahr. Ein besonderes Schutzbedürfnis entsteht bei Unternehmen außerdem dann, wenn

---

668 *Kopp/Ramsauer*, VwVfG, 17. Aufl. 2016, § 30, Rn. 12.

669 Vgl. *Rosenberger*, Geheimnisschutz und Öffentlichkeit in Verwaltungsverfahren und -prozeß, 1998, S. 48 f.; *Frank*, Der Schutz von Unternehmensgeheimnissen im Öffentlichen Recht, 2009, S. 76; in diesem Sinne auch *Druey*, Information als Gegenstand des Rechts, 1995, S. 256.

670 §§ 67 Abs. 1 BBG, § 37 Abs. 1 BeamtStG, § 9 BAT.

671 §§ 203, 353b, 354 StGB.

672 In diesem Sinne *Bullinger*, NJW 1978, 2121 (2123).

673 Vgl. *Greenberg*, The Shadow Brokers Mess Is What Happens When the NSA Hoards Zero-Days, Wired vom 17.08.16, online abrufbar.

für die Ausübung von Informationsbefugnissen private Dritte herangezogen werden. So hat das BSI bei der Auswahl und Akkreditierung von Unternehmen, die die Untersuchung von IT-Sicherheitsprodukten und -systemen nach § 7a BSIG vornehmen, die besonders schutzwürdigen Interessen des Herstellers zu berücksichtigen. Zum Schutz dieser Interessen gehört, dass die Beauftragung eines direkten Wettbewerbers ausgeschlossen ist und die Beauftragten zur Wahrung einer den Risiken entsprechenden Vertraulichkeit verpflichtet werden.

Nach all dem können Informationserhebungen der NIS-Verwaltung grundsätzlich, mit Ausnahme der Meldepflichten, rechtfertigungsbedürftige Eingriffe in den grundrechtlich gewährleisteten Schutz von Betriebs- und Geschäftsgeheimnissen darstellen. Für die Zumutbarkeit von Eingriffen spricht insbesondere, dass die generierten Informationen dem Verwaltungsgeheimnis unterliegen, das vor unbefugter Offenlegung der betreffenden Informationen schützt.

F. Zwischenergebnis

Die Funktion und Rechtfertigung der staatlichen Wissensgenerierung im Bereich der betrachteten Netz- und Informationssicherheit kann vor allem in der Erfüllung der Gewährleistungsverantwortung gesehen werden, die im Grundgesetz für den Bereich der Telekommunikation in Art. 87f GG ausdrücklich angelegt ist, die jedoch auch eine unionsrechtliche Dimension hat. Das Internet ist vielfach auch eine Bedingung der effektiven Ausübung von Grundrechten. Aus den Grundrechten folgt in der Infrastrukturdimension ein Recht auf Internetzugang und aus den staatlichen Schutzpflichten das Gebot, die Sicherheit der wesentlichen Internetinfrastrukturen zu gewährleisten.

Die Informationen und das sicherheitsrelevante Wissen sind gesellschaftlich verstreut und vor allem bei den Unternehmen zu verorten. Als Quellen für die Informationsgewinnung dienen in erster Linie die durch die NIS-RL adressierten Betreiber kritischer Infrastrukturen und Anbieter digitaler Dienste sowie Betreiber öffentlicher Telekommunikationsnetze und Erbringer öffentlich zugänglicher Telekommunikationsdienste, aber auch die Verarbeiter personenbezogener Daten, die vor der Geltung der DS-GVO telemedienrechtlich erfasst wurden. Am Beispiel der Over-the-Top-Kommunikationsdienste lässt sich darstellen, dass die telekommunikationsrechtliche Einordnung neuer digitaler Geschäftsmodelle noch nicht abschließend geklärt ist. Die Anwendbarkeit des telekommunikationsrechtlichen Informationsverwaltungsrechts ist jedoch ein Argument für eine Einordnung in das Telekommunikationsrecht.

Zu den maßgeblichen administrativen Wissens- und Informationsakteuren zählen auf europäischer Ebene die ENISA und auf nationaler Ebene das BSI

und die Bundesnetzagentur. Die NIS-Richtlinie erlaubt diese Parallelstruktur. Das BSI fungiert allerdings als zentrale Stelle für die Sicherheit in den Informationstechniken kritischer Infrastrukturen und für die Zusammenarbeit mit europäischen Stellen. Aufgaben, die einen spezifischen Bezug zu den Schutzzielen der Netz- und Informationssicherheit aufweisen, übernehmen darüber hinaus auch die Nachrichtendienste. Die Datenschutzbehörden sind insoweit zum Bereich der Netz- und Informationssicherheit zu zählen, als Datenschutz auch die Datensicherheit umfasst. Die NIS-Behörden haben den organisationsrechtlich verankerten Auftrag, Informationen zu sammeln und zu analysieren und ggf. die Informationen zu teilen. Auf operativer Ebene spielen die IT-Notfallteams (CSIRTs) eine Rolle.

Die informationsrechtlichen Instrumente zur eigentlichen Generierung von Informationen sind vielfältig. Das Instrumentarium ist mit der NIS-Richtlinie und dem IT-Sicherheitsgesetz erweitert worden. Im Rahmen der Informationsbeibringungspflichten erhalten sowohl das BSI als auch die Bundesnetzagentur von den Betreibern kritischer Infrastrukturen respektive den Telekommunikationsunternehmen regelmäßige Nachweise über die Einhaltung der Sicherheitsstandards. Für die Einhaltung der Sicherheitsmaßnahmen durch Anbieter digitaler Dienste ist unionsrechtlich vorgesehen, dass die NIS-Behörde lediglich im Wege von *Ex-post*-Überwachungsmaßnahmen tätig werden darf, und dies auch nur dann, wenn ihr Nachweise darüber vorliegen, dass die Anforderungen nicht eingehalten werden.

Meldepflichten bestehen für Telekommunikationsunternehmen, Betreiber kritischer Infrastrukturen, Anbieter besonderer digitaler Dienste sowie datenschutzrechtlich Verantwortliche. Die Meldetatbestände weisen aber Unterschiede auf, die zu jeweils anderen Meldeschwellen führen. Eine einheitliche unionsrechtliche Klassifikation erscheint hier sinnvoll.

Die Meldepflichten aufgrund von Sicherheitsverletzungen bei Telekommunikationsunternehmen, Betreibern kritischer Infrastrukturen und Anbietern digitaler Dienste bezwecken in der Hauptsache die Gewinnung von Erkenntnissen über die aktuelle und zukünftige Gewährleistung der Sicherheit. Die Meldepflichten aufgrund von Datenschutzverletzungen dienen vorrangig dazu, die Datenschutzaufsicht in den Stand zu versetzen, die Rechte der nunmehr von einer Verletzung Betroffenen zu schützen. Zwar können über die Meldung auch Kenntnisse über die Sicherheit von Datenverarbeitungssystemen oder über die allgemeine Sicherheitslage abgeleitet werden, der Informationsgewinn ist aber eher Reflex als das Ziel der datenschutzrechtlichen Meldepflicht.

Die inhaltlichen Vorgaben, die eine Meldung enthalten soll, regeln weder das Sekundärrecht noch die einfachen Gesetze mit einer spezifizierenden Detailtiefe. Die Art und Weise der Kommunikation ist ebenfalls nicht vorgegeben. Aus

der Funktion der Meldepflichten und der grundrechtlichen Eingriffstiefe, welche die Einführung eines Meldesystems für die Unternehmen darstellt, folgt jedoch, dass sich die Meldung nicht in der bloßen Mitteilung der Tatsache eines Angriffs erschöpft. Die Meldungen dienen auch der Informationsweitergabe, sodass andere potenziell betroffene Unternehmen nach der Information durch die zuständige NIS-Behörde konkrete Vorbereitungs- und Abwehrmaßnahmen treffen können. Die zu meldenden technischen Rahmenbedingungen eines Sicherheitsvorfalls können auch konkrete Informationen zu Sicherheitslücken beinhalten. Die zuständige Behörde oder das CSIRT muss zudem aus der Meldung bestimmten können, ob ein Sicherheitsvorfall grenzüberschreitende Auswirkungen hat.

Soweit die Meldepflichten dazu dienen sollen, ein einheitliches Lagebild beim BSI bezüglich der Sicherheit in der Informationstechnik der kritischen Infrastrukturen zu erstellen, steht dies im Widerspruch zu den separat geregelten Meldeverfahren für Telekommunikations-unternehmen. Der Ausschluss der Telekommunikationsunternehmen aus dem Anwendungsbereich des BSIG schafft parallele Warn- und Meldestrukturen. Ein auf die zentrale Meldestelle ausgerichtetes Meldewesen ist neben dem zu erstellenden Lagebild außerdem für die Krisenkommunikation essenziell. Diese ist im Idealfall direkt und unverzüglich. Insbesondere bei gravierenden IT-Sicherheitsvorfällen sind die gewonnenen Erkenntnisse schnellstmöglich auszutauschen. Dezentralisierte Kommunikationswege konterkarieren die Alarmierungsfunktion, die das BSI übernimmt. *De lege ferenda* wäre § 8c BSIG zu ändern oder dem BSI ausdrücklich die Rolle nicht nur als zentrale, sondern als alleinige Anlaufstelle zuzuschreiben. Die Aufgabe, „geeignete Kommunikationsstrukturen“ zur Krisenfrüherkennung, Krisenreaktion und Krisenbewältigung aufzubauen, ist nicht nur rechtspolitisch angezeigt, sondern durch § 3 Abs. 1 Nr. 15 BSIG geboten. Für eine solche Kommunikation eignen sich nur bidirektionale Meldewege über das Bundesamt. Die Regelung einer fragmentierten Aufsicht über kritische Infrastrukturen ist unverhältnismäßig, wenn sie zum Schutz der Infrastrukturen nicht geeignet ist.

Hinsichtlich der für die Netz- und Informationssicherheit wichtigen Soft- und Hardware kann sich das BSI auf eine Befugnis zur anlassunabhängigen Untersuchung von IT-Sicherheitsprodukten stützen. Grundsätzlich strafrechtlich bewehrte Methoden wie das Reverse Engineering können auch für Produkte gerechtfertigt angewendet werden, die noch nicht auf dem Markt sind. In gewisser Weise ausgeglichen ist damit, dass die Hard- und Softwarehersteller von dem Verpflichtungskanon der IT-Sicherheit, insbesondere den Meldepflichten, ausgenommen sind, obwohl Angriffe auf die Telekommunikationsnetze regelmäßig mittels manipulierter Hard- oder Software erfolgen.

Der Bundesnetzagentur steht außerhalb des ökonomischen Bereichs mit § 115 Abs. 1 S. 2 TKG eine Informationsbefugnis im Bereich der Sicherheit zu. Diese

Informationsbefugnis dient der Erfüllung der Aufsichtsfunktion der Behörde. Einzelfallbezogene Auskunftsersuchen, die über die zur Überwachung der Erfüllung der materiell-rechtlichen wie informationsverwaltungsrechtlichen Vorschriften des 7. Teils des TKG hinausgehen, sind in diesem Bereich grundsätzlich unzulässig.

Den Nachrichtendiensten kommt durch weitreichende Grundlagen zur Informationserhebung eine wachsende Bedeutung für die Gewährleistung der Internetsicherheit zu. Insbesondere der Bundesnachrichtendienst kann im Rahmen der technischen Fernmeldeaufklärung den internationalen Telekommunikationsverkehr, der unter das G10 fällt, mit SIGINT-Methoden nach Schadsoftware und anderen Cyberbedrohungen untersuchen. Die Begrenzungsregelung ist bei strenger Auslegung am gemessenen Datenstrom und nicht an der Vorabselektion des inländischen Telekommunikationsverkehrs zu bemessen. Eine Überwachung des Internetverkehrs in grundsätzlich allen Telekommunikationsnetzen erlaubt die Ausland-Ausland-Fernmeldeaufklärung auf Grundlage des BNDG. Eine Begrenzung besteht im Wesentlichen nur durch das Gebot der Erforderlichkeit der Daten für die Aufgabenerfüllung und die tatsächlichen technischen wie finanziellen Limitierungen. Der Bestand dieser Befugnisse ist ob der möglichen verfassungsrechtlichen Bedenken noch unklar. Im Einzelfall dürfen darüber hinaus Nachrichtendienste zur Aufgabenerfüllung Auskunftsverlangen an Anbieter von Telemediendiensten richten. An Telekommunikationsunternehmen können solche Auskunftsverlangen gerichtet werden, die Informationen über die Strukturen der Dienste und Netze betreffen, die erforderlich sind, um die G10- und BNDG-Beschränkungen, die der Abwehr von Cyberangriffen dienen können, durchzuführen.

Zur Wissensproduktion greift die NIS-Verwaltung neben den Informationsbefugnissen auf die kooperative Übernahme verwaltungsexternen Wissens und Expertise von Privaten zurück. Die Zusammenarbeit mit Privaten ist zum Teil als gesetzlicher Auftrag ausgestaltet. Infolge der Einbindung und Übernahme verwaltungsexternen Wissens gibt der Staat Teile der Handlungskompetenz an private Akteure ab. Das besagt hingegen nicht, dass die Behörde dadurch gänzlich entlastet würde oder die Wissensgenerierungsprozesse externalisieren kann. In jedem Falle bedarf es eines spezifischen Nichtwissens, d. h. eines Meta-Wissens, um die Koordinierungsfunktion überhaupt einnehmen zu können und erfolgreich außeradministratives Wissen zu übernehmen. Die Behörde muss mit hochqualifiziertem Personal ausgestattet sein, schon um die Expertise in der Breite zu entwickeln und eine qualitative Auswahl bezüglich der in Betracht kommenden externen Sachverständigen bzw. der Vergabe spezifischer amtsbezogener Aufgaben treffen zu können. Eine unzulässige Indienstnahme der Privaten ist in der bisherigen Ausgestaltung der Kooperation nicht zu erkennen.

Eine wesentliche Grenze der staatlichen Informations- und Wissensproduktion bildet der Grundsatz der Selbstbelastungsfreiheit nicht. Dieser für Meldepflichten relevante Grundsatz schützt grundsätzlich davor, sich durch eine Information in die Gefahr einer staatlichen Sanktion zu begeben. Allerdings schützt der Grundsatz nicht absolut und steht der Meldepflicht als solcher nicht entgegen. Sinnvoll erscheint es hier im Sinne eines Anreizes zur Erfüllung der Meldepflichten, systematisch einheitlich Verwendungsbeschränkungen zu regeln.

Dem Datenschutzrecht kommt als Regulativ kalkulierten Nichtwissens begrenzende Wirkung auf die Informationsgenerierung zu, sofern es anwendbar ist. Dies hängt insbesondere davon ab, ob Maschinendaten als personenbezogene Daten einzuordnen sind. Maßgeblich ist, ob mit rechtlichen Mitteln ein Zusatzwissen eingeholt werden kann, mit dem die Herstellung eines Personenbezugs möglich ist. Werden die von den Unternehmen und der NIS-Verwaltung verarbeiteten Daten als personenbezogene Daten qualifiziert, bestehen jedoch Rechtsgrundlagen, auf die sich Maßnahmen der Sicherheitsgewährleistung stützen können. Prinzipiell erkenntnishemmend wirkt bei Anwendung des Datenschutzrechts der Grundsatz der Datenminimierung. Kleinere Datenmengen erfordern mehr Wissen darüber, welche Erkenntnisse angestrebt werden. Dagegen bestehen bei größeren Datenmengen mehr Verknüpfungsmöglichkeiten, die zusätzliches Wissen durch nicht vorhersehbare Korrelationen entstehen lassen können.

Vor dem Hintergrund der prinzipiell geringen Eingriffstiefe ist die Verarbeitung mit dem allgemeinen Datenschutz vereinbar. Die Grundsätze zur Zweckbestimmung und Datenminimierung sind eingehalten und daher die Schaffung eines Datenschutzregimes mit höherer Regelungsdichte, trotz Öffnungsklauseln in der DS-GVO, nicht angezeigt.

Schließlich kommt dem Schutz von Unternehmensgeheimnissen grundsätzlich begrenzende Wirkung zu. Sicherheitsbezogene Informationen wie etwa unternehmensintern detektierte Sicherheitslücken können geschützte Betriebs- und Geschäftsgeheimnisse sein. Eingriffe in die Berufsfreiheit und das normgeprägte Eigentumsrecht sind jedoch gerechtfertigt, wenn sie sich auf eine gesetzliche Grundlage stützen und verhältnismäßig sind. Dem Geheimhaltungsinteresse der betroffenen Unternehmen wird im Rahmen der Meldepflichten von Betreibern kritischer Infrastrukturen durch ein abgestuftes Meldeverfahren und im Übrigen durch das Verwaltungsgeheimnis, das die Verwaltung verpflichtet, geschützte Geheimnisse nicht unbefugt zu offenbaren, Rechnung getragen.

Eine signifikante Grenze für die Generierung von Informationen stellen der Daten- und Unternehmensdatenschutz für die verhältnismäßige Datenverarbeitung zum Zwecke der Gewährleistung der Netz- und Informationssicherheit nach allem nicht dar.

§ 4 Transfer von Informationen im Rahmen der europäischen Zusammenarbeit zur Gewährleistung der Netz- und Informationssicherheit

Im vorangegangenen Kapitel wurde untersucht, welche NIS-Akteure mit welchen rechtlichen Instrumenten im Bereich der Netz- und Informationssicherheit Informationen generieren, um daraus entscheidungsrelevantes Wissen zu produzieren. Zu einer für die effektive Gewährleistung der Sicherheit ausreichenden Breitenwirkung führt das Wissen aber erst, wenn es zwischen den relevanten Akteuren geteilt und weitergegeben wird. Vor allem aufgrund der Bedeutung für den europäischen Binnenmarkt kommt dem auf Gegenseitigkeit beruhenden Informationsaustausch zur Gewährleistung der Internetsicherheit eine besondere Bedeutung zu.

Mit Blick auf die europäische Dimension der Netz- und Informationssicherheit verdienen die Regelungen über den Transfer der generierten Informationen und den Austausch von Wissen besondere Aufmerksamkeit, da die Weitergabe von Informationen eine zentrale Funktionsbedingung für die unionsweite Kooperation im Bereich der Internetsicherheit ist (A.). Der Informationsaustausch im Rahmen der NIS-Richtlinie, die die wesentliche Struktur der NIS-Zusammenarbeit vorgibt, findet aufgrund verschiedener Informationsaustauschmechanismen im vertikalen wie horizontalen Verhältnis statt und wird vor allem durch primärrechtliche Kooperationspflichten gefördert (B.). Besondere Grenzen des Informationsaustausches ergeben sich vor allem aus dem Schutz personen- wie unternehmensbezogener Daten, den Besonderheiten in der organisationsrechtlichen Gestaltung der NIS-Akteure und dem Informationsverweigerungsrecht der Mitgliedstaaten (C.).

A. Funktion des Informationstransfers für die Sicherheitsgewährleistung

Im Nachfolgenden wird aufgezeigt, dass der europäische Verwaltungsverbund eine kognitive Dimension aufweist (I.). Der Blick auf das Sicherheitsverwaltungsrecht im Allgemeinen und auf die europäische Zusammenarbeit im Bereich der Sicherheit von Netzen und Informationssystemen im Besonderen zeigt, dass Sicherheit auch und vor allem mit informationsverwaltungsrechtlichen Mitteln gewährleistet wird (II.).

I. Kognitive Dimension des Europäischen Verwaltungsverbunds

Mit der voranschreitenden technischen und rechtlichen Internationalisierung gehört das Wissensmanagement in zunehmendem Maße zu den zentralen Aufgaben des Verwaltungsrechts.[1] Insbesondere im europäischen Kontext zeigt sich in sachlicher Hinsicht das Bedürfnis nach einer Verzahnung der Rechtsordnungen und -ebenen. Die Integrationsprozesse erfordern daher verwaltungsrechtliche Strukturen für einen Informationsaustausch außerhalb des jeweils eigenen Verfügungsbereichs.[2] Kompetenzen mögen in auswärtigen Angelegenheiten zwar weiterhin nach dem „Erfordernis der Einheitlichkeit des staatlichen Auftretens" bei der Regierung monopolisiert sein,[3] die Behörden hingegen kommunizieren zunehmend untereinander und ebenenübergreifend.[4]

Der hierarchische Aufbau als herkömmliches Instrument zur Bewältigung von Komplexität kommt in einem verfassungsbedingten Mehrebenengefüge, dessen Verwaltungsverfahren sich durch eine polyzentrische Architektur auszeichnen, kaum in Betracht.[5] Aufgefangen wird die Komplexitätssteigerung des europäischen Verwaltungsrechts durch die Konzeption komplexerer Vollzugsmodelle. Die Verschaltung der Vollzugsstrukturen wird durch deskriptiv-analy-

---

[1] *Hofmann*/*Rowe*/*Türk*, Administrative Law and Policy of the European Union, 2011, S. 411; vgl. *Augsberg*, Informationsverwaltungsrecht, 2014, S. 24.

[2] *Schmidt-Aßmann*, Der Staat 45 (2006), 315 (315 ff.); vgl. *Möllers*/*Terhechte*, Europäisches Verwaltungsrecht und Internationales Verwaltungsrecht, in: Terhechte (Hrsg.), Verwaltungsrecht der Europäischen Union, 2011, § 40; *Slaughter*, Global Government Networks, Global Information Agencies, and Disaggregated Democracy, in: Ladeur (Hrsg.), Public Governance in the Age of Globalization, 2004, S. 121 ff.

[3] *Möllers*, ZaöRV 65 (2005), 351 (352).

[4] Vgl. zur Entwicklung vom bilateralen zum automatisierten steuerlichen Informationsaustausch *Czakert*, DStR 2015, 2697 (2697 f.).

[5] Zu hierarchischen Organisationsformen *Baecker*, Organisation als System, 1999, S. 221 ff.; allgemein *Slaughter*, A new world order, 2004.

tische Metaphern beschrieben.[6] Begriffe wie Verwaltungsverbund[7], Multi-Level-Governance[8] oder Informationsverbund[9] sollen die beobachtbaren Strukturen einfangen und operationalisieren. Eine strikte Trennung der Vollzugsformen ist kaum möglich, weil in den netzwerkartigen Strukturen gemeinsame Verfahren praktiziert werden und es zu sich intensivierenden Verknüpfungen und Kooperationen der Verwaltungen kommt.[10] Infolge der sich herausbildenden komplexen Verwaltungszusammenhänge verschwimmt die herkömmliche Trennung der Vollzugsarten im europäischen Verwaltungsrecht.[11]

Im Sinne einer kognitiven Konzeptualisierung kann der europäische Verwaltungsverbund insgesamt als Lernverbund begriffen werden.[12] Diese Konzeptualisierung berücksichtigt den Umstand, dass die Verwaltungskooperation vielfach über den Austausch von Einzelinformationen hinausgeht. Gegenstand der Kooperation sind auch Wissen, Kompetenzen und Erfahrungen, die häufig nicht kodifiziert, sondern eher unbewusst und implizit vorhanden sind. Als Charakteristikum des Informationsverwaltungsrechts verweist das Konzept des Lernverbunds darauf, dass und wie Verwaltungen lernen, ihr Handeln im Lichte neuer Kenntnisse und Einsichten zu verändern, zu entwickeln und zu wandeln.[13] Die Perspektive des Lernens tritt vor allem dann in Erscheinung, wenn die (selbst-

---

[6] Vgl. *Kahl*, Der Staat 50 (2011), 353 (354 f.); *Britz*, EuR 2006, 46 (47); für den Bereich der Telekommunikation *Trute*, Der europäische Regulierungsverbund in der Telekommunikation, in: Osterloh/Schmidt/Weber (Hrsg.), Staat, Wirtschaft, Finanzverfassung: Festschrift für Peter Selmer, 2004, S. 565 ff.

[7] *Schmidt-Aßmann*, Der Europäische Verwaltungsverbund und die Rolle des Europäischen Verwaltungsrechts, in: ders./Schöndorf-Haubold (Hrsg.), Der Europäische Verwaltungsverbund, 2005, S. 1 (16 f.).

[8] Zur Verfasstheit öffentlicher Gewalt in Mehrebenensystemen *Pernice*, Multilevel Constitutionalism and the Treaty of Amsterdam, CMLR 6 (1999), 703 (703 ff.).

[9] *Von Bogdandy*, Die Informationsbeziehungen im europäischen Verwaltungsverbund, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrecht, Band II, 2. Aufl. 2012, § 25 Rn. 106 f.

[10] *Schneider*, NVwZ 2012, 65 (65).

[11] *Stelkens*, in: ders./Bonk/Sachs (Hrsg.), VwVfG, 8. Aufl. 2014, Europäisches Verwaltungsrecht, Europäisierung des Verwaltungsrechts und Internationales Verwaltungsrecht, Rn. 120, 177 ff.

[12] *Eifert*, Europäischer Verwaltungsverbund als Lernverbund, in: Spiecker gen. Döhmann/Collin (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, 2008, S. 159 (159 ff.); *ders.*, Regulierte Selbstregulierung und die lernende Verwaltung, in: Berg (Hrsg.), Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates, Die Verwaltung, Beiheft 4, 2002, S. 137 (137 ff.); zum Europäischen Mehrebenensystem als Lernchance *Kaiser*, Wissensmanagement im Mehrebenensystem, in: Schuppert/Voßkuhle (Hrsg.), Governance von und durch Wissen, 2008, S. 217 (223 ff.).

[13] Für den betriebswirtschaftlichen Vorlauf des Konzepts lernender Organisationen *Garvin*, Harvard Business Manager 1/1994, 74 (76).

ständigen) Verwaltungseinheiten „vom Recht in (Informations-)Beziehungen gesetzt werden".[14] Eine Leitbildfunktion für die behördliche Wissensproduktion im Unionsrecht kann den Verpflichtungen zur „guten Verwaltung" zukommen. Neben Art. 41 GRCh, der in einem engeren Sinne die Außenbeziehungen der Verwaltung betrifft,[15] sind allgemeine Rechtsgrundsätze wie die „gute Verwaltungsführung" und „ordnungsgemäße" Verwaltung anerkannt.[16] Dies gilt für die Informationsgenerierung zumindest insoweit, als durch prozedurale Mechanismen wie den Untersuchungsgrundsatz versucht wird, rechtsstaatliche Rationalität zu gewährleisten.[17] In Bereichen wie der Bankenregulierung wird die Lernorientierung ganz besonders im Kontext der *cognitive governance* betrachtet und gar für die Bewertung der Leistungsfähigkeit der Risikoregulierung herangezogen.[18]

Die europäische Verwaltung ist außerdem im Vergleich zu den nationalstaatlichen Verwaltungen in besonderem Maße auf Informationen, Wissen und Lernen angewiesen. Je nach Regelungsbereich kann auf europäischer Ebene das Recht nur durch Informationen durchgesetzt werden. Soweit der europäischen Exekutive Rechts- und Fachaufsichtsbefugnisse fehlen, sind Informationspflichten und Informationsrechte die zentralen Herrschaftsinstrumente.[19] Dem Informationsverwaltungsrecht kommt insofern auch eine Kompensations- und Ausgleichsfunktion zu.[20] Insofern ist die Union „zuallerst Informationsverwaltung"[21] und das auf Francis Bacon zurückgehende Weber'sche Diktum von der

---

[14] *Eifert*, Europäischer Verwaltungsverbund als Lernverbund, in: Spiecker gen. Döhmann/Collin (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrecht, 2008, S. 159 (160).

[15] *Magiera*, in: Meyer (Hrsg.), Charta der Grundrechte der Europäischen Union, 4. Aufl. 2014, Art. 41 Rn. 7.

[16] Vgl. *Kopp*/*Raumsauer*, VwVfG, 16. Aufl. 2015, § 24 Rn. 3b.

[17] *Voßkuhle*, Sachverständige Beratung des Staates, in: Isensee/Kirchhof (Hrsg.), HbStR III, 3. Aufl. 2005, § 43, Rn. 1.

[18] Siehe *Kette*, Bankenregulierung als Cognitive Governance, 2008, S. 26, zur „Kognitivierung von Regulierungsprogrammen" und deren Folgeprobleme; allgemein *Strulik*, Cognitive Governance, in: Schuppert /Voßkuhle (Hrsg.), Governance von und durch Wissen, 2008, S. 87 ff.; ferner *Schuppert*, Governance durch Wissen, in: ders./Voßkuhle (Hrsg.), Governance von und durch Wissen, 2008, S. 259 (264 ff.); Allgemeiner *Ladeur*, Der Staat 48 (2009), 163 (177, 183 ff.); *Willke*, Smart Governance: governing the Global Knowledge Society, 2007, S. 34 ff., 130 ff.

[19] *Von Bogdandy*, Die Informationsbeziehungen im europäischen Verwaltungsverbund, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band II, 2. Aufl. 2012, § 25 Rn. 5.

[20] *Sommer*, Verwaltungskooperation am Beispiel administrativer Informationsverfahren im Europäischen Umweltrecht, 2003, S. 508 ff.

[21] *Schmidt-Aßmann*, Europäische Verwaltung zwischen Kooperation und Hierarchie, in:

Herrschaft der bürokratischen Verwaltung als „Herrschaft kraft Wissen" nicht überholt.[22] Art. 114 Abs. 3 S. 1 AEUV macht deutlich, dass bereits die Politikentwicklung wissensbasiert ist. In ihren Vorschlägen von Maßnahmen zur Harmonisierung des Binnenmarktes geht die Kommission unter anderem im Bereich der Sicherheit von einem hohen Schutzniveau aus und „berücksichtigt dabei insbesondere alle auf wissenschaftliche Ergebnisse gestützten neuen Entwicklungen."

Wissen kann nur dann wirksam nutzbar gemacht werden, wenn es den relevanten Akteuren zur Verfügung steht. Sie können Informationen in neue Kontexte setzen, sodass neue Erkenntnisse gefördert werden. Im Verhältnis zur Wissensgenerierung kommt dem Informationsaustausch keine nachrangige, sekundäre Funktion zu.[23] Im europäischen Mehrebenensystem ist die Gestaltung des Informationsverwaltungsrechts als rechtlich dirigierte Informationsverteilung ein Hauptanliegen, um den Vollzug des Unionsrechts einheitlich und effizient zu organisieren.[24] Der in Art. 4 Abs. 3 EUV zum Ausdruck kommende Grundsatz der loyalen Zusammenarbeit zeigt, dass das Paradigma der Trennung nationaler und unionaler Verwaltung nicht dominieren kann. Um die Ziele in Art. 3 EUV zu verwirklichen, müssen die europäischen Verwaltungen kooperieren.[25] Informationsaustausch ist der Anfang der Kooperation. Der kollaborative und koordinative Informationsaustausch führt nämlich zu einer Wechselwirkung, die das „Wissen der Verwaltung […] fortlaufend reflexiv weiterentwickelt".[26] Der „Zugriff auf Informationen [und] Sachwissen" sowie „gegenseitige Lernprozesse" sind daher gleichsam Ziele des europäischen Verwaltungsverbunds.[27]

Cremer et al. (Hrsg.), Tradition und Weltoffenheit des Rechts – Festschrift für Helmut Steinberger, 2002, S. 1375 (1391).

[22] *Weber*, Wirtschaft und Gesellschaft, in: *Winckelmann* (Hrsg.), Nachdr. 5. Aufl. 2013, S. 129; vgl. mit Blick auf spezifisch moderne Problemstellungen ferner *Wolf*, „Herrschaft kraft Wissen" in der Risikogesellschaft, Soziale Welt 39 (1988), 164 ff.

[23] *Augsberg*, Informationsverwaltungsrecht, 2013, S. 80; *Spiecker gen. Döhmann*, Wissensverarbeitung im Öffentlichen Recht, Rechtswissenschaft 2010, 247 (270).

[24] Mit Bezug auf den Aufbau eines Informationsnetzwerks *Terhechte*, Europäisches Verwaltungsrecht und europäisches Verfassungsrecht, in: ders. (Hrsg.), Verwaltungsrecht der Europäischen Union, § 7, Rn. 29; vgl. *Augsberg*, Informationsverwaltungsrecht, 2013, S. 80, 100.

[25] *Schmidt-Aßmann*, EuR 1996, 270 (290); *ders.*, Aufgaben und Perspektiven verwaltungsrechtlicher Forschung, 2006, S. 431.

[26] *Eifert*, Europäischer Verwaltungsverbund als Lernverbund, in: Spiecker gen. Döhmann/Collin (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, 2008, S. 159 (159).

[27] Zum Verfassungsverbund und Verfassungsnetzwerk *Pernice*, La Rete Europea di Costituzionalità – Der Europäische Verfassungsverbund und die Netzwerktheorie, ZaöRV 70 (2010), 51 (61).

II. Verwaltungskooperation im Bereich Sicherheit von Netz- und Informationssystemen

Am Beispiel des europäischen Sicherheitsverwaltungsrechts lässt sich darstellen, dass der Rückgriff auf europäische Informationskooperation und Informationsverwaltungsrecht auch der Effektivierung der nationalen Sicherheitsbemühungen dient (1.). Die hier relevante europäische Zusammenarbeit zur Gewährleistung der Sicherheit von Netzen und Informationssystemen ist in ähnlicher Weise als Gewährleistung der Sicherheit mit informationsverwaltungsrechtlichen Mitteln angelegt (2.).

1. Europäisches Sicherheitsverwaltungsrecht als Informationsverwaltungsrecht

Das europäische Sicherheitsrecht hat sich in besonderem Maße zu einem Bereich entwickelt, in welchem die informationelle Vernetzung im vertikalen, horizontalen und diagonalen Verhältnis verdichtet ist. Für den Informationsaustausch zur präventiven Gefahrenabwehr und zur repressiven Strafverfolgung wurde der Begriff des europäischen Sicherheitsverwaltungsrechts geprägt.[28] Gemeint ist die Gewährleistung der Sicherheit innerhalb der EU mit verwaltungsrechtlichen Mitteln. Die Entwicklung der europäischen Sicherheitsverwaltung geht auf intergouvernementale Komplementärmaßnahmen zur Errichtung des Binnenmarktes zurück. Mit der Vergemeinschaftung, Institutionalisierung und schließlich der Aufgabe der Säulenstruktur mit dem Vertrag von Lissabon hat sich die Sicherheitsverwaltung dann zunehmend im Politikbereich des Raums der Freiheit, der Sicherheit und des Rechts (Art. 67 ff. AEUV) emanzipiert.[29] Während es in nationalen Kontexten den Behörden um die Gewährleistung innerer Sicherheit und der Abwehr konkreter Gefahren geht, ist Gegenstand der europäischen Sicherheitsgewährleistung hauptsächlich die Zusammenarbeit, die Unterstützung und die Koordinierung der innerstaatlichen Sicherheitsbemühungen. Die Zuständigkeiten der Mitgliedstaaten werden dabei geschont, Kompetenzen werden grundsätzlich weder übertragen noch ersetzt. Europäisches Sicherheitsverwaltungsrecht ist daher in erster Linie als Informationsverwaltungs- bzw. Verwaltungskooperationsrecht ausgeprägt, das den einzelstaatlichen Behörden die Zusammenarbeit ermöglicht und diese organisiert.[30]

---

[28] *Schöndorf-Haubold*, Europäisches Sicherheitsverwaltungsrecht, 2010.

[29] *Schöndorf-Haubold*, Europäisches Sicherheitsverwaltungsrecht, in: Terhechte (Hrsg.), Verwaltungsrecht der Europäischen Union, 2011, § 35 Rn. 17.

[30] *Schöndorf-Haubold*, Das Recht der Zivilen Sicherheit an der Schnittstelle von nationaler, europäischer und internationaler Zuständigkeit, in: Gusy/Kugelmann/Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, 2017, S. 691 (704); dazu ferner *Schmidt-Aßmann*,

Das Informationskooperationsrecht geht mitunter über die bloße Koordinierung hinaus, im Rahmen derer die Abstimmung auf horizontaler Ebene über Politiken und Aufgabenwahrnehmung stattfindet. Dabei geht es um das Zusammenwirken des nationalen Verwaltungsrechts, des unionalen Eigenverwaltungsrechts und des Unionsrechts zur gemeinsamen Aufgabenerfüllung.[31]

Die zahlreichen Informationssysteme in der Sicherheitsverwaltung (als Beispiele können die Informationsverwaltung durch Europol[32] [TECS] oder das Schengener Informationssystem genannt werden) verfügen in der Regel über keine echten Eingriffsbefugnisse oder Befugnisse zur Erhebung von Daten und Informationen. Europäischen Informationsverfahren und -systemen kann allerdings eine wichtige „Kompensations-, Sicherheits- und Auffangfunktion" zugeschrieben werden.[33]

Das Schengener Informationssystem (SIS) etwa gleicht den nationalen Verlust nationaler Vollzugskompetenzen und -instrumente aus, der aus dem Wegfall der Grenzkontrollen im Schengenraum resultiert. Das Informationssystem schafft Vorkehrungen für eine informatorisch abgesicherte grenzüberschreitende Aufsicht.

Europäische Warnsysteme wie das Lebensmittelwarnsystem (RASFF) fungieren als Sicherheitsnetz für Gefahren, die von unionsweit zugelassenen oder zulassungsfrei vermarkteten Produkten ausgehen, indem über die Kommission sternförmig Warnmitteilungen bei Gefahren ausgegeben werden. Die Mitgliedstaaten können Gegenmaßnahmen ergreifen, diese sind aber im Informationssystem bekannt zu geben.

Das TRACES-System fängt die mögliche europäische Reichweite von Tiertransporten auf und erweitert den Schutz, indem Tiertransporte informationell erfasst werden und grenzüberschreitende Besitz- und Eigentumswechsel unabhängig vom Wissensstand der letzten Tierbesitzer dokumentiert werden, um potenzielle Verbreitungspfade von Tierseuchen zu klären.

EuR 1996, 270 (290); *ders*., Aufgaben und Perspektiven verwaltungsrechtlicher Forschung, 2006, S. 431.

[31] Vgl. *Schmidt-Aßmann*, Das allgemeine Verwaltungsrecht als Ordnungsidee, 2. Aufl. 2006, S. 388 f.; zur Entwicklung siehe *Sydow*, Verwaltungskooperation in der Europäischen Union, 2004, S. 14 ff.; vgl. *Pitschas*, Europäisches Verwaltungsverfahrensrecht und Handlungsformen der gemeinschaftlichen Verwaltungskooperation, in: *Hill/ders.* (Hrsg.), Europäisches Verwaltungsverfahrensrecht, 2004, S. 301 f., 324.

[32] *Schoppa*, Europol im Verbund der Europäischen Sicherheitsagenturen, 2013, S. 95 ff.

[33] Dazu und zum Folgenden *Schneider*, NVwZ 2012, 65 (65 f.); ähnlich *Schmidt-Aßmann*, Verfassungsprinzipien für den Europäischen Verwaltungsverbund, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band I, 2. Aufl. 2012, § 5 Rn. 16.

2. Informationskooperation zur Gewährleistung der Netz- und Informationssicherheit

Um die Effekte der Liberalisierung zu absorbieren, richten sich die Steuerungsbemühungen der Kommission auch im Bereich der Netz- und Informationssicherheit schon früh darauf, die auf nationaler Ebene verschiedenen, dezentralen Regulierungen auf europäischer Ebene durch Informationsaustausch zu koordinieren und zu integrieren.[34] Vom Anspruch und vom Ansatz her schafft die Richtlinie 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie) die wesentlichen rechtlichen Rahmenbedingungen dafür, eine informationelle Kooperation zu etablieren.

Dem Gesetzgebungsverfahren zur NIS-Richtlinie ist ein aufwendiger Konsultationsprozess vorausgegangen. Die Kommission hat in ihrer Wirkungsabschätzung zur Richtlinie festgestellt, dass aus Gründen unterschiedlicher NIS-Kapazitäten in den Mitgliedstaaten auf europäischer Ebene ein unzureichender Informationsaustausch über Sicherheitsvorfälle, Risiken und Bedrohungen besteht.[35] Das fragmentierte Vorgehen in den Mitgliedstaaten führte im Verhältnis zur hohen Integrationsdichte der digitalen Infrastrukturen in Europa zu einem unzureichenden europäischen Sicherheitsniveau. Die NIS-Richtlinie reagiert auf den fehlenden Mechanismus der vertrauensvollen Zusammenarbeit über Sicherheitsvorfälle und -risiken.[36] Dementsprechend verfolgt die NIS-Richtlinie den Zweck, einen Rahmen für die Zusammenarbeit und den Informationsaustausch zwischen den Mitgliedstaaten und den Computer-Notfallteams (CSIRTs) zu schaffen (Art. 1 Abs. 2 und Kapitel 3 NIS-RL).[37]

Die Zusammenführung verteilten Wissens durch den Austausch von Informationen kann zu konkreten und nutzbaren Erkenntnissen sowie zu einer differenzierteren Lageeinschätzung führen. Die Zusammenführung von Informationen ist sicherheitstechnisch sinnvoll, da internationale Angriffe in den verschiedenen Mitgliedstaaten regelmäßig auf denselben Methoden und Angriffswegen beruhen und unter Verwendung derselben Systeme durchgeführt werden. Durch informationelle Kooperation auf dem Gebiet der Netz- und Informationssicherheit können schneller Handlungsmuster erkannt und wirksamer Gegenmaßnah-

---

[34] Vgl. *Wiater*, Sicherheitspolitik zwischen Staat und Markt, 2013, S. 210 ff.; vgl. zur NIS-Politik der Kommission die Kommunikation „Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", COM(2009) 149 final, S. 6.

[35] *Kommission*, Commission Staff Working Document, Impact Assessment, SWD (2013) 32 final, S. 25.

[36] Vgl. Entwurf einer NIS-RL, COM(2013) 48 final, S. 3.

[37] Siehe auch Erwägungsgründe 6, 43, 59 NIS-RL.

men eingeleitet werden. Andernfalls müssten alle Akteure und Institutionen selbst relevante Informationen zusammentragen und auswerten. Ausgehend von diesem Ansatz zielt der europäische Informationsaustausch also darauf, eine Wissensgemeinschaft (*epistemic community*) zu bilden und so die Beschränkungen aufgrund der nur begrenzten Rationalität (*bounded rationality*), denen Individuen wie Organisationen unterliegen und unter deren Bedingungen diese zu einer selektiven Berücksichtigung vorhandener Informationen neigen,[38] partiell aufzuheben.

B. Struktur des Informationsaustausches

Nachdem für die europäische Verwaltung im Bereich der Netz- und Informationssicherheit das Informationsverwaltungsrecht als zentrale Funktionsbedingung ausgemacht wurde, ist nun zu untersuchen, in welchen informationsverwaltungsrechtlichen Strukturen der Informations- und Wissenstransfer erfolgt.

Je nach Integrationsdichte findet der europäische Informationsaustausch im Wege verschiedener Bausteine europäischen Informations- und Wissensaustausches statt (I.). Der Austausch von Informationen und Wissen im Rahmen der NIS-Kooperation beschränkt sich angesichts der vergleichsweise geringen Integration nicht auf einen der Mechanismen (II.). Gefördert wird der Informationsaustausch im Bereich der Netz- und Informationssicherheit durch primärrechtliche Kooperationspflichten (III.).

I. Formen des europäischen Informationstransfers

Ein einheitliches europäisches Verfahrens- und Organisationsrecht, das als Folie für die weitere Untersuchung herangezogen werden könnte, besteht mangels vereinheitlichter Kodifizierung nicht. Die rechtliche Struktur eines europäischen Informationsaustausches ist dem Verfahrens- und Organisationsrecht des jeweils eine Regelungsmaterie betreffenden Sekundärrecht zu entnehmen (1.). Phänomenologisch lassen sich aber Grundtypen des Informationsaustausches ausmachen (2.).

---

[38] Vgl. *Schneider*, Vorüberlegungen zum Informationsmanagement in europäischen Verwaltungsverfahren, in: Lipowicz/Schneider (Hrsg.), Perspektiven des deuschen, polnischen und europäischen Informationsrechts, S. 163 mit Verweis auf *Simon*, Organization Science 1991, 125 ff.

1. Vielgestaltigkeit europäischer Informationsaustauschverfahren

Der Informationsaustausch kann grundsätzlich vertikal, d. h. zwischen mitgliedstaatlichen Behörden und unionalen Stellen, horizontal, d. h. zwischen Behörden und unterschiedlichen Mitgliedstaaten, sowie diagonal, d. h. unter Einschaltung von Informationsagenturen,[39] verlaufen.[40] Die Gestaltung eines europäischen Informationsaustausches ist jedoch nicht durch ein europäisches Verfahrensrecht vorgegeben. Weder ist das Verfahrensrecht der Unionsorgane einheitlich kodifiziert noch sind die Verfahrensgesetze in den Mitgliedstaaten aufeinander abgestimmt.[41] Einige Mitgliedstaaten haben gar keine gesetzlichen Bestimmungen über das Verwaltungsverfahren. Die Kommission hat grundsätzlich auch nicht die Kompetenzen einer Fach- und Rechtsaufsichtsbehörde.[42] Auch sonst steht ihr grundsätzlich kein ungeschriebenes, allgemeines Weisungsrecht zu, mit dem sie einen bestimmten Informationsaustausch veranlassen könnte. Die rechtliche Erfassung und Analyse des institutionalisierten Informationsmanagements in europäischen Verwaltungsverfahren steht insofern immer noch am Anfang.[43]

Der Vollzug einer Informationskooperation folgt daher im Ausgangpunkt grundsätzlich den unionsrechtlichen Vollzugsprinzipien: dem Trennungsprinzip einerseits und dem Kooperationsprinzip andererseits.[44] Die europäische Verwaltung ist außerhalb des Eigenverwaltungsrechts der EU für die Durchsetzung des Unionsrechts auf die mitgliedstaatlichen Behörden angewiesen.[45]

---

[39] *Kahl*, Der Europäische Verwaltungsverbund: Strukturen – Typen – Phänomene, Der Staat 50 (2011), 353 (354 ff.).

[40] *Augsberg*, Informationsverwaltungsrecht, 2014, S. 92; *Schmidt-Aßmann*, EuR 1996, 270 (273). Entscheidungsvernetzungen werden im „inner-unionalen" Bereich auch als „intervertikal" oder „interhoriziontal" bezeichnet, so etwa *Siegel*, Entscheidungsfindung im Verwaltungsverbund, 2009, S. 320 f.

[41] Vgl. nunmehr den ReNEUal-Musterentwurf (ME) für ein EU-Verwaltungsverfahrensrecht. *Schneider/Hofmann/Ziller* (Hrsg.), ReNEUAL-Musterentwurf für ein EU-Verwaltungsverfahrensrecht, 2015. Dazu *Lenz*, NVwZ 2016, 38 (38 ff.). Der ME soll im Übrigen nicht für mitgliedstaatliche Behörden gelten, soweit er nicht für anwendbar erklärt wird (Art. I-1 ME).

[42] *Hatje*, Die gemeinschaftsrechtliche Steuerung der Wirtschaftsverwaltung, 1998, S. 156 ff.

[43] *Schneider*, Vorüberlegungen zum Informationsmanagement in europäischen Verwaltungsverfahren, in: Lipowicz/ders. (Hrsg.), Perspektiven des deutschen, polnischen und europäischen Informationsrechts, 2011, S. 159 (186).

[44] Dazu *Augsberg*, Europäisches Verwaltungsorganisationsrecht und Vollzugsformen, in: Terhechte (Hrsg.), Verwaltungsrecht der Europäischen Union, 2011, § 6 Rn. 8; für den prinzipiellen Vorrang des mitgliedstaatlichen Vollzugs *von Danwitz*, Europäisches Verwaltungsrecht, 2008, S. 303.

[45] *Priebe*, Die Aufgaben des Rechts in einer sich ausdifferenzierenden EG-Administra-

Liegt für einen Regelungsbereich die Kernzuständigkeit bei den Mitgliedstaaten, resultiert eine dezentrale Verwaltungsstruktur. Eine solche Struktur ist eng verbunden, aber nicht gleichbedeutend mit dem indirekten Vollzug des Unionsrechts. Demnach wenden mitgliedstaatliche Behörden nationales Recht an, das jedoch durch das EU-Recht inhaltlich determiniert ist (mittelbar mitgliedstaatlicher Vollzug). Im Bereich des indirekten Vollzugs obliegt es nach Art. 291 Abs. 1 AEUV den Mitgliedstaaten, das Unionsrecht auszuführen (Trennungsprinzip).

Soweit Mitgliedstaaten das Vollzugsrecht aufgrund ihrer Verwaltungsautonomie selbst gestalten und eigene Verfahren der Informationsgenerierung und des Informationstransfers festlegen, haben sie die Prinzipien der einheitlichen Anwendung des Unionsrechts zu beachten. Die nationalen Gesetze haben insbesondere dem Äquivalenzprinzip und dem Effektivitätsprinzip zu genügen.[46] Eine nationale Stelle, die unionsrechtlich eine Informationspflicht trifft, kann sich aufgrund des auf dem Effektivitätsgebot folgenden Vereitelungsverbots nicht auf das Fehlen hinreichender nationaler Befugnisnormen berufen.[47]

Die Rechtsgrundlagen zum interadministrativen Transfer von Informationen sind also entweder dem anwendbaren Unionsrecht oder dem nationalen Recht zu entnehmen.[48] Für die Untersuchung des Vollzugs einer Informationskooperation ist daher das jeweils konkretisierte Verfahrens- und Organisationsrecht einer Regelungsmaterie maßgebend.

---

tion, in: Schmidt-Aßmann/Hoffmann-Riem (Hrsg.), Strukturen des Europäischen Verwaltungsrechts, 1999, S. 71 f.

[46] EuGH, verb. Rs. C-205-215/82; EuGH, C-392/04 und C-422/04, Rn. 57. Dazu *Stelkens*, in: ders./Bonk/Sachs (Hrsg.), VwVfG, 8. Aufl. 2014, Europäisches Verwaltungsrecht, Rn. 96 f.; *Sydow*, Verwaltungskooperation in der Europäischen Union, 2004, S. 105 (Fn. 23); vgl. *Hombergs*, Europäisches Verwaltungskooperationsrecht auf dem Sektor der elektronischen Kommunikation, 2006, S. 72; *Ohler*, Europäisches und nationales Verwaltungsrecht, in: Terhechte (Hrsg.), Verwaltungsrecht der Europäischen Union, 2011, § 9 Rn. 11.

[47] *Schneider*, Vorüberlegungen zum Informationsmanagement in europäischen Verwaltungsverfahren, in: Lipowicz/ders. (Hrsg.), Perspektiven des deutschen, polnischen und europäischen Informationsrechts, 2011, S. 159 (172), der weiter fragt, ob das unionale Vereitelungsgebot zu einem strengeren Gebot effektiver Informationshilfe auszubauen ist; vgl. auch *David*, Inspektionen als Instrument der Vollzugskontrolle im Europäischen Verwaltungsverbund, in: Schmidt-Aßmann/Schöndorf-Haubold (Hrsg.), Der Europäische Verwaltungsverbund, 2005, S. 237 (251).

[48] *Von Danwitz*, Europäisches Verwaltungsrecht, 2008, S. 312, 618; vgl. *Röhl*, Ausgewählte Verwaltungsverfahren, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band II, 2. Aufl. 2012, § 30 Rn. 48; vgl. *Galetta/Hofmann/Schneider*, European Public Law 20 (2014), 65 ff.

2. Grundtypen europäischer Informationsaustauschmechanismen

Die Grundform der grenzüberschreitenden behördlichen Zusammenarbeit ist die Amtshilfe.[49] Die Amtshilfe in Gestalt der Informationshilfe ist die klassische Form der Informationskooperation.[50] Die Informationshilfe erfolgt gemäß der Funktionsweise der Amtshilfe auf Ersuchen sowie *ad hoc*. Sie kommt damit bei spontanen Einzelfragen in den Verwaltungen zum Einsatz.[51] Die Informationshilfe dient ihrem Wesen nach der Unterstützung fremder Aufgaben auf Ersuchen hin und unterscheidet sich insofern von der gemeinsamen Aufgabenverantwortung.[52] Eine allgemeine primärrechtliche Rechtsgrundlage für die Amtshilfe ist allerdings nicht vorgesehen; sie resultiert auch nicht aus dem oben beschriebenen Grundsatz der loyalen Zusammenarbeit in Art. 4 Abs. 3 EUV.[53] Sie ist punktuell im Primärrecht[54] und in Richtlinien sowie Verordnungen[55] geregelt.

Von den Auskunftspflichten im Rahmen der anfragebezogenen Amtshilfe sind die Informationsbeschaffungspflichten zu unterscheiden. In der Regel handelt es sich um spezifizierte Mitteilungspflichten, die anlassbezogen oder anlassunabhängig ausgestaltet sein können. Eine nationale Behörde kann etwa auf Anfrage der Kommission verpflichtet sein, bei einem Unternehmen Informationen einzuholen.[56] Auskunftspflichten entstehen reaktiv aber auch bei einem Ersuchen von Seiten anderer Verwaltungseinheiten.[57] Unterrichtungspflichten, die eine Stelle verpflichten, von sich aus aktiv tätig zu werden, greifen, wenn ein bestimmter Tatbestand erfüllt ist.[58] Bei Berichtspflichten muss die relevante Information in qualifizierter Form, d. h. systematisch und umfassend, übermittelt werden.[59] Notifizierungspflichten haben die Eigenschaft, dass sie rechtsförmig sind und Rechtsfolgen auslösen können.[60] Pflichten zur Gewährung von Infor-

---

[49] Vgl. *Ohler*, Europäisches und nationales Verwaltungsrecht, in: Terhechte (Hrsg.), Verwaltungsrecht der Europäischen Union, 2011, § 9 Rn. 31.

[50] *Schöndorf-Haubold*, Europäisches Sicherheitsverwaltungsrecht, 2010, S. 91.

[51] *Wettner*, Die Amtshilfe im Europäischen Verwaltungsrecht, 2005, S. 141.

[52] *Wettner*, Die Amtshilfe im Europäischen Verwaltungsrecht, 2005, S. 190.

[53] *Kahl*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, 4. Aufl. 2011, EUV, Art. 4 Rn. 113 („allenfalls die Pflicht zur kooperationsfreundlichen Auslegung spezieller Vorschriften über eine Amts- oder Rechtshilfe"); *Hatje*, in: Schwarze/Becker/ders./Schoo (Hrsg.), EU-Kommentar, 3. Aufl. 2012, EUV, Art. 4 Rn. 79.

[54] Zum Beispiel Art. 105 Abs. 1 S. 2 AEUV.

[55] Art. 61 DS-GVO; vgl. §§ 8a ff. VwVfG.

[56] Zum Beispiel Art. 11 der Kartellverfahrens-Verordnung (EG) 1/2003.

[57] Zum Beispiel Art. 15 Abs. 4 der Abwasser-Richtlinie RL 91/271/EWG.

[58] Zum Beispiel Art. 8 der Informations-Richtlinie RL 98/34/EG.

[59] Zum Beispiel Art. 16 der Abwasser-Richtlinie RL 91/272/EWG.

[60] Zum Beispiel Art. 9 der Abfallverbringungs-Verordnung (EG) Nr. 1013/2006.

mationen bestehen zudem im Rahmen von Inspektionsrechten, wobei es sich um konkrete Instrumente der Vor-Ort-Kontrolle europäischer Aufsichtsstellen kraft sekundärrechtlicher Anordnung handelt.[61] Sie tragen zwar zur Informationsproduktion bei, haben aber den primären Zweck der Vollzugskontrolle.[62]

Das koordinierte Zusammenspiel unterschiedlicher Informationspflichten ist das eigentliche Charakteristikum der „Informationsverteilungsprozesse im Mehrebenengeflecht der EU".[63] Die Verkopplung und Integration der Mitteilungs- und Weiterleitungspflichten vollzieht sich über das immer häufiger eingesetzte Instrument der EU-Informationssysteme.[64] Darunter sind besonders intensive Formen grenzüberschreitender interadministrativer Verbindungen zu verstehen. Zu den Merkmalen gehört ein erhöhter Grad der Institutionalisierung und der Dauerhaftigkeit.[65] Im Bereich der Informationssysteme lösen sich die Regelungen zudem von der strikten Ausrichtung auf die mitgliedstaatliche Zusammenarbeit ab und es kommt zu einer eigenständigen europäischen Sicherheitsverwaltung mit einem Überbau europäischer Stellen.[66]

II. Ausgestaltung der Informationszusammenarbeit durch die NIS-Richtlinie

Gemessen an der Typologie europäischer Informationsaustauschverfahren ist die NIS-Informationskooperation in ihrer Grundstruktur dezentral angelegt. Sie geht über den Informationsaustausch im Wege der Informationshilfe hinaus, kann aber noch nicht als integriertes Informationssystem bezeichnet werden. In organisationsrechtlicher Hinsicht kann zwischen strategischem und operativem Informationsaustausch unterschieden werden (1.). In verfahrensrechtlicher Hinsicht vollzieht sich der Informationsaustausch anlass- und gegenstandsbezogen im vertikalen wie horizontalen Verhältnis (2.).

---

[61] *Ohler*, in: Streinz (Hrsg.), EUV/AEUV, 2. Aufl. 2012, AEUV, Art. 197 Rn. 5.

[62] *David*, Inspektionen als Instrument der Vollzugskontrolle im Europäischen Verwaltungsverbund, in: Schmidt-Aßmann/Schöndorf-Haubold (Hrsg.), Der Europäische Verwaltungsverbund, 2005, S. 237 ff.

[63] *Augsberg*, Informationsverwaltungsrecht, 2014, S. 93 f.

[64] *Schneider*, NVwZ 2012, 65 (65); zum weiteren Ausbau der Informationsaustauschinstrumente *Kommission*, Die Europäische Sicherheitsagenda, COM(2015) 185 final, S. 6.

[65] *Heußner*, Informationssysteme im Europäischen Verwaltungsverbund, 2007, S. 18 f.

[66] *Schöndorf-Haubold*, Europäisches Sicherheitsverwaltungsrecht, in: Terhechte (Hrsg.), Verwaltungsrecht der Europäischen Union, 2011, § 35 Rn. 6 f.; zu Beispielen für Informationssysteme bereits unter § 4 A. II. 1.

1. Organisationsrechtliche Ausgestaltung

Die informationelle Kooperation ist sowohl strategisch als auch operativ. Eine Kooperationsgruppe ist zur Unterstützung der strategischen Kooperation zwischen den Mitgliedstaaten auf europäischer Ebene eingerichtet (a). Ein Netzwerk von Computer-Notfallteams soll die schnelle und wirksame operative Kooperation der Mitgliedstaaten fördern (b). Der Informationsaustausch der Datenschutzbehörden und der Nachrichtendienste findet grundsätzlich außerhalb der NIS-Informationskooperation statt (c).

a) Strategischer Informationsaustausch in der Kooperationsgruppe

Für die strategische Zusammenarbeit sowie des Informationsaustausches zwischen den Mitgliedstaaten wird eine Kooperationsgruppe eingesetzt.[67] Sie soll den Informationsaustausch unterstützen und erleichtern und Vertrauen zwischen den Mitgliedstaaten aufbauen (Art. 1 Abs. 2 lit. b). Die NIS-Kooperationsgruppe setzt sich aus Vertretern der Mitgliedstaaten, der Kommission und der ENISA zusammen.[68] Die Kommission stellt das Sekretariat bereit. Weder die Kommission noch ein anderes vertretenes Organ übernimmt eine zentrale Funktion. Demnach handelt es sich bereits im Ausgangspunkt insgesamt um eine dezentrale Kooperation.

Die Organisation ist grundsätzlich offen. Andere Interessengruppen können auf Einladung der Kooperationsgruppe an der gemeinsamen Arbeit teilnehmen (Art. 11 Abs. 2 UAbs. 2 NIS-RL). In Betracht kommt insbesondere die Teilnahme an der sog. NIS-Plattform. Die Schaffung dieser öffentlich-privaten Plattform wurde mit der europäischen Cybersicherheitsstrategie angekündigt.[69] Darin sollen die „einschlägigen europäischen Interessenträger des öffentlichen und privaten Sektors" zusammengeführt werden, damit empfehlenswerte Cybersicherheitsverfahren in der gesamten Wertschöpfungskette ermittelt und günstigere Marktbedingungen geschaffen werden können. Die Plattform setzt sich aus drei Arbeitsgruppen zusammen, von denen die zweite sich mit dem Informationsaustausch, der Koordination bei Sicherheitsvorfällen und den Risikometriken für den Informationsaustausch beschäftigt.[70]

---

[67] Der ursprüngliche Entwurf der Kommission, COM(2013) 48 final sah in Art. 8 noch die Schaffung eines „Kooperationsnetzes" vor.

[68] Art. 11 Abs. 2 NIS-RL.

[69] Kommission, JOIN(2013) 1 final, S. 14 f.

[70] ENISA, NIS-Platform, abrufbar unter: https://resilience.enisa.europa.eu/nis-platform.

b) Operativer Informationsaustausch im CSIRTs-Netzwerk

Neben der Einrichtung der Kooperationsgruppe schafft die NIS-Richtlinie ein Netzwerk von Computer-Notfallteams (CSIRTs-Netzwerk, Art. 1 Abs. 2 lit. c NIS-RL). Das Netzwerk setzt sich aus Vertretern der mitgliedstaatlichen CSIRTs und des europäischen CERT-EU zusammen (Art. 12 Abs. 2 NIS-RL). Die Kommission ist an dem Netzwerk beteiligt, nimmt aber nur eine Beobachterposition ein. Die ENISA stellt das Sekretariat und unterstützt aktiv die Kooperation der CSIRTs. Die Aufgabe des Netzwerks ist es, eine rasche und wirksame operative Zusammenarbeit zwischen den Mitgliedstaaten zu fördern. Zu den Kernaufgaben des Netzwerks gehört der Informationsaustausch zu Diensten, Tätigkeiten und Kooperationsfähigkeiten der nationalen CSIRTs (Art. 12 Abs. 3 lit. a NIS-RL). Die CSIRTs-Netzwerk steht zur Kooperationsgruppe in keinem besonderen hierarchischen Verhältnis. Die Kooperationsgruppe stellt lediglich strategische Leitlinien hinsichtlich der Weiterentwicklung der Tätigkeiten des CSIRTs-Netzwerks bereit (Art. 11 Abs. 3 lit. a NIS-RL).

c) Informationsaustausch außerhalb der NIS-Zusammenarbeit

Die Zusammensetzung der Kooperationsgruppe und des CSIRTs-Netzwerk zeigt, dass die Datenschutzbehörden und die Nachrichtendienste an der NIS-Zusammenarbeit nicht direkt mitwirken. Die Datenschutzaufsichtsbehörden wirken allerdings am Informationsaustausch im Rahmen vorgesehener Konsultationen und bei der Bewältigung von Sicherheitsvorfällen mit.[71] Die Informationen und Erkenntnisse werden im Rahmen der NIS-Zusammenarbeit nur geteilt, sofern die Vertreter der Mitgliedstaaten diese in der Kooperationsgruppe einbringen oder sofern NIS-Behörden auf nationaler Ebene mit Nachrichtendiensten Informationen austauschen und diese dann wiederum im horizontalen Verhältnis mit anderen mitgliedstaatlichen NIS-Stellen austauschen.[72] Der nachrichtendienstliche Austausch personenbezogener Daten mit ausländischen Stellen wird jedoch zunehmend formalisiert.[73]

2. Verfahrensrechtliche Ausgestaltung

Der Austausch von Informationen erfolgt im vertikalen Verhältnis über die Kooperationsgruppe bzw. das CSIRTs-Netzwerk und im horizontalen Verhältnis über die nationalen NIS-Behörden bzw. die CSIRTs der Mitgliedstaaten. Zur

---

[71] Siehe § 4 B. II. 2. a) (cc) (2). Vgl. im Übrigen zur Zusammenarbeit und gegenseitigen Amtshilfe der Aufsichtsbehörden Art. 60 ff. DS-GVO.

[72] Zum Austausch im Nationalen Cyber-Abwehrzentrum siehe § 4 B. II. 2. c) (aa) (1).

[73] Siehe § 4 C. I. 2. c).

Untersuchung der maßgeblichen Informationsaustauschprozesse bietet es sich an, die aus der Informatik und dem Netzwerkmanagement bekannte Lösungslogik von Prävention (a), Detektion (b) und Reaktion[74] (c) heranzuziehen. Die Frage ist dann, inwiefern das Informationsverwaltungsrecht dazu beiträgt, Sicherheitsproblemen im Vorhinein zu begegnen, diese zu erkennen und im Falle eines Sicherheitsvorfalls mit Sachkenntnis auf sie zu reagieren.

a) Prävention durch Informations- und Wissensaustausch

Die europäischen Fähigkeiten zur Prävention von Sicherheitsvorfällen und Risiken bei Netz- und Informationssystemen werden nicht so sehr über den punktuellen Austausch einzelner Informationen, sondern durch Wissensaustausch entwickelt. Das Wissen ist regelmäßig das Ergebnis der gewonnenen Erfahrung, dass als gespeicherte aggregierte Information weitergegeben wird. Der Austausch vollzieht sich im Wesentlichen durch Berichte (aa), durch den Austausch von explizierbarer Erfahrung und bewährter Praktiken (bb) sowie im Wege gegenseitiger Konsultationen (cc).

aa) Sach- und Kontrollberichte

Es können Sach- und Kontrollberichte unterschieden werden. Die Sachberichte dienen im Schwerpunkt der formalisierten Darstellung sicherheitstechnischer Umstände (1), die Kontrollberichte geben Auskunft über den Vollzug des Rechts (2). Die Bundesnetzagentur kann zur Erfüllung von Berichtspflichten gegenüber der Kommission und anderen internationalen Gremien auf die Informationsbefugnis des § 4 TKG zurückgreifen (3).

(1) Sachberichte über gemeldete Sicherheitsverletzungen

Sachberichte sind über die im Wege der Meldepflicht generierten Informationen zu erstellen. Die zentralen Anlaufstellen der Mitgliedstaaten legen der Kooperationsgruppe jährlich einen zusammenfassenden Bericht über die eingegangenen Meldungen vor (Art. 10 Abs. 3 UAbs. 2 NIS-RL).[75]

Die zentralen Anlaufstellen sind die Verbindungsstellen zur Gewährleistung der grenzüberschreitenden Zusammenarbeit der Mitgliedstaaten (Art. 8 Abs. 3 NIS-RL). Dies kann die in einem Mitgliedstaat ohnehin zuständige NIS-Behör-

---

[74] Dazu *Kurose/Ross*, Computer Networking: A Top-Down Approach, 6. Aufl. 2013, S. 756; zum Incident-Response-Zyklus *Skopik/Bleier/Fiedler*, Cyber Attack Information System: Gesamtansatz, in: Leopold/Bleier/Skopik (Hrsg.), Cyber Attack Information System, 2015, S. 53 (55).

[75] Zur Informationsgenerierung über Meldepflichten siehe § 3 D. I. 2.

de sein. Die zentrale Anlaufstelle berichtet an die Kooperationsgruppe. Deren Aufgabe ist die „Prüfung" dieser Berichte. Unter Prüfung ist nicht die Kontrolle des Vollzugs zu verstehen, sondern vielmehr die Aufgabe der Kooperationsgruppe, die wesentlichen Erkenntnisse der Berichte zur Kenntnis zu nehmen und zu bewerten (Art. 11 Abs. 3 lit. j NIS-RL; engl. *examine*).

Die Berichtspflicht über Sicherheitsverletzungen kann vor dem Hintergrund der Funktion von Berichtspflichten im Allgemeinen ausgelegt werden. Berichtspflichten und Monitoringprozesse führen zu einer Rückkopplung zwischen Berichtendem und Adressaten, die Erfolge und Lücken aufzeigt. Eine Bilanzierung in zeitlichen Abständen macht es möglich, rechtzeitig auf Veränderungen zu reagieren und gezielt Maßnahmen zu ergreifen und erforderliche Mittel effizienter einzusetzen.[76] Berichtspflichten sind grundsätzlich weitreichender als punktuelle Auskunfts- und Unterrichtungspflichten. Sie sind mit diesen verbunden, knüpfen aber an einen länger dauernden Zeitraum an und sind für die Vollzugskontrolle von Bedeutung. Berichtspflichten stellen aufgrund der Art der Aufbereitung der zu übermittelnden Informationen eine qualifizierte Kategorie von Informationsbeschaffungspflichten dar. Durch Berichte werden nicht bloße Informationen übermittelt. Diese werden vielmehr erhoben, gesammelt und dann systematisch und topisch zusammengestellt.[77]

Der Inhalt der Berichte der nationalen zentralen Anlaufstellen ist nicht abschließend vorgegeben. Eine eigene Richtlinie zur Vereinheitlichung und zweckmäßigen Gestaltung der Berichte wie im europäischen Umweltrecht gibt es im europäischen NIS-Recht nicht.[78] Entsprechend ihrem Zweck sind die Berichte nicht umfassend, sondern zusammenfassend. Harmonisiert sind allerdings Anforderungen wie die Anzahl der Meldungen und Minimalangaben die wie die Art der gemeldeten Sicherheitsvorfälle sowie die ergriffenen Maßnahmen. Unter diesen Maßnahmen sind aber nicht etwaige Abwehr- und Abhilfemaßnahmen, sondern die jeweils erfolgte Unterrichtung eines anderen Mitgliedstaates im Fall eines grenzüberschreitenden Sicherheitsvorfalls zu verstehen (vgl. Art. 14 Abs. 5, Art. 16 Abs. 6 NIS-RL). Die Schwere und Dauer eines Sicherheitsvorfalls fallen nicht unter die Minimalangaben, sind aber als aussagekräftige Parameter gewünschte Informationen.[79] Die Pflichtangabe von Informationen auf quanti-

---

[76] Vgl. *Ladeur*, Die Kommunikationsinfrastruktur der Verwaltung, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band II, 2. Aufl. 2012, § 21 Rn. 21.

[77] *von Bogdandy*, Informationsbeziehungen im europäischen Verwaltungsverbund, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band II, 2. Aufl. 2012, § 25 Rn. 13.

[78] Vgl. RL 91/692/EWG.

[79] Erwägungsgrund 33 NIS-RL.

tativer Basis ist geeignet, der tendenziell bei Berichten bestehenden Gefahr verzerrter Darstellungen aus dem Motiv der Selbstrechtfertigung der Behörden zu begegnen.[80] Insofern eignet sich der Informationsaustausch durch die Berichtspflicht insgesamt zur Verbesserung der Sicherheitsgewährleistung.

Die Berichte über gemeldete Sicherheitsverletzungen sind als wesentliches Element des Lernprozesses in der europäischen Sicherheitsgewährleistung einzuordnen. Die Berichte ermöglichen die Beobachtung von Entwicklungen über einen längeren Zeithorizont. Für die Phasen des Politikzyklus (Vorbereitung, rechtliche Programmierung, Vollzug, Rückkopplung)[81] schaffen die Berichte eine faktenbasierte Diskussionsgrundlage, die gerade auf dem Gebiet der Sicherheit den wichtigen Abgleich der vermuteten mit der wirklichen Bedrohungslage erlaubt. Zugleich dienen die aus den Berichten gewonnenen Erkenntnisse zur Weiterentwicklung der technischen Schutzmaßnahmen auf europäischer Ebene.[82] Des Weiteren bildet die Berichterstattung als „Steuerungselement jeder organisierten Rechtsform" die informationelle Grundlage für weitere Steuerungselemente.[83] Die Kooperationsgruppe hat alle zwei Jahre ein Arbeitsprogramm zur Umsetzung der Ziele der NIS-RL zu erstellen (Art. 11 Abs. 3 UAbs. 2 NIS-RL). Die Zusammenfassung der Sicherheitsvorfälle kann hier der Ausgangspunkt der prospektiven Zielorientierung wie der Formulierung von Zwischenzielen sein. Die Kooperationsgruppe bildet im Übrigen selbst den Motor der Entwicklung der Modalitäten für die Berichterstattung. Da die Kooperationsgruppe die Erörterung der Berichterstattung initiieren darf (Art. 11 Abs. 3 lit. m NIS-RL), hat sie es in der Hand, einen förmlichen Feedback-Mechanismus zu schaffen, der auf die Mitgliedstaaten zurückwirkt.

(2) Kontrollberichte über den Vollzug

Der Aspekt der Steuerung durch Berichte ergibt sich deutlicher bei den Berichtspflichten zum Zweck der Überprüfung der Anwendung des NIS-Verwaltungsrechts. Der Kommission kommt eine übergeordnete Koordinierungsfunktion bei der Überprüfung der Anwendung der NIS-RL zu. Sie hat die Anwendung der Richtlinie regelmäßig zu überprüfen und den Organen der Unionsgesetzgebung darüber zu berichten (Art. 23 NIS-RL).

---

[80] *Sommer*, Verwaltungskooperation am Beispiel administrativer Informationsverfahren im Europäischen Umweltrecht, in: Schmidt-Aßmann/Schöndorf-Haubold (Hrsg.), der Europäische Verwaltungsverbund, 2005, S. 57 (63).

[81] *Eifert*, Europäischer Verwaltungsverbund als Lernverbund, in: Spiecker gen. Döhmann/Collin (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, 2008, S. 159 (165).

[82] Vgl. für die Berichtspflicht der Bundesnetzagentur BT-Drs. 17/5707, S. 83.

[83] *Loeser*, Das Berichtswesen der öffentlichen Verwaltung, 1991, S. 92.

Die Berichtspflicht dient damit zunächst der demokratischen Rückanbindung des Richtlinienvollzugs an die original legitimierte Legislative. Der im Europäischen Parlament repräsentierten Allgemeinheit und den im Rat repräsentierten Exekutiven der Mitgliedstaaten wird ihrerseits die Möglichkeit gegeben, eine Kontrollfunktion wahrzunehmen. Eine Pflicht zur Stellungnahme seitens des Parlaments oder des Rats korrespondiert mit der Berichtspflicht allerdings nicht.

Aus den Formulierungen in Art. 23 Abs. 2 NIR-RL („im Hinblick auf die weitere Förderung […] der Zusammenarbeit", „Bei ihrer Überprüfung bewertet die Kommission […]") ergibt sich, dass der Kommissionsbericht nicht lediglich als Tatsachenfeststellung zu gestalten ist, sondern vielmehr das Ergebnis einer Wissensverarbeitung sein soll. Der periodische Review-Prozess erfordert von der Kommission ein gesteuertes Lernen, d. h. den Ausblick in die Zukunft durch hypothetische Modelle und Simulationen. Bei der Erstellung des Berichts hat sie daher die in der Kooperationsgruppe und im CSIRTs-Netzwerk „gemachten Erfahrungen" (Art. 23 Abs. 2 S. 2 NIS-RL) aufzunehmen.

(3) Telekommunikationsrechtliche Informationsbefugnis zur Erfüllung von Berichtspflichten

Zur Erfüllung internationaler Berichtspflichten stellt § 4 TKG eine Befugnis bereit, die es der Bundesnetzagentur erlaubt, Informationen anzufordern, die sie zur Erfüllung von Berichtspflichten gegenüber der Kommission oder anderen internationalen Gremien benötigt. Die Informationsbefugnis ist in systematischer Hinsicht der Informationsgenerierung zuzuordnen, deren sachliche Reichweite soll aber wegen der sachlichen Nähe zu den Berichtspflichten hier im Rahmen des Informationstransfers untersucht werden.

Die Berichte über Sicherheitsverletzungen an die Kooperationsgruppe enthalten Informationen über die gemeldeten Sicherheitsvorfälle. Die Berichte werden grundsätzlich durch die nationalen zentralen Anlaufstellen erstellt. Die dafür erforderlichen Meldedaten erhalten sie, sofern die Aufgabe der Anlaufstelle nicht ohnehin durch die nationale NIS-Behörde wahrgenommen wird, von den NIS-Behörden oder den CSIRTs (Art. 10 Abs. 3 UAbs. 1 NIS-RL). Die Berichte gehen allerdings nicht direkt an die Kommission. Erst die Kooperationsgruppe legt der Kommission einen Bericht vor. Eine direkte Informationspflicht gegenüber der Kommission trifft hingegen die Bundesnetzagentur auf Grundlage von Art. 13a Abs. 3 S. 3 Rahmen-RL. Der Kommission sind jährlich die eingegangenen Meldungen über Sicherheitsvorfälle zusammenfassend zu berichten. Abgesehen davon, dass darin eine dysfunktionale Doppelung der Berichtspflichten besteht,[84] ist diese Plicht jedoch bereits mit § 109 Abs. 5 S. 5

[84] Es ergibt sich die Situation, dass die Bundesnetzagentur Meldedaten sowohl dem BSI

TKG umgesetzt. Ein praktischer Anwendungsbedarf für § 4 TKG besteht demnach nicht.[85]

bb) Austausch von Erfahrung und bewährten Praktiken

Der Austausch gewonnener Erfahrung und bewährter Verfahren und Vorgehensweisen über die Kooperationsgruppe substituiert fehlendes eigenes Wissen durch Kenntnisse anderer und ermöglicht eine effektivere wie effizientere Sicherheitsgewährleistung (1). Die Speicherung des generierten Wissens fällt im Wesentlichen der Kooperationsgruppe zu (2).

(1) Austausch spezifischer Formen von Wissen über die Sicherheit

Wissen auf dem Gebiet der Netz- und Informationssicherheit entsteht nicht nur durch eigene Wahrnehmung oder Deduktion, sondern durch Konstruktion, d. h. durch Wissensaustauschprozesse. Komplexere kognitive Prozesse sind ohne die Zirkulation von Informationen gar nicht denkbar, weil die erforderlichen Informationen vor allem rechtlich gerade nicht selbst ermittelt werden können. Sie sind nur durch die Übermittlung zu erreichen.[86] Da auf europäischer Ebene keine Einzelverfahren geführt werden, für die eine „Akte" angelegt wird, die das entscheidungsrelevante Wissen sammelt, ist die Informationsübermittlung auf eine Prozeduralisierung angewiesen. Dies meint, dass ein Wissen für einen gestreckten Zeitraum vorgehalten werden muss. In hochgradig arbeitsteiligen Organisationen wie der Administrative ist daher ein Erfahrungsaustausch erforderlich. Erfahrung als spezifisches Wissen ist allerdings nicht allgemein zugänglich, der Austausch muss vielmehr normativ angeregt und gestützt sein.

Eine institutionelle Stabilisierung des Erfahrungsaustausches sieht Art. 11 Abs. 3 lit. g NIS-RL vor. Zu den Aufgaben der Kooperationsgruppe gehört der „Erfahrungsaustausch zu Angelegenheiten der Sicherheit von Netz- und Informationssystemen mit den einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union". Dieser Erfahrungsaustausch bezieht sich in der Praxis primär auf den Austausch mit dem bei Europol angesiedelten Europäischen Zentrum zur Bekämpfung der Cyberkriminalität.[87]

---

als auch der Kommission berichtet. Das BSI wiederum berichtet der Kooperationsgruppe, die ihrerseits der Kommission berichtet.

[85] Zur möglichen weiten Auslegung *Berliner*, Informationsbefugnisse der Bundesnetzagentur im Telekommunikationsrecht, 2012, S. 137 ff.

[86] *Krämer*, Medium, Bote, Übertragung. Kleine Metaphysik der Medialität, 2008, S. 224; *Augsberg*, Informationsverwaltungsrecht, 2014, S. 79.

[87] Vgl. Art. 8 Abs. 3 lit. f des ursprünglichen Entwurfs der Kommission COM(2013) 48 final.

Neben dem (mündlich tradierten) Austausch von Erfahrung ist der Austausch bewährter Praktiken eine weitere Variante des Transfers strukturierten Wissens.[88] Bewährte Verfahren sind Ergebnisse von Lernprozessen, d. h. der Beobachtung von Entscheidungen und Handlungen, die nachträglich (*ex post*) strukturiert werden. Dieser Lernmechanismus ist als solcher weder originell noch innovativ. Der Einsatz von Benchmarking und Best-Practice-Empfehlungen ist in der Union und auch in internationalen Zusammenschlüssen zur Herstellung von Leistungsvergleichen üblich.[89] Ein struktureller Vorteil dieser Methode ist, dass sich die aus dem Vergleich ergebende Anreizwirkung nicht auf die Exekutive von Mitgliedstaaten beschränkt, sondern auch auf die nachgeordnete Fachadministrative ausstrahlt.

Die NIS-RL macht den Austausch von bewährten Verfahren zur wesentlichen Aufgabe der Kooperationsgruppe. Dabei ist der Austausch nicht als allgemeine Aufgabe programmiert. Er bezieht sich konkret auf die Informationsaustauschverfahren im Zusammenhang mit Meldungen von Sicherheitsvorfällen (Art. 11 Abs. 3 lit. b NIS-RL), Verfahren beim Kapazitätenaufbau der Mitgliedstaaten (Art. 11 Abs. 3 lit. c NIS-RL), die Fähigkeiten und die Abwehrbereitschaft der Mitgliedstaaten (Art. 11 Abs. 3 lit. d NIS-RL), die Sensibilisierung und Schulung (Art. 1 Abs. 3 lit. e NIS-RL), die Verfahren zu Forschung und Entwicklung bezüglich der Sicherheit (Art. 11 Abs. 3 lit. f NIS-RL) sowie die Verfahren zur Ermittlung der Betreiber wesentlicher Dienste durch die Mitgliedstaaten (Art. 13 Abs. 3 lit. l NIS-RL).

Durch die Aufführung konkreter Themen wird der bei abstrakteren Austauschverfahren grundsätzlich bestehenden Gefahr begegnet, dass zu unspezifische Erkenntnisse mitgeteilt werden. Die erfolgreiche Übernahme externer Wissensbestände setzt nämlich voraus, dass die eigenen Wissensdefizite erkannt werden. Diese Beobachterkapazität setzt wiederum Kontextwissen seitens der Verwaltung voraus.[90] Unspezifisch bleibt jedoch die Bildung des Vergleichswertverfahrens. So sind das „Ob" und das Worüber des Wissenstransfers vorgegeben, allerdings nicht das „Wie". Im grenzüberschreitenden Vergleich ist eine Verständigung hinsichtlich der Objektivität, Validität und Reliabilität von

---

[88] *Ladeur*, Die Kommunikationsinfrastruktur der Verwaltung, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band II, 2. Aufl. 2012, § 21 Rn. 52.

[89] *John-Koch*, in: Oebbecke (Hrsg.), Nicht-normative Steuerung in dezentralen Systemen, 2005, S. 363 (364 ff.).

[90] Vgl. *Spiecker gen. Döhmann*, Die informationelle Inanspruchnahme des Bürgers im Verwaltungsverfahren, in: dies./Collin (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, 2008, S. 196 (203); *Augsberg*, Informationsverwaltungsrecht, 2014, S. 133.

besonderer Bedeutung, da andernfalls die Qualität einer Vorgehensweise kaum zu bewerten ist. Es ist aber gerade Ziel der NIS-RL, ein „hohes gemeinsames" Sicherheitsniveau zu erreichen, sodass hier die Zusammenarbeit mit der ENISA einzufordern ist, um Kennzahlen und Indikatoren zu entwickeln.

(2) Kooperationsgruppe als Wissensspeicher

Der administrative Erfahrungsaufbau steht im Allgemeinen wie im Besonderen im komplexen Bereich der Netz- und Informationssicherheit nicht nur vor der Herausforderung, Steuerungsanliegen und -ziele vollzugsfähig zu beschreiben. Neben Verfahren der Allokation von Wissen im Raum der europäischen Union bedarf es in zeitlicher Hinsicht der Bewahrung des generierten und ausgetauschten Wissens. Erst die Speicherung erlaubt es, Wissen abrufbar zu halten. Ein verfügbarer Wissensvorrat macht es möglich, singuläre Problem- und Fragestellungen zu rekontextualisieren und wieder zu Wissen und Informationen zu transformieren.[91]

Die Speicherfunktion wird im Wesentlichen durch die Kooperationsgruppe erfüllt. Ausdrückliche Regeln und Routinen zum Wissensmanagement durch Speicherung sind ihr nicht aufgegeben. Allerdings obliegt ihr die „Sammlung von Informationen über bewährte Verfahren bei Risiken und Sicherheitsvorfällen" (Art. 11 Abs. 3 lit. i NIS-RL).

Durch die Sammlung und Bewahrung bewährter Praktiken baut die Kooperationsgruppe gleichsam ein europäisches Gedächtnis hinsichtlich erfolgreicher Prozesse zur Prävention, Erkennung, Reaktion und Bewältigung in Bezug auf Sicherheitsvorfälle und Risiken auf. Denn Lernen bedeutet, „ein Gedächtnis zu haben und in der Lage zu sein, aus gespeicherten Informationen Konsequenzen zu ziehen".[92]

Die Bedeutung dieser Wissenssammlung durch die Kooperationsgruppe lässt sich durch einen Vergleich mit Eigenschaften von Informationssystemen bemessen, die das Europäische Verwaltungsrecht kennt. Informationssysteme stellen für sich eine spezifische Informationsressource in der europäischen Verwaltung dar.[93] Die maßgeblichen Eigenschaften von europäischen Informationssystemen können aufgezeigt werden, wenn verfahrensintegrierte und nicht

---

[91] *Voßkuhle*, Sachverständige Beratung des Staates, in: Isensee/Kirchhof (Hrsg.), HbStR III, 3. Aufl. 2005, § 43 Rn. 4; *Augsberg*, Informationsverwaltungsrecht, 2014, S. 159.

[92] *Stolleis*, Der lernfähige und der lernende Staat, in: Fried/ders. (Hrsg.), Wissenskulturen, 2009, S. 58 (58); vgl. *Trute*, Wissen – Einleitende Bemerkungen, in: Röhl (Hrsg.), Wissen – Zur kognitiven Dimension des Rechts, Die Verwaltung, Beiheft 9, 2010, S. 11 (21 f.).

[93] *Schneider*, Vorüberlegungen zum Informationsmanagement in europäischen Verwaltungsverfahren, in: Lipowicz/ders. (Hrsg.), Perspektiven des deutschen, polnischen und europäischen Informationsrechts, 2011, S. 159 (178); siehe § 4 B. I. 2.

verfahrensintegrierte Informationssysteme als zwei typisierbare Pole unterschieden werden.[94]

Verfahrensintegrierte Informationssysteme übernehmen als Instrumente der gezielten interadministrativen Kooperation Aufgaben in konkreten Verwaltungsvorgängen im Vollzug des Unionsrechts gegenüber dem Bürger oder einem Unternehmen. Nicht verfahrensintegrierte Informationssysteme fördern die Entstehung einer Kommunikationskultur, indem sie über die aus dem nationalen Zusammenhang konventionell bekannten Formen der informationellen Interaktion zwischen verschiedenen Informationsträgern hinausgehen und Informationssammlungen staatlicher und nichtstaatlicher Herkunft verbinden. Sie zeichnen sich regelmäßig durch Verwendungsoffenheit aus. Die Sammlung personenbezogener und vertraulicher Daten ist nicht vorgesehen, vorrangig werden wissenschaftliche oder technische Daten gesammelt.[95] Auch wenn die nicht verfahrensintegrierten Informationssysteme der Informationsvorsorge dienen, werden die Informationen häufig nicht gegenüber dem Bürger oder Unternehmen verwendet.

Informationssysteme haben typischerweise Kompetenzen zur zentralisierten Informationsverwaltung und zum Betreiben der Netze und Datenbanken, sodass sie über Informationen verfügen, diese speichern, berichtigen, löschen, auswerten und weitergeben oder Zugangsrechte vergeben können. Da jedes Informationssystem in seiner Gesamtheit bezweckt, Informationen zusammenzutragen und diese zu speichern, spielt die jeweilige konkrete Bedeutung und Position der Datenbanken eine wichtige Rolle. Diesbezüglich können dezentrale und zentrale Architekturen, aber auch Mischformen ausgemacht werden. Dezentrale Architekturen beruhen auf nationalen Datenbanken, die zu einem Netzwerk integriert werden. Bei zentralen Architekturen wird der Datenbestand an einem Ort gepflegt, wobei die Eingaben dezentral erfolgen. Das Schengener Informationssystem (SIS) ist insofern eine Mischform, als bei den teilnehmenden Partnern identische Datenbanken bestehen (N-SIS), deren Synchronisation und Datensicherung durch eine zentrale Unterstützungseinheit vorgenommen wird (C-SIS), Art. 92 Schengener-Durchführungsübereinkommen (SDÜ). Als Spezifikum von Informationssystemen kann ein Direktzugriff auf fremde oder gemeinsame Datenbestände angesehen werden.[96]

---

[94] Dazu *Heußner*, Informationssysteme im Europäischen Verwaltungsverbund, 2007, S. 143 ff., 154 ff., 161 f.

[95] *Heußner*, Informationssysteme im Europäischen Verwaltungsverbund, 2007, S. 159.

[96] *Sommer*, Informationskooperation am Beispiel des europäischen Umweltrechts, in: Schmidt-Aßmann/Schöndorf-Haubold (Hrsg.), Der Europäische Verwaltungsverbund, 2005, S. 57 (71 f.); *Schneider*, Vorüberlegungen zum Informationsmanagement in europäischen

Die aufzubauende Sammlung der Kooperationsgruppe dient nur indirekt dem Vollzug von Unionsrecht. Die Teilnehmer der Kooperationsgruppe haben grundsätzlich keine operativen Befugnisse, die ausgetauschten Informationen werden nicht erst für die konkreten Zwecke, denen sie dienen sollen, erhoben. Die Informationssammlung ist gleichwohl zentral auf europäischer Ebene lokalisiert. Primäres Anliegen ist die Zusammenführung der auf mitgliedstaatlicher Ebene vorhandenen Informationen und des gesammelten Erfahrungswissens. Die Sammlung bei der Kooperationsgruppe bildet mindestens die Summe des aus den Mitgliedstaaten über die Berichte zusammengetragenen Wissens. Die mnemotechnische Leistung der Kooperationsgruppe betrifft mit den „bewährten Verfahren bei Risiken und Sicherheitsvorfällen" Formen allgemeinen, kondensierten Wissens und eben nicht den Aufbau eines statischen Vorrats an Informationen mit Relevanz für die Sicherheitsgewährleistung. Das durch diese Aggregation entstehende Wissen kann der Nutzung im Unionsraum zugeführt werden. Ressourcen können so besser verwendet, Synergieeffekte ausgenutzt und Doppelarbeit vermieden werden. Der Wissensspeicher der Kooperationsgruppe erfüllt damit den typischen Zweck nicht verfahrensintegrierter Systeme. Die gespeicherten Praktiken erlauben den Austausch von Informationen und Wissen zu Zwecken der Vorsteuerung, Begleitung und Nachsteuerung von Entscheidungen. Gerade der stabilisierte Austausch über Best Practices ermöglicht eine Angleichung der mitgliedstaatlichen Gewährleitungspraktiken in tatsächlicher Hinsicht.

cc) Konsultationspflichten

Die interadministrative Informationskooperation muss sich nicht auf die bloße Weitergabe von Informationen beschränken. Auf ein zusätzliches Zusammenwirken von Verwaltungen zielen als weitere Kategorie des formalisierten Informationsaustausches die Konsultationsverfahren. Sie ermöglichen die Informationsbewertung in einem dialogischen Modus und können damit eine höhere Form der Informationsverarbeitung erreichen.[97] Dabei handelt es sich um Informationspflichten, die den beteiligten Stellen typischerweise einen weiten Spielraum bezüglich Zeitpunkt, Form und Umfang des Austausches einräumen.[98] Die gemeinsamen Interessen der Stellen können so grundsätzlich bestmöglich

---

Verwaltungsverfahren, in: Lipowicz/ders. (Hrsg.), Perspektiven des deutschen, polnischen und europäischen Informationsrechts, 2011, S. 159 (165).

[97] *Schneider*, Vorüberlegungen zum Informationsmanagement in europäischen Verwaltungsverfahren, in: Lipowicz/ders. (Hrsg.), Perspektiven des deutschen, polnischen und europäischen Informationsrechts, 2011, S. 159 (178).

[98] *Heußner*, Informationssysteme im Europäischen Verwaltungsverbund, 2007, S. 17.

gewahrt werden.[99] Als Prozess fortgesetzter Beobachtung und Abstimmung sind Konsultationen ein weiterer Mechanismus des Lernens.[100] Die NIS-Behörden haben die nationalen Strafverfolgungsbehörden (1), die Datenschutzaufsicht (2) und zum Teil die für Katastrophenschutz zuständigen Behörden zu konsultieren (3).

(1) Konsultation mit nationalen Strafverfolgungsbehörden

Der Transfer von Informationen an Strafverfolgungsbehörden ist keine vorrangige Angelegenheit der NIS-Kooperation. Der Informationsaustausch über strafrechtlich relevante Angriffe auf Informationssysteme mit europäischer Reichweite ist indes nicht grundlegend gefährdet. Zur Kompensation fehlender transnationaler und europäischer Ermittlungsbefugnisse schafft Art. 13 RL 2013/40/EU[101] außerhalb der NIS-Informationskooperation eine eigenständige Struktur für den Informationsaustausch über Straftaten. Die Mitgliedstaaten haben danach im Wesentlichen eine operative nationale Kontaktstelle einzurichten, die rund um die Uhr verfügbar ist und auf Ersuchen höchstens acht Stunden nach Eingang eine Antwort gibt. Darüber hinaus haben sie Meldekanäle einzurichten, damit die Straftaten den jeweils zuständigen nationalen Behörden gemeldet werden können. In Deutschland besteht diese Stelle beim Bundeskriminalamt.[102] Mittels dieser Maßnahmen finden insbesondere die Vorschriften über den internationalen Informationsaustausch Anwendung (§§ 14 ff. BKAG). Die Richtlinie zielt nicht nur auf den Austausch forensischer Daten über die Vorgehensweise von Tätern und den Austausch mit Europol und dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (European Cybercrime Centre – EC3).

Der Informationsaustausch soll vielmehr auch ein allgemeines Verständnis der Bedrohungen ermöglichen und so auf politischer Ebene zu entsprechenden Beschlussfassungen beitragen. Für die Strafverfolgung von Cyberkriminalität nimmt das EC3 die Rolle des zentralen Wissens- und Informationsakteurs auf europäischer Ebene ein. Das Zentrum wurde 2013 als Teil von Europol eingerichtet und dient der Koordination der strafrechtlichen Ermittlungen in den Mit-

---

[99] *Holznagel*, Informationsbeziehungen in und zwischen Behörden, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band II, 2. Aufl. 2012, § 24 Rn. 37.

[100] *Herzmann*, Konsultationen – Eine Untersuchung von Prozessen, kooperativer Maßstabskonkretisierung in der Energieregulierung, S. 162.

[101] Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates.

[102] BT-Drs. 18/4350, S. 15.

gliedstaaten.[103] Die Kommission weist dem EC3 neben der operativen eine analytische Funktion zu.[104] Es sei die zentrale Anlaufstelle für Informationen über Cyberstraftaten, der eine „Informationsverknüpfungsfunktion" zukomme. Der Kenntnisstand soll zum einen verbessert werden, um hochwertige Strategieberichte zu erstellen, und zum anderen, um „cyberkriminalistisches Fachwissen" zur Unterstützung beim Kapazitätenaufbau der Mitgliedstaaten zu erlangen.[105] Gerade weil der Informationsaustausch im Bereich der Strafverfolgung auch darauf zielt, ein „umfassenderes Bild des Problems der Cyberkriminalität und der Netz- und Informationssicherheit auf Unionsebene" zu gewinnen, sollen relevante Daten auch der ENISA „im Einklang mit ihrer Aufgabe und ihrem Informationsbedarf" zur Verfügung gestellt werden[106] Die Voraussetzungen und das Verfahren für den Informationsfluss an die ENISA legt die RL 2013/40/EU dagegen nicht fest.

Neben der eigenständigen Struktur des Informationsaustausches zur Bekämpfung der Computerkriminalität auf Grundlage der RL 2013/40/EU bestehen Verbindungsstrukturen auf Basis des NIS-Kooperationsrechts. Den nationalen NIS-Behörden ist gemäß Art. 8 Abs. 6 NIS-RL aufgegeben, die zuständigen Strafverfolgungsbehörden „gegebenenfalls" nach Maßgabe des nationalen Rechts zu „konsultieren". Dem Wortlaut nach zielt diese sekundärrechtliche Vorgabe darauf, dass sich die Behörden gegenseitig um Rat fragen. Die Intention der Weitergabe (IT-forensischer) Daten bzw. ermittlungsrelevanter Informationen kommt nicht zum Ausdruck. In der Regel dürften die Strafverfolgungsbehörden auf die technische Expertise der NIS-Behörden angewiesen sein, sodass der Konsultationsprozess grundsätzlich nicht von den NIS-Behörden ausgeht. Unionsrechtlich besteht letztlich keine Pflicht zur Meldung strafrechtlich relevanter Angriffe auf die Netz- und Informationssicherheit. Dies ergibt sich auch im Umkehrschluss aus Erwägungsgrund 62 der NIS-RL, demzufolge die Mitgliedstaaten Betreiber wesentlicher Dienste und Anbieter digitaler Dienste „dazu anhalten" sollten, Sicherheitsvorfälle mit einem schwerwiegenden kriminellen Hintergrund den entsprechenden Strafverfolgungsbehörden zu melden. Die NIS-Behörde hat nach Art. 8 Abs. 6 NIS-RL demnach nicht die Pflicht, Strafverfolgungsbehörden über Sicherheitsvorfälle von sich aus zu unterrichten.

Die entsprechende Regelung für das BSI entspricht dem Ansatz einer nur schwachen Beziehung zu Strafverfolgungsbehörden. Das BSI unterstützt Straf-

---

[103] *Kommission*, Mitteilung der Kommission an den Rat und das Europäische Parlament, COM(2012) 140 final, S. 6; *Oerting*, Kriminalistik 2012, 705 (705 f.).

[104] *Berger*, Integration 2013, 307 (313).

[105] *Kommission*, Mitteilung der Kommission an den Rat und das Europäische Parlament, COM(2012) 140 final, S. 4 f.

[106] Erwägungsgrund 24 RL 2013/40/EU.

verfolgungsbehörden nur auf deren Ersuchen hin (§ 3 Abs. 1 S. 4 BSIG: „Unterstützungsersuchen"). Im Übrigen liegt die Datenübermittlung im Ermessen des BSI und dies auch nur hinsichtlich der Angriffe auf die Kommunikationstechnik des Bundes (§ 5 Abs. 6 und 7 BSIG). Die Gewährleistung der Netz- und Informationssicherheit über die Strafverfolgung hängt somit maßgeblich davon ab, ob die Betreiber wesentlicher Dienste und Anbieter digitaler Dienste Sicherheitsvorfälle mit einem mutmaßlich kriminellen Hintergrund den entsprechenden Strafverfolgungsbehörden melden.

Sind nationale NIS-Behörden selbst auf Unterstützung, etwa bei der Koordinierung mit den Strafverfolgungsbehörden anderer Mitgliedstaaten, angewiesen, können sie sich an das Europäische Zentrum gegen Cyberkriminalität wenden.[107]

(2) Konsultation mit Datenschutzbehörden

Neben der Konsultation mit Strafverfolgungsbehörden ist die Konsultation mit Datenschutzbehörden vorgesehen. Die nationalen NIS-Behörden und zentralen Anlaufstellen „konsultieren gegebenenfalls" die nationalen Datenschutzbehörden nach Maßgabe des nationalen Rechts und arbeiten mit ihnen zusammen (Art. 8 Abs. 6 NIS-RL).

Für die NIS-Behörden kann die Fachkunde der Datenschutzaufsicht insbesondere in Bezug auf zwei Fragenkomplexe relevant werden. Zum einen kann die NIS-Behörde datenschutzrechtliche Einschätzungen bei der Konkretisierung der materiell-rechtlichen Sicherheitspflichten, die mit der Verarbeitung personenbezogener Daten einhergehen, für die Betreiber und Anbieter von Internetinfrastrukturen und -diensten einsetzen. Zum anderen kann sie die eigene Informationsgenerierung auf datenschutzrechtliche Risiken durch Konsultation mit den Aufsichtsbehörden überprüfen. Vor allem wenn es um die Spezifizierung der geforderten technischen-organisatorischen Maßnahmen nach dem „Stand der Technik" (vgl. Art. 14 Abs. 1, Art. 16 Abs. 1 NIS-RL) geht, kommt es auf Konsultationen der Behörden an. Die im Sicherheitsrecht geläufige Regelungstechnik, auf den Stand der Technik oder die Wissenschaft Bezug zu nehmen, trägt besonders instabilen Wissensverhältnissen Rechnung. Diesen kann nur durch eine ständige und situationsangepasste Weiterentwicklung der vorhandenen und hinzukommenden Informationen und durch Austausch begegnet werden.

Aber auch für die Datenschutzaufsichtsbehörden dürfte ein Anreiz zur Beteiligung an der Konsultation bestehen.

Der Primäranreiz der Datenschutzaufsichtsbehörden liegt darin, bestehende Wissensdefizite und Ungewissheiten in spezifisch sicherheitstechnischen Fragestellungen zu bewältigen. Zwar haben in personeller Hinsicht die Mitglieder der

[107] Erwägungsgrund 62 NIS-RL.

Datenschutzaufsichtsbehörden über die für die Erfüllung ihrer Aufgaben und Ausübung ihrer Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde zu verfügen (Art. 53 DS-GVO). Dennoch kann bei hoher Arbeitsbelastung oder spezifischen Einzelfragen eine willkommene Entlastung dadurch entstehen, die NIS-Behörde als Fachbehörde um Rat zu fragen. Gerade weil die Aufsichtsbehörde in ihren beratenden Stellungnahmen von sich aus oder auf Anfrage „zu allen Fragen" im Zusammenhang mit dem Datenschutz Stellung nimmt (Art. 58 Abs. 3 lit. b DS-GVO), können besondere Sachfragen eine besondere Sachkompetenz und damit eine Konsultation erfordern.

Die Datenschutzaufsicht kann ihrerseits mit für die Verarbeitung personenbezogener Daten Verantwortlichen in einem Konsultationsprozess stehen, insbesondere bei neuen Formen der Datenverarbeitung durch Verwendung neuer Technologien. Hat eine Form der Verarbeitung ein hohes Risiko für Rechte und Freiheiten natürlicher Personen zur Folge, hat der Verantwortliche gemäß Art. 35 DS-GVO eine Datenschutz-Folgenabschätzung durchzuführen. Trifft der Verantwortliche daraufhin keine Maßnahmen zur Eindämmung des Risikos, hat er vor der Verarbeitung die Aufsichtsbehörde zu konsultieren. Für den Fall, dass die Aufsichtsbehörde der Auffassung ist, die geplante Verarbeitung stehe nicht im Einklang mit dem Datenschutzrecht, hat sie eine schriftliche Empfehlung auszusprechen (Art. 36 Abs. 2 S. 1 DS-GVO) und den Verantwortlichen zu beraten (Art. 58 Abs. 3 lit. a DS-GVO). Eine „Rückkonsultation" mit den NIS-Behörden kann hier vor allem bei raschen technologischen Entwicklungen angezeigt sein.

Eine Konsultationspflicht, die so allgemein wie Art. 8 Abs. 6 NIS-RL gehalten ist („gegebenenfalls"), besteht dagegen weder für die Bundesnetzagentur noch für das BSI. Das Einholen besonderer Fachkunde ist lediglich punktuell vorgesehen.

Die Bundesnetzagentur hat die Expertise des Bundesbeauftragten für Datenschutz und Informationsfreiheit und das BSI bei der Erstellung des Katalogs von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Bearbeitung personenbezogener Daten mit einzubeziehen (§ 109 Abs. 6 TKG). Der Katalog ist „im Einvernehmen" mit den genannten Fach- und Aufsichtsbehörden herzustellen. Mit der novellierten Fassung durch das IT-Sicherheitsgesetz ist der Modus des Wissenstransfers sogar normativ gestärkt worden. Nach § 109 Abs. 6 TKG a. F. war lediglich das „Benehmen" herzustellen. Einvernehmen ist grundsätzlich dann hergestellt, wenn ein vollständiger Konsens zwischen den Behörden besteht.[108] Das Zustan-

[108] Vgl. *Fetzer/Groß*, in: Arndt/Fetzer/Scherer/Graulich (Hrsg.), TKG, 2. Aufl. 2015, § 123 Rn. 11.

dekommen und der Inhalt sind demnach vom Einverständnis der Behörden abhängig. Die Behörden begegnen sich demnach auf gleichgelagerter Stufe. Mit der Einbeziehung dieser Behörden werden die fachliche Expertise und Kompetenz des BSI und des Bundesbeauftragen in Fragen der Informationssicherheit stärker genutzt.[109] Mit der Beteiligung des BSI wird zudem der zunehmenden Nutzung von Informationstechnik in der Telekommunikationstechnik Rechnung getragen.[110]

Das BSI kann die „fachliche Expertise" anderer Behörden im Rahmen der Feststellung, ob die von Betreibern kritischer Infrastrukturen und ihrer Branchenverbände vorgeschlagenen Sicherheitsstandards geeignet sind, die materiell-rechtlichen Sicherheitsanforderungen zu gewährleisten, in Anspruch nehmen.[111] Die Feststellung erfolgt „im Benehmen" mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe sowie „im Einvernehmen" mit der zuständigen Aufsichtsbehörde des Bundes oder „im Benehmen" mit der sonst zuständigen Aufsichtsbehörde (§ 8a Abs. 2 S. 3 BSIG). Die Variation des Konsultationsmodus ist aber nicht so sehr auf eine etwaigig geringere Fachkunde bei den sonstigen Aufsichtsbehörden zurückzuführen als auf das grundgesetzliche Verbot der Mischverwaltung. Einrichtungen der Landesverwaltung dürften nach diesem aus Art. 83 ff. und 87 ff. GG abgeleiteten kompetenz- und organisationsrechtlichen Grundsatz nur in eng begrenztem Umfang zu Zwecken der Bundesverwaltung herangezogen werden. Denn grundsätzlich gilt, dass Verwaltungsaufgaben mit eigenen personellen und sachlichen Mitteln wahrzunehmen sind.[112] Die Datenschutzaufsichtsbehörden der Länder haben folglich nur beschränkt Mitentscheidungsbefugnisse. Da die unionsrechtliche Vorgabe in Art. 8 Abs. 6 NIS-RL unter dem Vorbehalt des nationalen Rechts steht, kommt auch keine unionsrechtliche Derogation dieses grundgesetzlichen Grundsatzes in Betracht. Das Benehmenserfordernis sichert aber prinzipiell die Beteiligung der Aufsichtsbehörden ab.

(3) Konsultation als Teil des Notfallmanagements

Ein besonderer Bereich der Behandlung von Sicherheitsvorfällen ist das Notfallmanagement. Ein Notfall in der Netz- und Informationssicherheit ist ein Schadensereignis, bei dem wesentliche Prozesse oder Ressourcen einer Institu-

[109] BT-Drs. 18/4096, S. 63; vgl. aber *Heinickel*/*Feiler*, CR 2014, 708 (714), die darauf hinweisen, dass die bewährte Zusammenarbeit der Behörden gestört werden könnte, die Bundesnetzagentur für den Telekommunikationssektor die sachnähere Behörde sei, und die im Übrigen darin eine Gefahr der Überregulierung erkennen.

[110] *Graulich*, in: Arndt/Fetzer/Scherer/ders. (Hrsg.), TKG, 2. Aufl. 2015, § 109 Rn. 49.

[111] BT-Drs. 18/4096, S. 26.

[112] BVerfGE 63, 1 (37 ff.).

tion nicht wie vorgesehen funktionieren. Die Verfügbarkeit entsprechender Prozesse oder Ressourcen kann bei Notfällen nicht innerhalb der geforderten Zeit oder insgesamt nicht wiederhergestellt werden. Wird die Kontinuität des Geschäftsbetriebs beeinträchtigt, können Notfälle eskalieren und sich zu einer Krise ausweiten, welche die Existenz eines Betriebs oder höchste Rechtsgüter von Personen gefährdet. Um die Robustheit und Ausfallsicherheit zu erhöhen und ein zielgerichtetes Reagieren zu ermöglichen, sind geeignete Präventivmaßnahmen erforderlich.[113]

Dem Kontinuitätsmanagement bei Betreibern kritischer Infrastrukturen und digitaler Dienste wird durch die NIS-RL hohe Priorität eingeräumt. Die Mitgliedstaaten haben sicherzustellen, dass die Betreiber wesentlicher Dienste geeignete Maßnahmen treffen, damit die Verfügbarkeit der Dienste gewährleistet wird (Art. 14 Abs. 2 NIS-RL). Hinsichtlich der Anbieter digitaler Dienste ist sicherzustellen, dass dem Business Continuity Management Rechnung getragen wird (Art. 16 Abs. 1 lit. c NIS-RL, deutsche Sprachfassung). Die Durchführungsakte der Kommission haben dieses betriebliche Notfallmanagement durch Strategien für die Verfügbarkeit der Dienste und Notfallpläne zu konkretisieren.[114]

Eine präventive Konsultation zum Zwecke des Notfallmanagements sieht die NIS-RL trotz deren durch sie selbst beigemessenen Bedeutung nicht vor. Gleichwohl besteht für die NIS-Verwaltung wie auch im europäischen Katastrophenschutzrecht Konsultationsbedarf. Art. 222 Abs. 4 AEUV sieht regelmäßige Einschätzungen von Bedrohungen, denen die Union ausgesetzt ist, durch den Europäischen Rat vor. Aus der systematischen Stellung in Art. 222 AEUV wird teilweise gefolgert, dass sich die Lagebeurteilung nur auf terroristische Bedrohungen und ggf. Naturkatastrophen beziehe.[115] Dies ist aber mit Blick auf Art. 222 Abs. 1 S. 1 AEUV nicht zwingend, da dieser auch sonstige anthropogene Katastrophen umfasst. Die Einschätzung kann dementsprechend der allgemeinen Analyse von Katastrophen dienen.[116] Da Gefahren für die Netz- und Informationssicherheit durch terroristisch motivierte Bedrohungen gegeben sein können, kann ein Austauschbedarf bestehen. Der Informationsaustausch mit Organen und Einrichtungen außerhalb der NIS-Verwaltung ist zwar Aufgabe der Kooperationsgruppe. Zu Angelegenheiten der Netz- und Informations-

---

[113] BSI, IT-Grundschutz, 1.3 Notfallmanagement, 11. EL Stand 2009.

[114] Art. 16 Abs. 8, Erwägungsgrund 69 NIS-RL.

[115] *Ohler*, in: Streinz (Hrsg.), EUV/AEUV, 2. Aufl. 2012, AUEV, Art. 222 Rn. 16; *Vedder*, in: ders./Heintschel von Heinegg (Hrsg.), Europäisches Unionsrecht, 2011, EVV, Art. III-329 Rn. 7.

[116] Vgl. *Lachmayer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Europäisches Unionsrecht, Band 4, 7. Aufl. 2015, AEUV, Art. 222 Rn. 6; *Calliess*, in: ders./Ruffert (Hrsg.), EUV/AEUV, 4. Aufl. 2011, AEUV, Art. 222 Rn. 38.

sicherheit tauscht die Gruppe aber nur „Erfahrungen“ aus, falls dazu ein Anlass besteht („gegebenenfalls“). Im Ergebnis mag der Wissensaustausch gleichwertig sein. Die Differenzierung zwischen Konsultation und Erfahrungsaustausch entspricht hingegen den Facetten des Austauschprozesses. Erfahrungen werden vor allem ausgetauscht, indem auf vergangene Ereignisse Bezug genommen wird, die Teil eines Lernprozesses waren. Die Konsultation ist gerade ein Instrument der Mitwirkung, das sogar vorrangig zur prospektiven Krisenprävention eingesetzt werden muss.

Ein nicht unionsrechtlich vorgegebenes, aber vorbildliches Spezifikum in Deutschland ist die Beteiligung des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK) bei der Analyse von Informationen. Dem BBK kommen gemäß § 8a Abs. 2 BSIG Mitwirkungsaufgaben bei der Analyse der Informationen über Sicherheitslücken, Schadprogramme und Angriffe zu.[117] Die Beschränkung auf solche Risiken, die die Verfügbarkeit kritischer Infrastrukturen beeinträchtigen können, entspricht dem Gedanken des Notfallmanagements. Die Beteiligung des BBK schafft eine Schnittstelle mit dem BSI, welche die Synchronisierung der zeitkritischen Eskalationsverfahren erlaubt. Zumindest die behördliche Koordination wird von vorneherein effektiviert. Die Beteiligung des BBK geht im Übrigen nicht mit der Übertragung von Befugnissen einher. Das Dezentralisationsprinzip im Katastrophenorganisationsrecht wird durch die informativ-kooperative Zusammenarbeit mit dem BBK nicht unterminiert.[118] Die grundgesetzlichen Vorgaben des Art. 35 Abs. 2 S. 2 GG stehen mit einem Austausch von Wissen und Einschätzungen gerade nicht im Widerspruch. Eine Änderung der Zuständigkeit oder die Herstellung eines Subordinationsverhältnisses zwischen den Behörden geht mit der gemeinsamen Analyse nicht einher.

b) Detektion von Gefahren durch Frühwarnmechanismus

Eine wichtige Bedeutung für die Gewährleistung der Netz- und Informationssicherheit auf europäischer Ebene hat das Konzept der Frühwarnung. Mechanismen der Frühwarnung dienen der frühzeitigen Erkennung von Gefahren und der schnellen Information Gefährdeter (aa). In der europäischen NIS-Kooperation bestehen Ansätze eines Frühwarnsystems (bb).

---

[117] Außerdem ist das BBK im Feststellungsverfahren der branchenspezifischen Sicherheitsanforderungen zu konsultieren (§ 8a Abs. 2 S. 3 Nr. 1 BSIG).

[118] Zu den Prinzipien im Katastrophenorganisationsrecht *Walus*, Katastrophenorganisationsrecht – Prinzipien der rechtsstaatlichen Organisation des Katastrophenschutzes, 2012, S. 23 ff.

aa) Rascher Austausch über Gefahren durch Frühwarnsysteme

Frühwarnsysteme bezeichnen eine im Europäischen Verwaltungsverbund spezielle Art von Informationssystemen, die für ihren Benutzer „mögliche Gefährdungen mit zeitlichen Vorlauf signalisieren und diesen damit in die Lage versetzen sollen, noch rechtzeitig geeignete Gegenmaßnahmen zur Abwehr oder Minderung der signalisierten Gefährdungen ergreifen zu können".[119] Frühwarn- und Reaktionssysteme finden sich in europäischen Informationssystemen insbesondere in Sachgebieten, die durch sich schnell verbreitende Gefahren geprägt sind. Sie können beinhalten, dass Informationen in Echtzeit ausgetauscht werden.[120] Vor allem im Verbraucher- und Gesundheitsschutz sind Informationsaustauschprozesse als Schnellwarninformationssysteme gestaltet. Die unverzügliche und umfassende Information aller Mitgliedstaaten in der Union erfordert grundsätzlich feste Strukturen der Informationsübermittlung, weshalb Inhalt und Form von Warnmeldungen in Frühwarnsystemen durch das Unionsrecht vorgeschrieben werden.[121] So zeigt das Netz für die epidemiologische Überwachung und Kontrolle übertragbarer Krankheiten exemplarisch, dass mit einem Frühwarn- und Reaktionsmechanismus[122] ein Auftrag zur Informationssammlung einhergeht bzw. dass diese von den Teilnehmern gemeinsam betrieben wird.[123]

bb) Frühwarnungen durch CSIRTs

Im Bereich der Netz- und Informationssicherheit dienen Frühwarnungen der Optimierung präventiver Maßnahmen durch Früherkennung sowie der raschen

---

[119] *Hahn*, Frühwarnsysteme, Krisenmanagement und Unternehmensplanung, in: Albach/Hahn/Mertens (Hrsg.), Frühwarnsysteme, ZfB-Ergänzungsheft 2/1979, S. 25 (25); *Kujat*, Frühwarnsysteme zur Abwehr von Botnetzen, 2010, S. 20 f.

[120] Siehe *Kommission,* Commission Staff Working Document, Impact Assessment, SWD (2013) 32 final, S. 126; Vgl. in den USA 2014 die Beschreibung des U.S. Department of Homeland Security zum NCCIC Watch Floor nach dem National Cybersecurity Protection Act im Schreiben vom 31. Juli 2015, abrufbar unter: http://www.franken.senate.gov/files/documents/150731DHSresponse.pdf.

[121] *Heußner*, Informationssysteme im Europäischen Verwaltungsverbund, 2007, S. 137.

[122] Entscheidung Nr. 2000/57/EG der Kommission vom 22. Dezember 1999 über ein Frühwarn- und Reaktionssystem für die Überwachung und die Kontrolle übertragbarer Krankheiten gemäß der Entscheidung Nr. 2119/98/EG des Europäischen Parlaments und des Rates (ABl. L 21, S. 32).

[123] Das Europäische Zentrum für die Prävention und die Kontrolle von Krankheiten (ECDC) hat nach Art. 3 VO (EG) Nr. 851/2004 des Europäischen Parlaments und des Rates vom 21. April 2004 zur Errichtung eines Europäischen Zentrums für die Prävention und die Kontrolle von Krankheiten den Auftrag, umfassend Informationen zu sammeln, wobei sich der Auftrag zusätzlich auf nicht regierungsamtliche Quellen bezieht. Dazu *Pflug*, Pandemievorsorge – informationelle und kognitive Regelungsstrukturen, 2013, S. 115.

Reaktion im Falle von Cyberattacken.[124] Das Bedürfnis nach einem Frühwarnmechanismus auf europäischer Ebene hat die Kommission in der Cybersicherheitsstrategie der Europäischen Union artikuliert.[125] In einem Vorgängerentwurf zur NIS-RL war der Strategie entsprechend ein europäisches System zur Frühwarnung und koordinierten Reaktion vorgesehen.[126] Der Vorschlag der Kommission hat keinen Eingang in die nunmehr geltende NIS-RL gefunden. Ansätze eines Frühwarnmechanismus lassen sich gleichwohl ausmachen.

Das Basiselement eines Frühwarnsystems ist die Messung und Erfassung von Gefahrenindikatoren.[127] Zur Frage, welcher Akteur als Sensor in einem Früherkennungssystem fungiert, äußert sich die NIS-RL nicht. Insofern bleibt die Ausgangszuständigkeit für die operative Informationskooperation bei den CSIRTs. Die Aufgabe, Frühwarnungen und Alarmmeldungen auszugeben, ist den nationalen CSIRTs aufgetragen (Anhang I Nr. 2 lit. a. ii) NIS-RL). Dabei haben die CSIRTs auch die „einschlägige[n] Interessenträger" zu adressieren.

Ein weiterer wesentlicher Bestandteil von Frühwarnsystemen ist die (zentrale) Sammlung von Indikatoren. In der Zentrale können Messwerte überwacht und ausgewertet werden. Eine solche Stelle ist auf europäischer Ebene nicht eingerichtet. Der freiwilligen Weitergabe von Gefahrenindikationen steht vorbehaltlich der Grenzen des europäischen Informationstransfers im CSIRTs-Netzwerk nichts entgegen.[128]

Damit ist für grenzüberschreitende Frühwarnungen eine Netzwerkstruktur induziert, die weitgehend auf unmittelbare Kommunikation der Beteiligten in einer heterarchischen Struktur angelegt ist.[129] Das Netzwerk kann allgemein als „neuartige Institution der Wissensverteilung" begriffen werden, die spezifische Vorteile in der Beobachtungskapazität hat und durch welche die Weiterentwicklung expliziten Wissens innovativ befördert wird.[130] Eine rhizomorphe Organi-

---

[124] Vgl. *Leopold/Bleier/Skopik*, Vorwort der Herausgeber, in: dies. (Hrsg.), Cyber Attack Information System, 2015, S. VII; *Kurose/Ross*, Computer Networking: A Top-Down Approach, 6. Aufl. 2013, S. 756; *Engeler/Jensen/Obersteller/Deibler/Hansen*, Monitoring durch Informationsfusion und Klassifikation zur Anomalieerkennung, 2014, S. 19.

[125] *Kommission*, Cybersicherheitsstrategie der Europäischen Union, S. 7, 14, 18; *Kommission*, Commission Staff Working Document, Impact Assessment, SWD (2013) 32 final, S. 124, zur Evaluierung der Kriterien für ein EU Early Warning and Response System (EWRS).

[126] Art. 10 und 11 COM(2013) 48 final.

[127] Siehe United Nations, International Strategy for Disaster Reduction, Platform for the Promotion of Early Warning, online abrufbar: http://www.unisdr.org/2006/ppew/whats-ew/basics-ew.htm.

[128] Siehe § 4 C.

[129] Siehe dazu *Augsberg*, Europäisches Verwaltungsorganisationsrecht und Vollzugsformen, in: Terhechte (Hrsg.), Verwaltungsrecht der Europäischen Union, 2011, § 6 Rn. 54 f.

[130] *Wielsch*, Die epistemische Analyse des Rechts. Von der ökonomischen zur ökologischen Rationalität in der Rechtswissenschaft, JZ 2009, 67 (74).

sation, d. h. ein Netzwerk, „das azentrisch, nicht hierarchisch" und „ohne General"[131] aufgebaut ist, welches den Gefahren einer Informationsüberforderung möglicherweise besser gewachsen sein kann,[132] wird für das europäische Umweltinformations- und Beobachtungsnetz EIONET beobachtet, in dem zahlreiche Behörden und private Einrichtungen zu einem Rhizom verknüpft sind.[133] Zu bedenken ist, dass in Ermangelung expliziter sekundärrechtlicher Anleitungen zur Ausgabe von Frühwarnungen und zum Zweck koordinierter Reaktion kein Vakuum besteht, sondern die dynamische Teilnahme im Netzwerk eine normative Verdichtung durch die primärrechtlichen Grundsätze, wie den zur loyalen Zusammenarbeit (Art. 4 Abs. 3 UAbs. 1 EUV), erfährt.[134]

Anders als etwa die Meteorologie kann die junge „Disziplin der IT-Frühwarnungen" nicht auf einen über Jahrhunderte konsolidierten Erfahrungsschatz zurückgreifen. Ob sich im azentrischen Netzwerk der CSIRTs ohne Einrichtung einer zentralen Sammelstelle zur Auswertung der Indikatoren ein effektives Frühwarnsystem etabliert, bleibt abzuwarten. Für den gelingenden Aufbau eines europäischen Frühwarnmechanismus sind Prozesse der autonomen Rezeption und Fortentwicklung, d. h. des gegenseitigen Lernens, Voraussetzung. In technischer Hinsicht besteht hoher Forschungsbedarf, um die sensorbasierte und quellenbasierte Datengewinnung und Verfahren automatisierter Analyse von Frühwarnungen fortzuentwickeln.[135] Insbesondere das Problem, wie trotz der netzwerkartigen Struktur der CSRITS-Kooperation der „dringend benötigte Gesamtüberblick" ermöglicht werden kann, ist dabei eine Herausforderung.[136] Sekundärrechtlich wird das Verfahren zur Exploration neuer Kooperationsformen zur Aufgabe des CSIRTs-Netzwerk gemacht. Frühwarnungen können im CSRITs-Netzwerk zum Gegenstand der Erörterung gemacht werden, um weitere Formen der operativen Zusammenarbeit zu sondieren und zu ermitteln

---

[131] *Deleuze*/*Guattari*, Tausend Plateaus: Kapitalismus und Schizophrenie, Nachdr. der 6. Aufl. 2010, S. 36.

[132] *Augsberg*, Informationsverwaltungsrecht, 2014, S. 101; vgl. aber zur maßgeblichen Einbindung der Kommission im Schnellwarnsystem im Lebensmittelrecht Art. 50 Abs. 1 VO (EG) Nr. 178/2002.

[133] *Kaiser*, Wissensmanagement im Mehrebenensystem, in: Schuppert/Voßkuhle (Hrsg.), Governance von und durch Wissen, 2009, S. 217 (231); kritische organisationsrechtliche Bewertung bei *Gärditz*, Hochschulorganisation und verwaltungsrechtliche Systembildung, 2009, S. 209 ff.

[134] Siehe § 4 B. III.

[135] *Neugebauer*/*Jarke*/*Thoma* (Hrsg.), Herausforderungen für die IT-Sicherheitsforschung, 2014, S. 30 f.

[136] *Bundesamt für Sicherheit in der Informationstechnik*, Cyber-Sicherheit – IT-Lagezentrum – Frühwarnungen, abrufbar unter: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/IT-Lagezentrum/Fruehwarnung/ fruehwarnung_node.html.

(Art. 12 Abs. 3 lit. f. ii NIS-RL). Die ENISA hat ausdrücklich die Aufgabe, den Aufbau eines Frühwarnsystems in der Union, das die Systeme der Mitgliedstaaten ergänzt, zu unterstützen (Art. 3 Abs. 1 lit. b. vii). Da die Mitgliedstaaten ihre nationalen Strategien für die Sicherheit von Netz- und Informationssystemen, die gemäß Art. 7 Abs. 1 lit. e NIS-RL Angaben der Forschungs- und Entwicklungspläne behandeln müssen, der Kommission mitzuteilen sind (Abs. 3), besteht zumindest bei der Kommission ein Überblick darüber, ob und welche nationalen Forschungsprioritäten bezüglich eines Frühwarnsystems gesetzt werden. Auf den Forschungsbedarf kann die Kommission im CSIRTs-Netzwerk hinweisen, da ihr trotz des Beobachterstatus ein Rederecht zusteht.

c) Reaktion auf Sicherheitsvorfälle und Abschwächung von Risiken

Der Informationsaustausch über konkrete Sicherheitsrisiken und -vorfälle ist von herausgehobener Relevanz, da er geeignet ist, unmittelbar zur Gewährleistung der Sicherheit beizutragen.

aa) Horizontaler Informationsaustausch über Sicherheitsvorfälle

Der Informationsaustausch auf horizontaler, mithin nationaler und zwischenstaatlicher Ebene ist von erheblicher Bedeutung, da die Mitgliedstaaten eine oder mehrere für die Sicherheit von Netz- und Informationssystemen zuständige nationale Behörde benennen können.

(1) Informationsaustausch in Deutschland

Ein besonderer Informationsaustausch besteht hinsichtlich der gesammelten Informationen über die Sicherheit in kritischen Infrastrukturen.

Da die Meldungen bei Sicherheitsbeeinträchtigungen von Telekommunikationsunternehmen direkt an die Bundesnetzagentur zu richten sind, besteht das Erfordernis eines Informationsaustauschverhältnisses zwischen der Bundesnetzagentur und dem BSI. Die bei der Bundesnetzagentur eingegangenen Meldungen sowie die Informationen über die von dem betreffenden Unternehmen ergriffenen Abhilfemaßnahmen sind dementsprechend gemäß § 109 Abs. 5 S. 5 TKG unverzüglich an das BSI weiterzuleiten. Die Weiterleitungspflicht besteht indes nur, „soweit es sich um Sicherheitsverletzungen handelt, die die Informationstechnik betreffen". Dass nur „Sicherheitsverletzungen" und nicht auch alle gemeldeten Beeinträchtigungen weitergeleitet werden, steht in einem Spannungsverhältnis zu der Aufgabe des BSI, ein möglichst vollständiges und valides Lagebild zu erstellen.[137] Angesichts der technischen Möglichkeiten, eine

[137] BT-Drs. 18/4096, S. 36.

Nachricht mehreren Adressaten gleichzeitig zu melden, bleibt die Eignung des indirekten, über die Bundesnetzagentur verlaufenden Meldeweges zum BSI fragwürdig. Die Verlängerung des Meldewegs lässt sich allenfalls damit begründen, die Bundesnetzagentur übernehme eine gewisse Filterfunktion. Aus Gründen der operativen Funktionsfähigkeit der Informationsverarbeitung und angesichts notorisch unzureichender kognitiver Kompetenzen in der administrativen Wissensverarbeitung kann es sinnvoll sein, tatsächlich oder vermeintlich nicht erhebliche Informationen nicht zur Kenntnis nehmen zu müssen. Zu den Strategien im Wissensmanagement gehören vorab eingerichtete Sperren gegenüber der Wissensgewinnung.[138] Allerdings betrifft dieser Modus des Umgangs mit Informationen eher die menschliche als die automatisierte Datenverarbeitung. Insofern ist die Ausgestaltung des nationalen Informationstransfers Ausdruck herkömmlicher, am einzelnen Amtswalter orientierter Informationsverarbeitung.

Die Pflicht der Bundesnetzagentur, unverzüglich das BSI zu unterrichten, besteht im Übrigen gemäß § 109 Abs. 8 TKG hinsichtlich der im Rahmen von Sicherheitsaudits aufgedeckten Mängel bei der Erfüllung der Anforderungen in der Informationstechnik sowie für die in diesem Zusammenhang geforderten Abhilfemaßnahmen.

Dem BSI kommt es als zentrale Informationssicherheitsbehörde seinerseits zu, andere zuständige Bundesbehörden und die zuständigen Aufsichtsbehörden der Länder über die zur Erfüllung ihrer Aufgaben erforderlichen Informationen zu unterrichten (§ 8b Abs. 2 Nr. 4 c) BSIG). Als Adressaten kommen insbesondere das Bundesamt für Verfassungsschutz und der Bundesnachrichtendienst in Betracht, da die kritischen Infrastrukturen zum einen Gefahren durch terroristische Bestrebungen ausgesetzt sind, zum anderen Ziel von Angriffen „mit Bezug zur Bundesrepublik Deutschland" (vgl. § 5 Abs. 1 S. 3 Nr. 8 G10) sein können. Die Tätigkeit der Nachrichtendienste bezieht sich vor allem auf die Rückverfolgung von Schadsoftware im Ausland.[139] In praktischer Hinsicht kann der Informationsaustausch im Nationalen Cyber-Abwehrzentrum realisiert werden. Dort ist das BSI mit den anderen Bundesbehörden unter eine organisatorische Einheit zusammengefasst.[140] Die Weitergabe von Intelligence und sonstigen Informationen an die zuständigen Aufsichtsbehörden des Bundes und der Länder ist zwingend („hat […] unverzüglich […] zu unterrichten"). Die Formulierung weist auf die Begründung einer gesetzlichen Verpflichtung zur Kooperation hin, die über die Aufgabenzuweisungen des § 3 BSIG und die erforderlichen-

---

[138] *Augsberg*, Informationsverwaltungsrecht, 2014, S. 272.

[139] BT-Drs. 18/4096, S. 5.

[140] Siehe § 3 B. II. 3.

falls statthafte Amtshilfe gegenüber Strafverfolgungs- und Sicherheitsbehörden hinausgeht. Erkennen lässt sich in der Kooperationspflicht ein vorsichtiger Wandel vom Prinzip des „need to know“ hin zum Prinzip des „need to share”. Bei einem Informationsaustausch auf der Basis von „need to know“ werden nur Erkenntnisse weitergegeben, wenn diese unbedingt erforderlich sind, und nicht schon dann, wenn ein Austausch rechtlich erlaubt ist. Der Grundsatz des „need to share“ meint den erleichterten Austausch bzw. die Verpflichtung zum Datenaustausch.[141] Die Unterrichtung der Bundes- und Länderbehörden betrifft dem Wortlaut nach nur die zur Aufgabenerfüllung „erforderlichen Informationen“, die Pflicht zur unverzüglichen Weitergabe besteht aber in jedem Falle, sodass der Informationsaustausch im Ansatz begünstigt wird. In welcher Form das BSI das Datenmaterial bereitzustellen hat, ist fraglich. In Betracht kommen ausgehend vom Rohdatenmaterial verschiedene Verarbeitungsstufen. Im Ergebnis richtet sich die Form der Datenbereitstellung grundsätzlich danach, ob der Schutz von Quellen und Geheimnissen geboten ist oder ob rechtlich schutzwürdige Interessen der Betreiber kritischer Infrastrukturen dem Austausch entgegenstehen. Die zu übermittelnden Daten können dem rechtlichen Schutzbedürfnis angepasst werden. Je nach gebotenem Schutz können sie dann als unstrukturiertes Rohdatenmaterial, aggregiert (konsolidiert bzw. verdichtet) oder sanitarisiert (den Quellschutz beachtend) zur Verfügung gestellt werden.[142]

(2) Informationsaustausch zwischen den Mitgliedstaaten

Grundsätzlich wird der Informationsaustausch zwischen den Mitgliedstaaten nicht durch unmittelbare Pflichten angeleitet. Eine Ausnahme besteht für Informationen über meldepflichtige Sicherheitsvorfälle. Deren Austausch erfolgt horizontal und wird unionsrechtlich vorgegeben. Dabei ist zwischen Meldungen über Sicherheitsvorfälle bei Betreibern wesentlicher Dienste und denen bei Anbietern digitaler Dienste zu differenzieren.[143]

Die einer nationalen NIS-Behörde oder einem CSIRTs von einem Betreiber kritischer Infrastrukturen gemeldeten Informationen sind einem anderen betroffenen Mitgliedstaat mitzuteilen (Art. 14 Abs. 5 NIS-RL). Über Sicherheitsvorfälle bei Anbietern digitaler Dienste sind andere Mitgliedstaaten nur „gegebenenfalls“ zu unterrichten (Art. 16 Abs. 6 NIS-RL).

---

[141] Vgl. auch *Best*, Intelligence Information: Need-to-Know vs. Need-to-Share, CRS 2011, S. 13; *Jäger*/*Daun* (Hrsg.), Geheimdienste in Europa: Transformation, Kooperation und Kontrolle, 2009, S. 156.

[142] BT-Drs. 18/4096, S. 27.

[143] Siehe zu den Meldepflichten § 3 D. I. 2.

Die Schwelle zur Weiterleitungspflicht ist gemessen an der Bedeutung der grenzüberschreitenden Zusammenarbeit der Mitgliedstaaten und der grenzüberschreitenden Tätigkeit der Betreiber und Anbieter von internetbezogenen Infrastrukturen und Diensten hoch.[144]

Die Pflicht zur Weitergabe der Informationen über Sicherheitsvorfälle bei kritischen Infrastrukturen greift nur, sofern der Vorfall erhebliche Auswirkungen auf die Verfügbarkeit wesentlicher Dienste in jenem Mitgliedstaat hat. Dies erfordert eine Feststellung durch die zuständige Behörde. Informationen über Sicherheitsvorfälle, die nur potenziell eine grenzüberschreitende Folge haben, müssen nicht übermittelt werden. Ausgenommen von der Weiterleitungspflicht sind zudem Sicherheitsvorfälle, die andere Schutzziele der Netz- und Informationssicherheit neben der Verfügbarkeit, d. h. die Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder entsprechender Dienste, betreffen.

Die Weitergabe der Informationen über Sicherheitsvorfälle bei digitalen Diensten hängt ebenfalls davon ab, ob die weitergebende Behörde selbst annimmt, dass ein Vorfall mit grenzüberschreitendem Bezug vorliegt. Der Sicherheitsvorfall muss zwei oder mehr Mitgliedstaaten betreffen. Denkbar sind aber auch andere Fallgestaltungen („gegebenenfalls und insbesondere, wenn […]“). Insofern kommt der Behörde tatsächlich wie rechtlich ein Wertungsspielraum zu. Die eventuell bestehende Informationspflicht ist in inhaltlicher Hinsicht nicht auf Sicherheitsvorfälle begrenzt, welche die Verfügbarkeit von digitalen Diensten betreffen.

Der horizontale Informationsaustausch in seiner europäischen Dimension lässt sich als Ausfluss der strategisch angelegten Informationskooperation der Mitgliedstaaten deuten. Den Informationspflichten liegt ein Gratifikationsprinzip zugrunde. Durch die Begrenzung der Informationspflicht bei Vorfällen in wesentlichen Diensten, die die Verfügbarkeit eines Dienstes betreffen, sind letztlich nur solche Vorfälle verpflichtend weiterzuleiten, deren Folgen sich potenzieren und auf den meldenden Mitgliedstaat zurückschlagen können. Eine unmittelbare Pflicht zur (ausschließlich) fremdnützigen Informationsweitergabe ergibt sich aus den Informationspflichten gerade nicht.

Eine nationale Entsprechung dieser Informationspflicht besteht für das BSI nicht. Dagegen trifft die Bundesnetzagentur eine aktive Unterrichtungspflicht gegenüber den „nationalen Regulierungsbehörden anderer Mitgliedstaaten“ nach § 109 Abs. 5 S. 3 TKG. Diese werden „erforderlichenfalls“ über die ihr gemeldeten Sicherheitsverletzungen unterrichtet. Solange eine entsprechend klarstellende Regelung für das BSI nicht besteht, kommt allerdings die Anwen-

[144] Vgl. Erwägungsgrund 49 NIS-RL.

dung von § 8d VwVfG in Betracht. Die Vorschrift regelt ein Tätigwerden der nationalen Behörde im Sinne einer Mitteilung von Informationen und Sachverhalten, sofern diese nach Maßgabe von Rechtsakten der Union geboten ist. § 8d VwVfG begründet selbst keine Verpflichtung zu einer Mitteilung, sondern macht diese nach Art und Umfang von Rechtsakten der Union abhängig.[145] Aus § 8e S. 1 VwVfG ergibt sich aber, dass die Regelung nur Anwendung findet, wenn der sekundärrechtliche Rechtsakt unmittelbare Wirkung entfaltet, im Übrigen mit Ablauf der jeweiligen Umsetzungsfrist. Auf § 8d VwVfG kann sich das BSI demnach erst mit Ablauf der Umsetzungsfrist der NIS-Richtlinie (vgl. Art. 25 NIS-RL) berufen.

bb) Horizontaler Informationsaustausch über Sicherheitsvorfälle mit vertikalen Bezügen

Für den Austausch von Informationen zwischen der mitgliedstaatlichen und der europäischen Ebene kommt dem CSIRTs-Netzwerk eine herausgehobene Position zu. Innerhalb dieses Netzwerks können Informationen zu einzelnen Sicherheitsvorfällen ausgetauscht und bereitgestellt werden (Art. 12 Abs. 3 lit. c NIS-RL) sowie Informationen im Zusammenhang mit diesem Vorfall und damit verbundenen Risiken ausgetauscht und erörtert werden (Art. 12 Abs. 3 lit. b NIS-RL).

(1) Informationen zu einzelnen Sicherheitsvorfällen im CSIRTs-Netzwerk

Informationen über einzelne Sicherheitsvorfälle werden unionsrechtlich auf freiwilliger Basis im CSIRTS-Netzwerk ausgetauscht und bereitgestellt. Die mitgliedstaatlichen Aufgaben im CSIRTs-Netzwerk nehmen Vertreter der mitgliedstaatlichen CSIRTs wahr. Dem sekundärrechtlichen Leitbild gemäß werden lediglich „nicht vertrauliche" Informationen ausgetauscht. Die Vertraulichkeit bezieht sich auf unternehmensbezogene Daten.[146] Die Informationen betreffen demnach grundsätzlich keine nach Unionsrecht oder dem Recht eines Mitgliedstaates geschützten Unternehmensgeheimnisse wie spezifische technische Rahmendaten oder Sicherheitslücken, hinsichtlich derer ein Unternehmen ein berechtigtes Geheimhaltungsinteresse hat.

Die Beschränkung des Informationsaustausches auf nicht vertrauliche Informationen entspricht nicht der herkömmlich CSIRTs zugeschriebenen Rolle im Ökosystem der IT-Sicherheit.

---

[145] *Ramsauer*, in: Kopp/ders., VwVfG, 17. Aufl. 2016, § 8d, Rn. 1.

[146] Vgl. Erwägungsgrund 41 NIS-RL.

Als zentrale Anlaufstellen für IT-Sicherheitsprobleme zeichnen sich CSIRTs durch ihre Vertrauensstellung aus, die sich aus der persönlichen Zusammenarbeit sowie aus der Institutionalisierung als Einrichtung für dringende Nothilfe ergibt.[147] Ein besonderes Merkmal ist die Verschwiegenheit. Dies kommt insbesondere in der Vernetzung und Kooperation der CSIRTs untereinander zum Tragen. Vertraulichkeit und Vertrauen spielen die zentrale Rolle, um Sicherheitsprobleme und Vorfälle kommunizieren und besprechen zu können. Das institutionelle Vertrauen in CSIRTs-Vernetzungen wird vor allem durch besondere Auswahl- und Aufnahmeverfahren hergestellt. Das Forum for Incident Response and Security Teams (FIRST) ist das weltweite Forum für CSIRTs. Um Mitglied der Vereinigung zu werden, müssen CSIRTs über ein CSIRT eingeführt werden, dem bereits vertraut wird (*trusted introducer*).[148] Durch diese Prozesse hat sich bei den CSIRTs eine eigene Kultur des Vertrauens und der Gegenseitigkeit etabliert.

Insofern ist die deskriptive Klarstellung in Art. 12 Abs. 3 lit. c NIS-RL, dass nichtvertrauliche Informationen freiwillig über das CSIRTs-Netzwerk ausgetauscht werden, so zu verstehen, dass bestehende informelle und vertrauenswürdige Kanäle und Netzwerke für den Austausch von sicherheitsbezogenen Informationen zwischen CSIRTs nicht berührt werden sollen.[149] Die NIS-RL erhebt demnach hinsichtlich des vertikalen Informationsaustausches nicht den Anspruch, die Informationsbeziehungen zwischen den CSIRTs abschließend informationsverwaltungsrechtlich zu ordnen. Die Nutzung und Weiterentwicklung von vertrauensbasierten, europäischen Informationsaustauschverfahren im Wege der Selbstregulierung der CSIRT ist somit nicht durch eine Sperrwirkung des Unionsrechts ausgeschlossen.[150]

Ein weiterer Meldeweg für Sicherheitsverletzungen besteht zwischen den nationalen telekommunikationsrechtlichen Regulierungsbehörden und der Europäischen Agentur für Netz- und Informationssicherheit. Auf Grundlage von Art. 13a Abs. 3 UAbs. 2 S. 1 RL 2009/140/EG und gemäß § 109 Abs. 5 S. 3 TKG hat die Bundesnetzagentur „erforderlichenfalls" die ENISA über von Telekommunikationsunternehmen gemeldete Sicherheitsverletzungen zu unterrichten.

Gegen diesen zusätzlichen Informationskanal spricht zumindest rechtlich nicht die dem BSI zugewiesene Rolle als zentrale Stelle für die Zusammenarbeit

---

147 Siehe § 3 A. III.

148 Dazu *Skierka*/*Morgus*/*Hohmann*/*Maurer*, CSIRT Basics for Policy-Makers, 2015, S. 10, online abrufbar; vgl. *Cormack*, Incident Response and Data Protection, Version 2.0, 2011, S. 7, online abrufbar.

149 Vgl. Erwägungsgrund 59 NIS-RL.

150 Vgl. zur möglichen Beteiligung von CSIRTs an internationalen Kooperationsnetzen Anhang I Nr. 1 lit. d NIS-RL.

mit den zuständigen ausländischen Stellen. Die Aufgabe des zentralen Kommunikationsknotens übernimmt das BSI unbeschadet besonderer Zuständigkeiten anderer Stellen (§ 3 Abs. 1 S. 2 Nr. 16 BSIG).[151]

Die Zweckmäßigkeit dieser interbehördlichen vertikalen Informationspflicht ist zu bezweifeln. Zum einen hat die ENISA selbst keinen operativen Auftrag. Sie unterstützt den Aufbau von Fähigkeiten durch spezifische Maßnahmen zur Erleichterung der Zusammenarbeit (vgl. Art. 3 Abs. 1 lit. b ENISA-VO). Innerhalb des eingerichteten CSIRTs-Netzwerks führt die ENISA lediglich die Sekretariatsgeschäfte und unterstützt die aktive Zusammenarbeit zwischen den CSIRTs. Die Aufgabe eines gleichberechtigten Gebers und Nehmers von Informationen über Sicherheitsvorfälle ist ihr nicht zugewiesen. Zum anderen besteht mit Art. 3a Abs. 3 UAbs. 2 S. 1 RL 2009/140/EG bzw. § 109 Abs. 5 S. 3 TKG eine überflüssige Parallelstruktur für den Austausch von Informationen über Sicherheitsverletzungen. Es sind die CSIRTs, die bereits gemäß ihrer Bezeichnung den Auftrag haben, Sicherheitsinformationen zu bewerten, Sicherheitsvorfälle zu erkennen und die Betroffenen bei deren Eindämmung zu unterstützen. Sie besitzen die notwendige Expertise im Umgang mit außergewöhnlichen Sicherheitsvorfällen in Netzen und Informationssystemen und zeichnen sich durch schnelle Reaktionszeiten aus. Sie haben die erforderliche Erfahrung in der Kommunikation mit anderen Akteuren der IT-Sicherheit und können Sacherhalte effizienter besprechen. Sofern der Sinn und Zweck der telekommunikationsrechtsspezifischen Meldestruktur darin zu sehen ist, Sicherheitsinformationen mit grenzüberschreitender Relevanz auf europäischer Ebene bereitzustellen, wird dieser Zweck bereits durch die Einrichtung des CSIRTs-Netzwerk erfüllt. Der Informationsaustausch über die CSIRTs ist typischerweise auch zügiger und damit effektiver. Geht es auf strategischer Ebene darum, aus den Sicherheitsmeldungen langfristiges Erfahrungswissen abzuleiten, so ist die Kooperationsgruppe die geeignete Einrichtung. Zu ihren Aufgaben gehört insbesondere die „Sammlung von Informationen über bewährte Verfahren bei Risiken und Sicherheitsvorfällen“ (Art. 11 Abs. 3 lit. i NIS-RL). Der Beitrag der informationsverwaltungsrechtlichen Pflicht des § 109 Abs. 5 S. 3 TKG ist demnach zweifelhaft.[152]

---

[151] Im Übrigen können der Bundesnetzagentur unbeschadet der Zuständigkeit anderer Stellen nach § 140 Abs. 1 S. 2 TKG internationale Aufgaben im „Eigenbefugnisbereich“ zukommen, *Groebel*, in: Säcker (Hrsg.), TKG, 3. Aufl. 2013, § 140 Rn. 1 ff.

[152] Eine weitere Pflicht zum vertikalen Informationsaustausch kann sich für die Bundesnetzagentur im Übrigen aus Art. 5 Abs. 2 RL 2002/21/EG ergeben. Danach hat die nationale Regulierungsbehörde der Kommission alle Informationen zur Verfügung zu stellen, die sie zur Erfüllung der sich aufgrund des AEUV ergebenden Aufgaben benötigt. Diese Pflicht ist fachgesetzlich in § 123b TKG umgesetzt, der die weiteren Voraussetzungen regelt. Die Vorschrift ist Verbindung mit § 123a TKG vor allem im Kontext der Informationsübermittlung im Regulierungsverbund der nationalen Telekommunikationsregulierungsbehörden zu lesen

(2) Informationen im Zusammenhang mit Sicherheitsvorfällen und über Computerkriminalität

Über das CSIRTs-Netzwerk werden neben Informationen zu einzelnen Sicherheitsvorfällen solche Informationen ausgetauscht, die im Zusammenhang mit einem konkreten Sicherheitsvorfall stehen. Welche Kontextinformationen Gegenstand dieses formalisierten Informationsaustausches sein können, wird durch die Vorschrift nicht näher spezifiziert. Der Wortlaut von Art. 12 Abs. 3 lit. b NIS-RL erlaubt es, insbesondere auch solche Informationen auszutauschen oder zum Gegenstand der Erörterung zu machen, die eine Relevanz für die Strafverfolgung aufweisen. Die Strafverfolgung im Bereich des Computerstrafrechts ist in besonderer Weise auf Informationen angewiesen.

Die Virtualisierung und die Vernetzung der informationstechnischen Systeme haben Folgen für die Attribution der angreifenden Akteure. Die Erkenntnis, dass der technische Ausgangspunkt eines Kommunikationsvorgangs identifiziert wurde, bedeutet nicht, dass davon ausgegangen werden kann, dass an eben diesem Ort die Kommunikation initiiert wurde. Durch Proxy-Programme können Internetverbindungen verschleiert werden, indem eine Kette von Verbindungen aufgebaut wird, die nur sehr aufwendig oder gar nicht zurückverfolgt werden kann. Für die Cyberforensik stellen sich demnach vor allem Probleme bei der Identifizierung der handelnden Personen zur Beweissicherung. Ihre Bestimmung und Nachverfolgung wird durch Praktiken der Anonymisierung oder Verschleierung oder des Identitätsdiebstahls erschwert.[153]

CSIRTs haben häufig Zugang zu den erforderlichen forensischen Informationen, unterliegen aber keinem Ermittlungszwang. Anders als Strafverfolgungsbehörden müssen CSIRTs nicht nach dem Legalitätsprinzip bei tatsächlichen Anhaltspunkten Ermittlungen einleiten und ihre Quellen und Erkenntnisse schützen. Für den darauf bezogenen Austausch von Informationen bedarf es insofern einer rechtlichen Anleitung. Art. 12 Abs. 3 lit. b NIS-RL sieht diesbezüglich vor, dass Informationen im Zusammenhang mit einem konkreten Sicherheitsvorfall „auf Antrag" des Vertreters eines CSIRTs im CSIRTs-Netzwerk ausgetauscht und erörtert werden. Der Informationsaustausch vollzieht sich *ad hoc* und damit im Wege der Informationshilfe. Antragsberechtigt sind nur CSIRT-Vertreter eines potenziell betroffenen Mitgliedstaats. Entsprechend

---

(vgl. § 123b Abs. 4). Das maßgebliche Gremium Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) übernimmt indes keine Aufgabe mit Bezug zur Gewährleistung der Netz- und Informationssicherheit, Art. 2 und 3 VO (EG) Nr. 1211/2009; vgl. *Schönau*, in: Geppert/Schütz (Hrsg.), BeckTKG, 4. Aufl. 2013, § 123b Rn. 1.

[153] *Brodowski*/*Freiling*, Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, 2011, S. 24.

dem Wesen dieses Mittels zur Informationskooperation in fremden Aufgabenbereichen ist der Informationsaustausch kein Automatismus. Die Informationshilfe resultiert nicht aus einer Informationsbeschaffungspflicht. Das CSIRT eines jeden Mitgliedstaats, d. h. nicht nur eines von einem Sicherheitsvorfall betroffenen Mitgliedstaats, kann daher die Beteiligung an diesen Erörterungen ablehnen, wenn die Gefahr einer Beeinträchtigung der Untersuchung des Vorfalls besteht (Art. 12 Abs. 3 lit. b 2. HS NIS-RL).

Trotz dieser Möglichkeit, den Antrag am Maßstab der Opportunität abzulehnen, und trotz der Vorgabe, dass nur „wirtschaftlich nicht sensible Informationen" ausgetauscht oder erörtert werden, stellt sich die Frage, ob bereits von der bloßen Möglichkeit, einen Informationsantrag zu stellen, ein Abschreckungseffekt (*chilling effect*) für den Informationsaustausch über Sicherheitsvorfälle ausgeht. Durch die Antragstellung wird im CSIRTs-Netzwerk eine Situation hervorgerufen, zu der sich der adressierte Mitgliedstaat kommunikationstheoretisch nicht nicht verhalten kann. Zumindest muss sich das CSIRT eines Mitgliedstaats durch eine Ablehnung des Erörterungswunsches verhalten. Gerade weil CSIRTs auf Vertrauensbasis operieren und sie Informationen auch von privaten Dritten beziehen können, kann ein CSIRT im Einzelfall ein Interesse daran haben, dass der Informationsaustausch keine strafprozessualen Ermittlungen nach sich zieht. Dieses Interesse kann insbesondere darin begründet sein, dass ein über einen Sicherheitsvorfall informierendes Unternehmen selbst Ziel von Ermittlungen werden könnte. Um seine Informationskanäle zu schützen und nicht in das Dilemma zu geraten, seine Quellen aufdecken zu müssen, könnte eine CSIRT davon Abstand nehmen, an dem – ohnehin nur auf freiwilliger Basis bestehenden – Informationsaustausch aktiv zu partizipieren. Da ein Antrag über den Austausch von Kontextinformationen überhaupt die Kenntnis über einen Sicherheitsvorfall voraussetzt, kann ein CSIRT die problematische Information gezielt vorenthalten, um einen Antrag nicht ablehnen zu müssen und auf diese Weise negative Auswirkungen auf die Vertrauensbeziehung zu anderen CSIRTs zu riskieren.

Im Ergebnis lässt sich festhalten, dass der Austausch von Informationen im Zusammenhang mit Sicherheitsvorfällen, insbesondere solcher mit Relevanz für die Strafverfolgung, kaum über das Informationsverwaltungsrecht gesteuert wird. Den Akteuren, denen Freiraum für opportunistische Erwägungen eingeräumt ist, wird der Austausch weitgehend selbst überlassen. Indem sich das Sekundärrecht in der NIS-RL auf die Beschreibung gesetzgeberischer Leitbilder beschränkt, können gleichwohl bestehende informelle etablierte Informationskanäle zwischen den CSIRTs mit einem je eigenen Modus vivendi erhalten bleiben. Der Austausch außerhalb der durch die NIS-RL vorgegebenen informationsverwaltungsrechtlichen Verfahren muss dem an sich bezweckten Informationsaustausch der Sicherheitsgewährleistung nicht abträglich sein.

cc) Reaktion auf einen Sicherheitsvorfall

Prävention allein kann keinen vollständigen Schutz vor konkreten Gefahren bieten. Denn Sicherheitsvorfälle ereignen sich trotz Präventions- und Detektionsmaßnahmen. Daher ist Reaktion auf Sicherheitsvorfälle Bestandteil jedes Konzepts zur Sicherheitsgewährleistung. Wegen der Spontaneität von Sicherheitsvorfällen sind Dringlichkeit, Dezision und Reaktion im Informationsaustausch erforderlich. Um in Situationen zeitnah handeln zu können, müssen alle mit der Gewährleistung der Sicherheit Beauftragen auf den Ernstfall vorbereitet sein. Ein darauf bezogener Informations- und Wissensaustausch verhindert übereiltes und unsachgemäßes Vorgehen und dient der Schadensminimierung.

(1) Austausch impliziten Wissens durch Übungen

Ein nützliches Instrument zur Prüfung der Abwehrbereitschaft der Mitgliedstaaten und deren Zusammenarbeit sind Übungen, bei denen Szenarien für Sicherheitsvorfälle in Echtzeit simuliert werden. Aus wissenstheoretischer Sicht sind Übungspraktiken vor allem geeignet, den sozialen Charakter der Wissensgenerierung und des Wissenstransfers zu entsprechen. Implizites Wissen, das nicht ohne Weiteres verbalisiert artikuliert werden kann, wird nämlich durch praktische Übung, d. h. durch „Nachahmung des ausgewiesenen Könners", und in personaler Interaktion erworben und ausgebildet.[154] Der Transfer dieser Form von Wissen ist außerhalb des binnenstaatlichen Kontexts und damit in transnationalen Konstellationen vor besondere Herausforderungen gestellt, da der Ersatz eigener Kenntnisse durch den Rückgriff auf die der anderen ein gewisses Vertrauen in Informationsquellen und die Akzeptanz nicht *ad hoc* überprüfbarer Verlässlichkeit voraussetzt.[155]

Zum Mandat der ENISA gehört es, die Organisation und Durchführung von Übungen auf Unionsebene zu unterstützen (Art. 3 Abs. 1 lit. b v) ENISA-VO). Allerdings sind die Mitgliedstaaten nicht verpflichtet, Übungen zu planen oder an ihnen teilzunehmen. Auf freiwilliger Basis finden dennoch Cyber-Übungen statt, aus deren Evaluierung Empfehlungen abgeleitet werden können.[156] Ungeachtet tatsächlich durchgeführter Übungen besteht zwischen den Mitgliedstaaten Informationsaustauschbedarf hinsichtlich der Planung und der strategischen

---

[154] *Augsberg*, Informationsverwaltungsrecht, 2014, S. 81.

[155] Vgl. *Scherzberg*, Zum Umgang mit implizitem Wissen- eine disziplinenübergreifende Perspektive, in: Schuppert/Voßkuhle (Hrsg.), Governance von und durch Wissen, 2008, S. 240 (240 ff.).

[156] ENISA, The 2015 Report on National and International Cyber Security Exercises, 2015, S. 26 ff.

Entscheidungen über die Ziele der Übungen.[157] So müssen die Prioritätsfelder, die Ausgestaltung der Szenarien, die Regelmäßigkeit, die Rollen und Übungssteuerung abgestimmt werden.[158] Vorgesehener Ort der Diskussion dieser Entscheidungen ist die Kooperationsgruppe. Die „durchgeführten Arbeiten im Zusammenhang mit Übungen" sind dort zu erörtern (Art. 11 Abs. 3 lit. k NIS-RL). Die Formulierung dieser Aufgabenzuweisung lässt aber kaum darauf schließen, dass noch durchzuführende Arbeiten, mithin Planungen von Übungen, Gegenstand der Debatte zu sein haben. Auch die im CSIRTs-Netzwerk stattfindende Erörterung der aus den Übungen „gezogenen Lehren" (Art. 12 Abs. 3 lit. h NIS-RL) hält rechtlich die Mitglieder wohl kaum an, Übungen zu initiieren und mit Unterstützung der ENISA durchzuführen. Die dem Projektmanagement entlehnte Terminologie, wie der Begriff „gezogene Lehren" (*lessons learnt*), verweist darauf, dass Erfahrungswissen zur zukünftigen Fehlervermeidung dokumentiert und erhalten werden soll.

Der Beitrag der informationsverwaltungsrechtlichen Regelungen ist hinsichtlich der Übungen für die Sicherheit von Netzen und Informationssystemen weitgehend auf die der Kooperationsgruppe zugewiesene Aufgabe der Dokumentation und Erörterung erfolgreich und weniger erfolgreich erprobter Prozesse in der Vergangenheit beschränkt.

(2) Koordinierte Reaktion

Ist in einem Netz oder einem Informationssystem ein Sicherheitsvorfall eingetreten, gilt es vorrangig, die Sicherheitsmängel zu beheben. Es ist die eigentliche Aufgabe der CSIRTs, auf Sicherheitsvorfälle zu reagieren (Art. 9 Abs. 1 NIS-RL in Verbindung mit Anhang I Nr. 2 lit. a iii) NIS-RL).

In der forensischen Informatik werden verschiedene Vorgehensmodelle behandelt, die den Prozess des sog. Incident Response in eine Reihe logischer Schritte unterteilen. Gemeinsam haben die Modelle, dass die Bewältigung auch eines akuten Vorfalls die Herstellung der Analysefähigkeit voraussetzt, beispielsweise indem Logdateien hergestellt und gesichert werden. Die hypothesenbasierten Modelle sind daher Grundlage für die Formulierung einer Reaktionsstrategie.[159] Die koordinierte Reaktion auf einen Sicherheitsvorfall erfordert vor allem deshalb den Austausch von Informationen, weil prinzipiell alle zur Verfügung stehenden Umstandsinformationen für die Abfassung einer kohärenten Strategie einzubeziehen sind.[160]

---

[157] Erwägungsgrund 42 NIS-RL.

[158] Vgl. zu politisch umstrittenen Übungen BT-Drs. 17/7578, S. 15.

[159] *Dewald*/*Freiling* (Hrsg.), Forensische Informatik, 2015, S. 151 (156).

[160] *Mandia*/*Prosise*, Incident Response and Computer Forensics, 2003, S. 151 ff.

Die grenzüberschreitende Reaktion auf einen Sicherheitsvorfall wird grundsätzlich im CSIRTs-Netzwerk koordiniert. Eingeleitet wird der dafür erforderliche Informationsaustausch jedoch nur auf Antrag des Vertreters des CSIRT eines Mitgliedstaats (Art. 12 Abs. 3 lit. d NIS-RL). Der Vorgängerentwurf zur NIS-RL sah noch vor, dass sich die zuständigen Behörden im Anschluss an eine Frühwarnung auf eine koordinierte Reaktion einigen mussten, die gemäß einem Kooperationsplan erfolgen sollte, den die Kommission ermächtigt gewesen wäre, mittels Durchführungsrechtsakten anzunehmen.[161] Durch das Antragserfordernis erübrigt sich jedweder Automatismus im gemeinsamen Vorgehen. Zusätzlich wird die Koordination durch den Vorbehalt geschwächt, dass die koordinierte Reaktion nur auszuarbeiten ist, sofern dies möglich ist. Praktisch besteht damit kein Mechanismus, der die koordinierte Reaktion auf Sicherheitsvorfälle gemäß informationsrechtlicher Standards etabliert. Mangels Sperrwirkung des Antragserfordernisses werden damit bestehende Informationsnetzwerke unter den CSRITs stabilisiert.

(3) Zusammenarbeit mit Datenschutzbehörden bei der Bearbeitung von Sicherheitsvorfällen bei wesentlichen Diensten

Kommt es in wesentlichen Diensten bzw. kritischen Infrastrukturen zu einem Sicherheitsvorfall, der zur Verletzung des Schutzes personenbezogener Daten führt, kooperiert die NIS-Behörde bei der Bearbeitung des Sicherheitsvorfalls eng mit den Datenschutzbehörden (Art. 15 Abs. 4 NIS-RL).

Aus dem systematischen Zusammenhang der Vorschrift ergibt sich, dass die Kooperation („enge Zusammenarbeit“) nicht schon bei der Bearbeitung bekannt gemachter oder gemeldeter Sicherheitsvorfälle greift, sondern nur bei Vorfällen in wesentlichen Diensten bzw. kritischen Infrastrukturen und dies auch nur bei der Verletzung des Schutzes personenbezogener Daten.

Die unionsrechtliche Pflicht zielt zudem auf die gemeinsame „Bearbeitung“ von Sicherheitsvorfällen. Damit ist der Begriff von der „Bewältigung von Sicherheitsvorfällen“ abzugrenzen. Unter Letzterer sind nach dem weiten Begriffsverständnis von Art. 4 Nr. 8 NIS-RL alle Verfahren zur Unterstützung der Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen sowie die Reaktion auf solche Vorfälle zu verstehen. Für die Bewältigung von Sicherheitsvorfällen sind nicht nur die NIS-Behörden, sondern auch die CSIRTs nach einem genau festgelegten Ablauf zuständig.[162]

Bearbeitung kann enger als Teil des sog. Security Incident Handling verstanden werden, und zwar als der Teil, der sich vorrangig mit der Behebung von

[161] Art. 11 COM(2013) 48 final.

[162] Siehe § 4 B II. 2. c) cc).

Sicherheitsvorfällen beschäftigt (Security Incident Response).[163] Bei der Störungsbehebung wird kontrolliert, ob ähnliche Störungen bereits aufgetreten sind und geeignete Lösungen zur Beseitigung der Fehlerursachen vorhanden sind oder ob nur deren Symptome beseitigt bzw. im Sinne eines Workarounds umgangen werden.[164] Für die Untersuchung und Beseitigung eines Sicherheitsvorfalls „ist das entsprechende Fachwissen" die „unabdingbare Voraussetzung", die Leitlinie des BSI sieht daher vor, dass das Verfahren zur Bereitstellung des notwendigen Expertenwissens vorbereitet sein soll.[165] Das Kooperationsgebot des Art. 15 Abs. 4 NIS-RL entspricht demnach dem sicherheitstechnischen Bedürfnis einer Zusammenführung des Fachwissens.

Das Kooperationsgebot kompensiert ein Stück weit die fehlende konsistente Harmonisierung der Meldepflichten. Da im Falle einer Sicherheitsverletzung, die zugleich eine Verletzung des Schutzes personenbezogener Daten darstellt, sowohl eine Meldung an die NIS-Behörden als auch an die Datenschutzbehörden in Betracht kommt,[166] kann zumindest im Rahmen der Zusammenarbeit eine gleichförmige Qualifikation und Bewertung des Sicherheitsvorfalles stattfinden.[167]

Eine allgemeine Pflicht des BSI zur Kooperation mit Datenschutzbehörden bei der Bearbeitung von Sicherheitsvorfällen besteht nicht. Die Unterrichtungspflicht des BSI gemäß § 5 Abs. 9 BSIG ist keine Umsetzung dieser Vorgabe. Das BSI unterrichtet den Bundesbeauftragten für Datenschutz und Informationsfreiheit über bestimmte Datenverarbeitung im Rahmen der Gefahrenabwehr für die Kommunikationstechnik des Bundes. Ungeachtet dessen, dass die Vorschrift die Sicherheit der Kommunikationstechnik des Bundes betrifft, ist darin kein Gebot zur Zusammenarbeit zu sehen, da das BSI mit dem Bundesbeauftragten nicht etwa einen Konsens herstellen, sondern eine Kontrolle *ex post* ermöglichen soll. Es liegt insofern beim nationalen Gesetzgeber, das über die Amtshilfe hinausgehende Zusammenarbeitsgebot näher zu spezifizieren.

---

[163] Vgl. BSI, IT-Grundschutz, B 1.8 Behandlung von Sicherheitsvorfällen, 11. EL Stand 2009.

[164] Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz, M 6.64 Behandlung von Sicherheitsvorfällen, 13. EL Stand 2013.

[165] Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz, M 6.64 Behandlung von Sicherheitsvorfällen, 13. EL Stand 2013.

[166] Siehe § 3 D. 2. und 3. Zur Kritik *Schallbruch*, CR 2016, 663 (668).

[167] Zur Erfordernis differenzierter Klassifizierungen eines Sicherheitsvorfalls Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz, M 6.131 Qualifizieren und Bewerten von Sicherheitsvorfällen, 11. EL Stand 2009.

III. Förderung des Informationsaustausches

Gelingende Informationsbeziehungen sind auch bei Bestehen von Informationsrechten und -pflichten keine Selbstverständlichkeit. Mitgliedstaaten kommen ihren in den Rechtsakten nur vage formulierten Informationsübermittlungspflichten häufig nicht hinreichend nach.[168] Verwaltungen unterliegen zudem Organisationsproblemen. Sie unterscheiden sich nicht nur durch die verschiedenartigen verfassungsrechtlichen Hintergründe, Abhängigkeiten und Loyalitätsverhältnisse, unterschiedliche Verfahren sowie Verwaltungskulturen, sondern letztlich auch durch die Sprache und ihr Selbstverständnis.[169]

Die dem Informationsaustausch abträglichen organisatorischen und kulturanthropologischen Gegebenheiten können indes durch rechtlich geleitete Mechanismen eingehegt werden.[170]

So sind für das Unionsrecht Prinzipien entwickelt worden, deren Qualität im Einzelfall die eines Rechtsgrundsatzes oder die eines ordnenden Konzepts ist.[171] Prinzipien unterscheiden sich durch Regeln dadurch, dass sie als Optimierungsgebote nach weitgehender Realisierung streben.[172] An erster Stelle zu nennen ist der Grundsatz der loyalen Zusammenarbeit, der zu den „verbundmoderierenden Prinzipien" gehört, die den Informationsaustausch quantitativ wie qualitativ zu fördern geeignet sind (1.). Im Zusammenhang mit sicherheitskritischen Informationen spielt zudem das Vertrauen eine bedeutende Rolle. Zum Aufbau der Vertrauensbasis können informationsverwaltungsrechtliche Maßnahmen beitragen (2.). Weiteres primärrechtliches Informationsverwaltungsrecht aktiviert den Wissenstransfer nur begrenzt (3.).

1. Grundsatz der loyalen Zusammenarbeit

Aus dem Grundsatz der loyalen Zusammenarbeit lässt sich eine allgemeine Kooperationspflicht ableiten (a), aus der Anforderungen an den Gehalt der ausgetauschten Information sowie die Art und Weise ihrer Übermittlung folgen (b).

---

[168] *Heußner*, Informationssysteme im Europäischen Verwaltungsverbund, 2007, S. 162.

[169] *Vogel*, National Styles of Regulation, 1986, passim; *von Bogdandy*, Die Informationsbeziehungen im europäischen Verwaltungsverbund, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band II, 2. Aufl. 2012, § 25 Rn. 4.

[170] Dazu *Terhechte*, Europäisches Verwaltungsrecht und europäisches Verfassungsrecht, in: ders. (Hrsg.), Verwaltungsrecht der Europäischen Union, 2011, § 7 Rn. 36 ff.

[171] Siehe *von Bogdandy*, Grundprinzipien, in: ders./Bast (Hrsg.), Europäisches Verfassungsrecht, 2. Aufl. 2009, S. 13 ff., *Tridimas*, The General Principles of EU Law, 2. Aufl. 2007, passim.

[172] In diesem Sinne *Dworkin*, Taking rights seriously, 1978, S. 22 ff.; *Alexy*, Theorie der Grundrechte, 1985, S. 71 ff.

a) Allgemeine Kooperationspflicht

Der Grundsatz der loyalen Zusammenarbeit ist in Art. 4 Abs. 3 und Art. 13 Abs. 2 S. 2 EUV kodifiziert. Ihm kommt eine Funktion zu, die vergleichbar ist mit der Bundestreue im Bundesstaat. Dort wird dieses Institut zur Begründung von Informationspflichten, zur Pflicht gegenseitiger Abstimmung und zur Kooperation und Konsultation herangezogen.[173] In der föderal aufgebauten Europäischen Union kann diesem auf alle Unionsbereiche anwendbaren Grundsatz auch in den europäischen Informationsbeziehungen Bedeutung zukommen, da aus ihm nicht nur eine Pflicht zur gegenseitigen Rücksichtnahme folgt, sondern auch eine allgemeine Kooperationspflicht mit wechselseitigen Informationspflichten.[174] Die Pflichten entfalten sich sowohl im Vertikalverhältnis als auch im Horizontalverhältnis zwischen den Mitgliedstaaten.[175] Das Gebot der loyalen Zusammenarbeit ermöglicht allerdings für sich noch keine effektiven Informationsflüsse in der täglichen Praxis. Denn es lässt sich nicht ableiten, welche Voraussetzungen eine Kooperationspflicht im Einzelfall auslösen. Für die Ausgestaltung konkreter Informationspflichten bedürfte es nach dem Grundsatz der begrenzten Einzelermächtigung (Art. 5 Abs. 1 und 2 EUV) jeweils einer gesonderten Ermächtigung im Primärrecht. Ungeschriebene Informationspflichten hat der Europäische Gerichtshof jedoch anerkennt, sofern diese essentiell für das Funktionieren der Union sind.[176] Ungeachtet sekundärrechtlicher Detailregelungen verpflichtet Art. 4 Abs. 3 EUV jedenfalls dazu, die Kooperationsverfahren in loyaler Weise zu gebrauchen, wobei sich die Verpflichtung vor allem auf Informations- und Konsultationspflichten fokussiert.[177] Stützt die Kommission ein Auskunftsverlangen etwa auf Art. 337 AEUV, kann sie ihrem Begehren mit Verweis auf die Kooperationspflicht Nachdruck verleihen.[178]

Jedenfalls verstärkt die allgemeine Kooperationspflicht die bestehenden informationellen Regelungen und ist zumindest geeignet, den Informationsaustausch zu fördern.

---

[173] *Bauer*, Die Bundestreue, 1992, S. 8 ff., 346 ff.

[174] EuGH, C-105/03, Rn. 41 ff.; EuGH, C-251/89, Rn. 57.

[175] *Wille*, Die Pflicht der Organe der Europäischen Gemeinschaft zur loyalen Zusammenarbeit mit den Mitgliedstaaten, 2003, S. 128 f.

[176] Dazu *Schmidt-Aßmann*, Strukturen europäischer Verwaltung und die Rolle des Europäischen Verwaltungsrechts, in: Blankenagel/Pernice/Schultz-Fielitz (Hrsg.), Verfassung im Diskurs der Welt, 2004, S. 395 (402).

[177] *Wille*, Die Pflicht der Organe der Europäischen Gemeinschaft zur loyalen Zusammenarbeit mit den Mitgliedstaaten, 2003, S. 47 ff.

[178] Weitergehend *Herrmann*, in: Streinz (Hrsg.), EUV/AEUV, 2. Aufl. 2012, AEUV, Art. 337 Rn. 1.

b) Inhaltliche Anforderungen an auszutauschende Informationen

Aus dem Kooperationspflicht können neben der grundsätzlichen Bedeutung für die Verwaltungskooperation praktische Anforderungen hinsichtlich des Gehalts der Information und der Art und Weise ihrer Übermittlung folgen. Das Informationsaustausch-Paradigma in der NIS-Kooperation beruht auf Annahmen bezüglich der Qualität, welche die Informationen aufweisen müssen. Expliziert sind die Eigenschaften, die ausgetauschte Informationen aufweisen müssen, in der NIS-RL indessen nicht. Damit Informationen verarbeitet werden können, müssen sie im Kontext der Sicherheitsgewährleistung grundsätzlich anschlussfähig (*actionable)* verlässlich (*reliable*) und handhabbar (*manageable*) sein.[179] Wird etwa eine Information über eine bereits bekannte IT-Sicherheitsschwachstelle geteilt, hat sie kaum einen Mehrwert für die empfangende Stelle. Ebenso nutzlos kann eine Information über unbekannte Schwachstellen sein, wenn die Fähigkeit und Kapazität fehlt, die entsprechenden Schutzmaßnahmen zu ergreifen. Informationen sind zudem irrelevant, wenn sie vom Empfänger nicht verarbeitet werden können. Ferner bemisst sich das Potenzial der Analyse im Rahmen von Monitoring- und Anomalieerkennungsverfahren an der Qualität der Algorithmen und daran, dass die analytisch festgestellten Muster von den Nutzern der Informationen als nützlich identifiziert werden.[180]

Soweit inhaltliche Anforderungen nicht durch die zu erlassenden Durchführungsrechtsakte der Kommission aufgestellt werden, kann Art. 4 Abs. 3 EUV selbst oder in Verbindung mit einer Hauptpflicht zur Informationsübermittlung herangezogen werden, um bestimmte Eigenschaften einzufordern. Primärrechtlich lassen sich etwa Anforderungen wie Entscheidungserheblichkeit (Relevanz), Verständlichkeit, Vergleichbarkeit, Wahrhaftigkeit, Vollständigkeit und Aktualität begründen.[181] In bestimmten Konstellationen dürfte außerdem die Nachprüfbarkeit und die Klarheit zu nennen sein.[182] Aus dem Aspekt der „loyalen" Zusammenarbeit ließe sich in Kombination mit dem Grundsatz der Rechtsstaatlichkeit (Art. 2 EUV) sogar ein Grundsatz der Datenrichtigkeit im europäischen

---

[179] *Bambauer*, Sharing Shortcomings, Loyola University Chicago Law Journal Vol. 47 (2015), 465 (473); vgl. *ENISA*, Actionable information for security incident response, 2014, S. 2 ff., die als maßgeblich „relevance", „timelessness", „accuracy", „completeness" und „digestibility" auflistet.

[180] Ähnlich sind die Anforderungen von Software im Bereich Cybersicherheit, vgl. etwa *Palantir*, Cyber Security, abrufbar unter: www.palantir.com/solutions/cyber.

[181] *von Bogdandy*, Informationsbeziehungen im europäischen Verwaltungsverbund, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band II, 2. Aufl. 2012, § 25 Rn. 26.

[182] *Sommer*, Verwaltungskooperation am Beispiel administrativer Informationsverfahren im Europäischen Umweltrecht, 2003, S. 424 ff.

Verwaltungsverbund formulieren.[183] Untermauert werden können die inhaltlichen Anforderungen mit dem Erfordernis des *effet utile* (praktische Wirksamkeit) insbesondere für den Informationsaustausch im CSIRTs-Netzwerk, da hier die schnelle und effektive operative Kooperation Zweck des Netzwerks ist und das Bedürfnis nach operablen Informationen am stärksten ausgeprägt ist.

Neben Anforderungen an die Qualität sind solche an die Quantität denkbar. Der Kooperationsgrundsatz kann auch zum Schutz vor zu vielen Informationen herangezogen werden. Als Sorgfaltspflicht umfasst der Grundsatz, die Aufnahmekapazität des Empfängers zu prüfen.[184] Abzustellen wäre hier maßgeblich auf die informations- und kommunikationstechnologische Ausstattung der europäischen und mitgliedstaatlichen Stellen. Je dichter der Organisationsgrad der Informationskooperation und je besser die Kapazitäten der Sammlung, Strukturierung und Auswertung von Informationen sind, desto geringer dürfte das Schutzbedürfnis sein.[185]

Die Einhaltung dieser Anforderungen ist nicht sanktionsbewehrt. Der Grundsatz ist nicht in einem Regime eingebettet, das die Rechtsfolgen der „Schlechtübermittlung" regelt. Der Verweis auf die Kooperationspflicht könnte freilich als verfassungsrechtliches Argument eingesetzt werden und mag so in Informationsbeziehungen als Legitimation der Ansprüche an die Qualität dienen.

2. Rechtliche Sicherung des gegenseitigen Vertrauens

Gegenseitiges Vertrauen ist eine außerrechtliche Voraussetzung für funktionierende Informationsaustauschbeziehungen in der NIS-Kooperation (a). Vertrauen kann rechtlich durch Maßnahmen der Erwartungsstabilisierung gefördert werden (b). Mit einer gewissen Ungewissheit ist beim Informationsaustausch umzugehen (c).

a) Vertrauen als Gelingensvoraussetzung der NIS-Informationskooperation

Gegenseitiges Vertrauen ist eine Wirksamkeitsbedingung zur Verwirklichung von Regelungen.[186] Eine Ordnung bereitzustellen, die Vertrauen ermöglicht,

[183] Vgl. *von Bogdandy*, Informationsbeziehungen im europäischen Verwaltungsverbund, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band II, 2. Aufl. 2012, § 25 Rn. 26.

[184] *Heußner*, Informationssysteme im Europäischen Verwaltungsverbund, 2007, S. 298 f.

[185] Vgl. *Sommer*, Verwaltungskooperation am Beispiel administrativer Informationsverfahren im Europäischen Umweltrecht, 2003, S. 32.

[186] Zum gegenseitigen Vertrauen im Europarecht *Majone*, Mutual Trust, Credible Commitments and the Evolution of Rules for a Single European Market, EUI Working Paper 1995; vgl. *Vesting*, Die Medien des Rechts: Schrift, 2011, S. 51; vgl. im Zusammenhang der justiziellen Zusammenarbeit im Raum der Freiheit, der Sicherheit und des Rechts *Kaufhold*, EuR

kann zu den zentralen Aufgaben des Rechts gezählt werden.[187] Die Mitgliedstaaten und deren Behörden als Vertrauenssubjekte müssen sich gegenseitig vertrauen können, damit Informationsflüsse tatsächlich entstehen. Vertrauen ist dann erforderlich, wenn Handlungsausführende oder Systeme mit einer Unwissenheit behaftet sind oder wenn die beteiligten Akteure nur über ein Teilwissen verfügen.[188] Wird Vertrauen entgegengebrachtbedeutet dies, dass die am Geschehen Beteiligten die Erwartung haben, dass sich ein Geschehen auf eine bestimmte Weise entwickelt oder zu einem bestimmten Ergebnis führt.[189] Vertrauen beruht auf Erfahrung und damit auf stabilisierten Erwartungen, also auf solchen, die sich bestätigt haben. Insbesondere wenn das Fehlen eigener Expertise oder einer eigenen Informationsbasis durch das Gegenüber substituiert werden soll, damit Wissen ressourcenschonend nicht selbst generiert und geprüft werden muss, bedarf es des Vertrauens.[190] Misstrauen kann sich nachteilig auf die Qualität und Validität der Vertrauensobjekte, die Informationen und die Vertraulichkeit des Informationskanals, auswirken.

Den Aufbau von Vertrauen in der Kooperationsgruppe und im CSIRTs-Netzwerk erhebt die NIS-RL ausdrücklich zum Ziel der durch sie festgelegten Maßnahmen (Art. 1 Abs. 2 lit. b und c NIS-RL).

b) Konkrete Maßnahmen der Erwartungsstabilisierung

Das Recht kann normative Sicherungsmechanismen bereitstellen, welche die sozialen Funktionen der persönlichen Ebene und der gesellschaftlichen Konvention institutionalisieren. Es kann sowohl Grund als auch Gegenstand von Vertrauen sein (Vertrauen durch Recht und in Recht).[191] Allgemeine Rechtsgrundsätze des Unionsrechts und die allgemein akzeptierten „Standards guter Verwaltungspraxis“ wirken vertrauenssichernd, erzeugen Vertrauen aber nicht unmittelbar.[192] Konkrete Maßnahmen zur Förderung des Vertrauens können nicht darin bestehen, Unwissen durch Wissen zu ersetzen, denn Vertrauen ist hier Voraussetzung für die Ingangsetzung des Informationstransfers. Maßnahmen zur Vertrauensbildung sind daher Maßnahmen der Erwartungsstabilisierung.

2012, 408 (417); *Schwarz*, Grundlinien der Anerkennung im Raum der Freiheit, der Sicherheit und des Rechts, 2016, S. 367 ff.

[187] Dazu *Bumke*, Relative Rechtswidrigkeit, 2004, S. 11 f.

[188] *Luhmann*, Vertrauen, 5. Aufl. 2014, S. 27 ff.

[189] *Kaufhold*, EuR 2012, 408 (419).

[190] Vgl. *Krämer*, Medium, Bote, Übertragung, 2008, S. 253 f.

[191] Vgl. *Vesting*, Die Medien des Rechts: Schrift, 2011, S. 111; *Augsberg*, Informationsverwaltungsrecht, 2014, S. 83.

[192] *Stelkens*, in: ders./Bonk/Sachs (Hrsg.), VwVfG, 8. Aufl. 2014, Europäisches Verwaltungsrecht, Europäisierung des Verwaltungsrechts und Internationales Verwaltungsrecht, Rn. 185.

Als Vertrauenssubjekte adressiert die NIS-RL die Mitgliedstaaten. Es sind im Einzelnen sowohl Gesetzgeber als auch Amtswalter, die Vertrauen entgegenbringen müssen und die konkrete Beiträge ungeachtet ihrer Qualität akzeptieren und daran weitere eigene Handlungen anschließen. Konkrete Quellen, aus denen sich das Vertrauen in eine verlässliche Umgebung für den Informationsaustausch speisen kann, sind die zu schaffenden Infrastrukturen, die den Austausch von sensiblen und vertraulichen Informationen gewährleisten sollen. Dieser Aspekt ist zu berücksichtigen, wenn die Mitgliedstaaten die Pflicht umsetzen, „sichere" Kommunikationskanäle zu schaffen (vgl. Art. 8 Abs. 5 NIS-RL). Relevant für den vertrauensvollen Austausch sensibler Informationen ist in diesem Zusammenhang der Beschluss des Rates über die Sicherheitsvorschriften 2013/488/EU, der die Grundprinzipien und Mindeststandards für die Sicherheit in Bezug auf den Schutz von EU-Verschlusssachen festlegt.[193] Die Vorgaben gelten für den Rat und dessen Generalsekretariat, werden aber von den Mitgliedstaaten nach Maßgabe ihrer jeweiligen innerstaatlichen Vorschriften beachtet (Art. 1 Abs. 2 Beschluss 2013/488/EU). So sollen alle Seiten darauf vertrauen dürfen, dass für die EU-Verschlusssachen ein gleichwertiges Schutzniveau gewährleistet wird.

Da die NIS-RL keine Sperrwirkung für alternative, informale Informationsbeziehungen entfaltet, kommt Vertrauensordnungen Bedeutung zu, die im Wege der Selbstregulierung entstehen. Relevanz haben vor allem Nichtveröffentlichungsvereinbarungen (*non-disclosure agreements*). Zu diesen gehört das Ampel-Protokoll (*traffic light protocol*), bei dem es sich um eine standardisierte Vereinbarung zum Austausch von schutzwürdigen Dokumenten handelt, die vor allem von CSIRTs angewendet wird.[194] Die Einstufung von Informationen anhand einer Farbskala soll den ungewollten Informationsabfluss an Dritte verhindern. Empfänger von Informationen mit der Klassifizierung „Rot" dürfen nur im Kreise der auf das Protokoll Verpflichteten mit in einer Besprechung anwesenden Personen ausgetauscht werden. Rechtliche Verbindlichkeit kommt den Protokollen nicht zu.

Die Bildung von Vertrauen in der NIS-Kooperation wird demnach durch konkrete Maßnahmen hinsichtlich der Vertrauensobjekte unmittelbar wie mittelbar durch das Gewähren von Raum für Vertrauensordnungen, die sich im Wege der Selbstregulierung bilden, gefördert.

---

[193] Vgl. Erwägungsgrund 8 NIS-RL.

[194] ENISA, Good Practice Guide, Network Security Information Exchanges, 2009, S. 17.

c) Umgang mit Ungewissheit als Gewissheit

Bezweckt die NIS-Richtlinie den *Aufbau* von gegenseitigem Vertrauen, impliziert dies, dass die Mitglieder der Kooperation hinzunehmen haben, dass eine Gewissheit über die Qualität der Kooperationsbeiträge oder über das Maß an Vertraulichkeit nicht immer besteht. Das Recht kann nicht darüber hinweghelfen, dass gewisse Unwägbarkeiten immer bestehen. Es kann aber Impulse für die Vertrauenserzeugung setzen. Der sekundärrechtlich aufgestellte Zweck der Vertrauensbildung ist demzufolge zugleich als normativer Appell an die Mitgliedstaaten und ihre Amtswalter zu lesen, die vorgesehenen Kooperationsmechanismen im Hinblick auf den Umgang mit der Ungewissheit zu vollziehen. Als Anreiz dafür, Vertrauen aufzubringen und Unsicherheiten hinzunehmen, können die möglichen Folgen fehlenden Vertrauens angeführt werden. Dazu können nicht nur Umsetzungs- und Vollzugsdefizite, sondern langfristig eine verstärkte Zentralisierung von Rechtssetzung und Rechtsanwendung gehören.[195] Die Kommission müsste im Wege von Durchführungsrechtsakten verstärkt Regelungen zur Vereinheitlichung und Harmonisierung schaffen. Die Mitgliedstaaten hätten zulasten ihres Spielraums mit erwartungsstabilisierenden, d. h. konkretisierenden Initiativen zu rechnen, die darauf abzielen, ihre Spielräume zu verengen.[196]

3. Primärrechtliche Möglichkeiten der Stärkung des Wissenstransfers

Das Primärrecht erlaubt der Union, die Mitgliedstaaten in ihren Bemühungen zur Verbesserung der Fähigkeit der Verwaltungen zu unterstützen (a). Das Auskunftsrecht der Kommission nach Art. 337 AEUV ist weitgehend bedeutungslos, da der Kommission für den Bereich der Netz- und Informationssicherheit keine Aufgaben vom AEUV übertragen sind (b).

a) Parallelität der mitgliedstaatlichen Informationsverarbeitung

Die weitgehend bei den Mitgliedstaaten liegende Vollzugsautonomie erlaubt es den Rechtsordnungen, eigene Handlungsrationalitäten weiterzuentwickeln.[197] Konträr zur mitgliedstaatlichen Fragmentierung steht das Erfordernis einer „ge-

---

[195] *Majone*, Mutual Trust, Credible Commitments and the Evolution of Rules for a Single European Market, EUI Working Paper 1995, S. 2 ff.

[196] Zu Misstrauen als produktiver Ressource der Institutionenbildung in der Internet Governance siehe *Hofmann*, Constellations of Trust and Distrust in Internet Governance, in: Report of the Expert Group ‚Risks of Eroding Trust – Foresight on the Medium-Term Implications for European Research and Innovation Policies', 2015, S. 8.

[197] Steffen *Augsberg*, Europäisches Verwaltungsorganisationsrecht und Vollzugsformen, in: Terhechte (Hrsg.), Verwaltungsrecht der Europäischen Union, 2011, § 6 Rn. 13; *Ladeur*, Die Bedeutung des Allgemeinen Verwaltungsrechts für ein Europäisches Verwaltungsrecht,

wissen Parallelität der Erkenntnisproduktion“ durch gleichförmige Daten- und Informationsverarbeitung.[198] Das Konzept des Lernverbunds ist nämlich auf eine gewisse Mindestharmonisierung von Problemwahrnehmungs- und Lösungsstrategien angewiesen.[199]

Das Unionsrecht macht in Art. 6 S. 1 AEUV an prominenter Stelle durch eine klare Formulierung deutlich, dass die Union „für die Durchführung von Maßnahmen zur Unterstützung, Koordinierung oder Ergänzung der Maßnahmen der Mitgliedstaaten zuständig“ ist. Die Maßnahmen können nach Art. 6 S. 2 lit. g AEUV im Bereich der Verwaltungszusammenarbeit getroffen werden. Der Begriff der Durchführung ist dabei weit zu verstehen. Darunter fällt jede durch das Unionsrecht veranlasste mitgliedstaatliche Tätigkeit.[200] Als „Eckpfeiler des Verwaltungsverfassungsrechts der EU“[201] – es ist die einzige Norm des Titels „Verwaltungszusammenarbeit“ – macht Art. 197 Abs. 1 AEUV integrationspolitisch deutlich, dass die Durchführung des Unionsrechts im „gemeinsamen“ Interesse von Union und Mitgliedstaaten liegt. Damit bildet Art. 197 Abs. 1 AEUV ein Gegengewicht zu dem in einem komplementären Verhältnis stehenden Art. 291 AEUV, nach dem die administrative Durchführung des Unionsrechts primär eine mitgliedstaatliche Aufgabe bezeichnet.[202]

Die Union kann gemäß Art. 197 Abs. 2 S. 3 durch eine Verordnung die erforderlichen Maßnahmen ergreifen, um die Mitgliedstaaten bei der Durchführung des Unionsrechts zu unterstützen. Allerdings bildet Art. 197 Abs. 2 AEUV bereits dem Wortlaut nach lediglich eine Unterstützungskompetenz und ist mit Blick auf die punktuell anderen Sachbereichen zugeordneten Kompetenzen eng auszulegen.[203] In seiner Funktion und aufgrund der Systematik bleibt Art. 197

---

in: Trute/Groß/Röhl/Möllers (Hrsg.), Allgemeines Verwaltungsrecht – Zur Tragfähigkeit eines Konzepts, 2008, S. 795 (813 f.).

[198] *Augsberg*, Informationsverwaltungsrecht, 2014, S. 96.

[199] *Eifert*, Europäischer Verwaltungsverbund als Lernverbund, in: Spiecker gen. Döhmann/Collin (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, 2008, S. 159 (161).

[200] *Zuleeg*, Das Recht der Europäischen Gemeinschaften im innerstaatlichen Bereich, 1969, S. 47 f.; *Ohler*, in: Streinz (Hrsg.), EUV/AEUV, 2. Aufl. 2012, AEUV, Art. 197 Rn. 4; vgl. *von Bogdandy*, Die Informationsbeziehungen im europäischen Verwaltungsverbund, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band II, 2. Aufl. 2012, § 25 Rn. 1 Fn. 1; *Nettesheim*, in: Grabitz/Hilf/ders. (Hrsg.), AEUV/EUV, 57. Aufl. 2015, AEUV, Art. 6 Rn. 27.

[201] *Ruffert*, in: Calliess/ders. (Hrsg.), EUV/AEUV, 4. Aufl. 2011, AEUV, Art. 197 Rn. 1.

[202] *Terhechte*, Die föderalen Strukturen der Europäischen Union und das europäische Verwaltungsrecht, in: Härtel (Hrsg.), Handbuch Föderalismus, § 89 Rn. 35; vgl. *Ruffert*, in: Calliess/ders. (Hrsg.), EUV/AEUV, 4. Aufl. 2011, AEUV, Art. 197 Rn. 4 f.

[203] Vgl. *Ruffert*, in: Calliess/ders. (Hrsg.), EUV/AEUV, 4. Aufl. 2011, AEUV, Art. 197 Rn. 22.

Abs. 2 darauf beschränkt, die bestehende Koordinierungsfunktion der Union zu thematisieren.[204] Aus der Kompetenz können demzufolge konkrete Kooperationspflichten nur durch Sekundärrecht begründet werden.[205] Art. 197 Abs. 1 AEUV ist also Interpretationshilfe für die Auslegung etwaiger Pflichten, die insofern schonend für die Mitgliedstaaten ausgelegt werden sollen.[206] Unmittelbare Informationsbefugnisse auf Unionsebene lassen sich demnach nicht aus Art. 197 Abs. 1 AEUV ableiten.

Wesentliches Potenzial zur Förderung des Wissenstransfers entfaltet Art. 197 Abs. 2 AEUV als Grundlage für Maßnahmen zur Verbesserung der mitgliedstaatlichen Verwaltungsfähigkeiten. Ausdrücklich sind die Erleichterung des Informationsaustausches und der Austausch von Beamten als Unterstützungsmaßnahmen genannt. Die Mitgliedstaaten müssen diese Unterstützung nicht annehmen (Art. 197 Abs. 2 S. 3 AEUV). Jedenfalls besteht mit dieser Norm eine primärrechtliche Grundlage, den Sender- und Empfängerhorizont beim Personal der am Informationsaustausch beteiligten NIS-Stellen durch Ausbildungsprogramme zu koordinieren und eine harmonisierte Wahrnehmung des Kontexts zu schaffen.

b) Allgemeine Informationsbefugnis der Kommission

Der Kommission als Vertreterin der Unionsinteressen obliegt es, für die Erfüllung des Unionsrechts Sorge zu tragen. Zur Erfüllung der ihr übertragenen Aufgaben hat die Kommission die Befugnis aus Art. 337 AEUV, „alle erforderlichen Auskünfte" einzuholen. Art. 337 AEUV hat eine größere Reichweite, als die deutsche Formulierung „Auskünfte einholen" vermuten lässt. In der englischen (*collect any information*) und französischen (*recueillir toutes information*) Fassung wird deutlich, dass die Informationsbeschaffung nicht auf eine bestimmte Art und Weise der Informationseinholung beschränkt ist.[207] Trotz ihrer Stellung in den Schlussbestimmungen wird die Informationsbefugnis da-

---

[204] Zur vertraglichen Verankerung der Verwaltungskooperation zwischen Mitgliedstaaten und Union durch Art. 197 AEUV *Frenz*, DÖV 2010, 66 (73).

[205] *Classen*, in: Grabitz/Hilf/Nettesheim (Hrsg.), AEUV/EUV, 57. Aufl. 2015, AEUV, Art. 197 Rn. 53; *Schmidt-Aßmann,* Perspektiven der Europäisierung des Verwaltungsrechts, in: Axer/Grzeszick/Kahl/Mager/Reimer (Hrsg.), Das Europäische Verwaltungsrecht in der Konsolidierungsphase, Die Verwaltung, Beiheft 10, 2010, S. 263 (272).

[206] So *Classen*, in: Grabitz/Hilf/Nettesheim (Hrsg.), AEUV/EUV, 57. Aufl. 2015, AEUV, Art. 197 Rn. 53.

[207] *Ladenburger*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Europäisches Unionsrecht, Band 4, 7. Aufl. 2015, AEUV, Art. 284 Rn. 6. Ausgenommen sind allerdings Sondertatbestände wie Sachverhaltsermittlungen vor Ort, vgl. *Sommer*, Verwaltungskooperation am Beispiel administrativer Informationsverfahren im Europäischen Umweltrecht, 2003, S. 373 ff.

her als *sedes materiae* des unionalen Informationsverwaltungsrechts bezeichnet.[208] Die Befugnis wird zum einen als Instrument der Vollzugskontrolle diskutiert. Zur Kompensation einer fehlenden Weisungsbefugnis gegenüber den zuständigen Aufsichtsstellen in den Mitgliedstaaten soll die Kommission, falls sie von Umständen Kenntnis erlangt, die auf die Missachtung von Unionsrecht in einem Mitgliedstaat schließen lassen, die Befugnis nach Art. 337 AEUV zur Vorbereitung eines Vertragsverletzungsverfahrens anwenden.[209] Sie wird zum anderen als Kompetenz diskutiert, auf die akzessorische Regelungen zur Festlegung der an einem Informationssystem zu beteiligenden Verwaltungsstellen, die Einrichtung nationaler Datenbanken und die Formulierung von Anforderungen an die zu übermittelnden Informationen zur unionsweiten Vergleichbarkeit gestützt werden können.[210]

Das informationsverwaltungsrechtliche Potenzial von Art. 337 AEUV für die europäische NIS-Verwaltung ist jedoch gering. Die Kommission kann von diesem Primärrecht nur zur Erfüllung der ihr übertragenen Aufgaben Gebrauch machen. Die Aufgabe muss dabei vom AEUV übertragen sein.[211] Da nun die Netz- und Informationssicherheit kein eigenständiger Politikbereich im kompetenzbeschränkenden Sinne des Art. 352 AEUV ist bzw. sich das Recht der europäischen NIS-Verwaltung im Wesentlichen mit Art. 114 AEUV auf eine zielbezogene Kompetenz mit Querschnittscharakter stützt und der Kommission keine Aufgabe zugewiesen ist, kommt Art. 337 AEUV als Grundlage für eine Stärkung des vertikalen Informationstransfers grundsätzlich nicht in Betracht. Auf die im Übrigen strittige Frage, ob die primärrechtliche Befugnis nur soweit reicht, wie sekundärrechtlich noch keine Pflicht auf Grundlage des Art. 337 AEUV festgelegt wurde, kommt es daher nicht an.[212]

Ungeachtet dessen steht Art. 337 AEUV unter einem Ausführungsvorbehalt. Der Rahmen und die nähere Maßgabe der Anwendung der Informationsbefugnis sind durch den Rat festzulegen (Art. 337 2. HS AEUV). Der Rat hat bis dato keine Ermächtigung nach dieser Vorschrift erteilt.[213]

---

[208] *Ladenburger*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Europäisches Unionsrecht, Band 4, 7. Aufl. 2015, AEUV, Art. 284 Rn. 3.

[209] *Arndt*/*Fischer*/*Fetzer*, Europarecht, Rn. 111.

[210] So *Heußner*, Informationssysteme im Europäischen Verwaltungsverbund, 2007, S. 252.

[211] EuGH, C-490/10, Rn. 63.

[212] Dazu *Herrmann*, in: Streinz (Hrsg.), EUV/AEUV, 2. Aufl. 2012, AEUV, Art. 337 Rn. 1.

[213] *Ladenburger*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Europäisches Unionsrecht, Band 4, 7. Aufl. 2015, AEUV, Art. 284 Rn. 9.

C. Besondere Grenzen des Informationstransfers

Der freie Informationsfluss genießt keinen immanenten Vorrang vor anderen rechtlich geschützten Interessen. Dem freien Informationsaustausch zwischen differenzierten Verwaltungseinheiten sind dort Grenzen gesetzt, wo schutzwürdige Belange dies erfordern. Gerade in sensiblen Bereichen hat das Recht dafür Sorge zu tragen, dass der Transfer von Informationen und Wissen rechtlich gestaltet ist, da mit dem Wechsel der Sphären die Beherrschbarkeit von Wissen beeinträchtigt ist.[214] Die Weitergabe und Übermittlung von Informationen im Rahmen der Kooperation zur Gewährleistung der Sicherheit von Netzen und Informationssystemen können insbesondere durch den Datenschutz (I.), den Schutz unternehmensbezogener Daten (II.) durch die organisationsrechtliche Ausgestaltung von NIS-Behörden (III.) oder das Auskunftsverweigerungsrecht der Mitgliedstaaten (IV.) begrenzt sein.

I. Grenzen des Informationstransfers durch den Datenschutz

Das europäische Verfassungsrecht macht in Art. 39 EUV und 16 Abs. 2 AEUV deutlich, dass neben dem Schutz natürlicher Personen der „freie Datenverkehr" ein zu schützendes Gut ist. In der Diskussion um den Datenschutz wird häufig übersehen, dass der freie Informationsfluss ein Ziel für sich ist, das der Datenschutz nicht unangemessen einschränken darf:[215] „Das Recht auf Schutz personenbezogener Daten […] muss im Hinblick auf seine gesellschaftliche Funktion gesehen […] werden."[216] Anders gewendet kann das Datenschutzrecht als Datenverkehrsrecht verstanden werden, das aber „nicht der Abschottung von Informationen" dient.[217]

Die Übermittlung personenbezogener Daten ist gleichwohl rechtfertigungsbedürftig, da die Übermittlung ein Akt der datenschutzrechtlichen Datenverarbeitung ist (vgl. Art. 4 Nr. 2 DS-GVO).[218] Eine Übermittlung im datenschutz-

---

[214] *Spiecker gen. Döhmann*, Wissensverarbeitung im Öffentlichen Recht, Rewi 2010, 247 (270).

[215] *Frenz*, Handbuch Europarecht, Band 4, 2009, Rn. 1358; vgl. allgemein *Kuner*, Transborder Data Flows under Data Protection and Privacy Law, 2013, S. 121 ff.; *Ballaschk*, In the Unseen Realm: Transnational Intelligence Sharing in the European Union – Challenges to Fundamental Rights and Democratic Legitimacy, Stanford Journal of International Law 2015, 19 (19 ff.).

[216] Erwägungsgrund 4 S. 2 DS-GVO.

[217] *Gurlit*, DVBl. 2003, 1119 (1121).

[218] Im Rahmen der europäischen NIS-Kooperation werden – abhängig von der datenschutzrechtlichen Bewertung von Maschinendaten und sonstigen identifizierenden Kennungen – personenbezogene Daten ausgetauscht, vgl. etwa den Austausch von IP-Adressen zwi-

rechtlichen Sinne ist das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass die Daten an den Dritten weitergegeben werden oder der Dritte Gelegenheit zur Einsicht oder zum Abruf bereitgehaltener Daten erhält. Das angewendete Verfahren ist für dieses Verständnis nicht von Belang.[219] Von entscheidender Bedeutung ist, dass die Kenntnis über den Inhalt der Daten vermittelt wird; eine Übertragung physischen Besitzes am Datenträger ist nicht erforderlich.[220]

Der Europäische Gerichtshof hat, ohne dies näher zu begründen und ohne weiter innerhalb der Datenschutzrechte zu differenzieren, die Weitergabe an einen Dritten, auch an eine andere Behörde, unabhängig von der späteren Verwendung als Beeinträchtigung betrachtet.[221] Eine Beeinträchtigung des Grundrechts auf Achtung des Privatlebens (Art. 7 GRCh) sei unabhängig davon gegeben, ob die betreffenden Informationen einen sensiblen Charakter haben oder ob die Betroffenen durch den Eingriff Nachteile erlitten haben könnten.[222] Gleiches gelte für die Beeinträchtigung des Datenschutzgrundrechts (Art. 8 GRCh). Eine Beeinträchtigung umfasse jeden Verarbeitungsvorgang.[223] Die Eingriffsqualität hängt nach teilweise vertretener Auffassung auch nicht von einer Zweckidentität ab, d. h., in ein Grundrecht werde ungeachtet dessen eingriffen, ob bei der empfangenden Stelle die Daten zum ursprünglichen Verwendungszweck verarbeitet werden.[224] Die Effektivität des Informationsaustausches ist damit grundsätzlich auf Rechtfertigungsebene zur Geltung zu bringen.[225]

---

schen deutschen Behörden und europäischen Stellen, Antwort der Bundesregierung (18/4437) auf eine Kleine Anfrage der Fraktion Die Linke (18/4267), Antwort Nr. 18: „Die mit einem Schadprogramm infizierten Computersysteme versuchen in der Regel, mit einem Kontrollserver Kontakt aufzunehmen. Seit der Abschaltung der Botnetz-Infrastruktur werden diese Verbindungsanfragen protokolliert. Das BSI erhält vom CERT-EU seit dem 25. Februar 2015 in unregelmäßigen Abständen entsprechende Informationen über IP-Adressen in Deutschland. Diese werden an die jeweils zuständigen Provider mit der Bitte weitergeleitet, die Kunden über die vermutete Infektion ihrer PCs zu informieren."

[219] *Buchner*, in: Taeger/Gabel (Hrsg.), BDSG, 2. Aufl. 2013, BDSG, § 3 Rn. 35.

[220] *Eßer*, in: Auernhammer, 4. Aufl. 2014, BDSG, § 3 Rn. 56.

[221] EuGH, verb. Rs. C-405/00, C-138/01, C-139/01, Rn. 74 f.

[222] EuGH, Urteil vom 08.04.2014 – C-293/12 u. C-594/12, Rn. 33.

[223] *Augsberg,* in: von der Groeben/Schwarze/Hatje (Hrsg.), Europäisches Unionsrecht, Band 1, 7. Aufl. 2015, GRCh, Art. 8 Rn. 11; *Kingreen,* in: Calliess/Ruffert (Hrsg.), EUV/AEUV, 4. Aufl. 2011, GRCh, Art. 8 Rn. 12.

[224] *Heußner*, Informationssysteme im Europäischen Verwaltungsverbund, 2007, S. 323; *Wettner*, Die Amtshilfe im europäischen Verwaltungsrecht, 2005, S. 323; a. A. *Scholz/Pitschas*, Informationelle Selbstbestimmung und staatliche Informationsverantwortung, 1984, S. 116 ff.

[225] Vgl. *Kment*, Grenzüberschreitendes Verwaltungshandeln, 2010, S. 689; *Heußner*, Informationssysteme im Europäischen Verwaltungsverbund, 2007, S. 323; *Wettner*, Die Amts-

Der Transfer personenbezogener Daten in der NIS-Kooperation kann sich auf allgemeine (1.) und fachgesetzliche Übermittlungsvorschriften stützen (2.). Die Übermittlung wird vor allem durch die besondere Zweckbindung bei Meldedaten begrenzt (3.).

1. Übermittlung nach Maßgabe des allgemeinen Datenschutzrechts

Die Datenverarbeitung gemäß der NIS-Richtlinie erfolgt nach Maßgabe der DS-GVO (Art. 2 NIS-RL in Verbindung mit Art. 94 Abs. 2 DS-GVO). Die Verarbeitung übermittelter personenbezogener Daten durch die Organe und Einrichtungen der Union erfolgt gemäß Art. 2 Abs. 2 NIS-RL nach Maßgabe der Verordnung (EG) Nr. 45/2001. Diese Verordnung und sonstige Rechtsakte der Union, die diese Verarbeitung personenbezogener Daten regeln, werden gemäß Art. 2 Abs. 3 S. 2 DS-GVO im Einklang mit Art. 98 DS-GVO an die Grundsätze und Vorschriften der vorliegenden Verordnung angepasst.

2. Übermittlung im Rahmen der Aufklärung von Cybergefahren zum Schutz kritischer Infrastrukturen

Fachgesetzliche Übermittlungsvorschriften bestehen für die Nachrichtendienste. Personenbezogene Daten dürfen vom Bundesamt für Verfassungsschutz zum Schutz kritischer Infrastrukturen an die NIS-Behörden übermittelt werden (a). Der Bundesnachrichtendienst darf die im Rahmen der strategischen Aufklärung gewonnenen Daten an das BSI übermitteln (b). Sondervorschriften für die Übermittlung von personenbezogenen Daten bestehen für die im Rahmen der Ausland-Ausland-Fernmeldeaufklärung generierten Informationen (c).

a) Übermittlung von Daten durch das Bundesamt für Verfassungsschutz

Die Übermittlung personenbezogener Daten durch das Bundesamt für Verfassungsschutz an nicht zum Verfassungsschutz gehörende Behörden regelt § 19 BVerfSchG. Das Bundesamt darf in drei Fällen Daten sowohl auf Ersuchen als auch nach dem Opportunitätsprinzip aus eigener Initiative an inländische Stellen übermitteln. Zulässig ist die Übermittlung zur eigenen Aufgabenerfüllung, ferner sofern der Empfänger die Daten zum Schutz der freiheitlich-demokratischen Grundordnung braucht und sofern der Empfänger die Daten sonst für Zwecke der öffentlichen Sicherheit im Rahmen der rechtlichen Aufgaben benötigt. Der Begriff der öffentlichen Sicherheit umfasst den Schutz aller Normen, die präventiv und repressiv zum Schutz des Staates, seiner Einrichtungen und

---

hilfe im europäischen Verwaltungsrecht, 2005, S. 321; *Scholz*/*Pitschas*, Informationelle Selbstbestimmung und staatliche Informationsverantwortung, 1984, S. 116 ff.

seiner Rechtsordnung gesetzt worden sind.[226] Für letztere Variante ergibt sich somit ein Nexus zum Schutz der kritischen Infrastrukturen. Ihnen kommt gemäß § 2 Abs. 10 Nr. 2 BSIG eine hohe Bedeutung für das Funktionieren des Gemeinwesens zu, weil Störungen zu Gefährdungen für die öffentliche Sicherheit führen könnten. Demzufolge darf das Bundesamt Daten an Stellen übermitteln, die für andere als die in § 3 Abs. 1 Nr. 1 bis 4 BVerfSchG genannten Zwecke benötigt werden. Auch wenn die Empfängerbehörde einen Aufgabenkreis hat, der weiter als der angegebene Zweck ist, ist sie an den konkreten Verwendungszweck gebunden.[227] In der präventiven Abwehr noch nicht konkreter Gefahren kommt vor allem eine Übermittlung an das BSI in Betracht.

b) Übermittlung der im Rahmen der Fernmeldeaufklärung von Cybergefahren gewonnenen Daten

Für den Bundesnachrichtendienst besteht mit § 9 BNDG eine nach § 19 Abs. 1 BVerfSchG entsprechende Rechtsgrundlage zur Datenübermittlung. Spezielle Übermittlungsbefugnisse finden sich für die im Rahmen der strategischen Fernmeldeaufklärung von Cybergefahren gewonnenen Daten.

Die nach § 5 Abs. 1 S. 1 in Verbindung mit § 5 Abs. 1 S. 3 Nr. 8 G10 erhobenen Daten dürfen nach § 7 Abs. 4a G10 vom BND unter besonderen Voraussetzungen an das BSI übermittelt werden. Die Daten müssen entweder erforderlich sein, um Gefahren für die Sicherheit in der Informationstechnik des Bundes abzuwehren, oder der Aufgabenerfüllung des BSI dienen, d. h. der Sammlung und Auswertung von Informationen über Sicherheitsrisiken für andere Stellen und Dritte. Die Übermittlung von Erkenntnissen über die Netz- und Informationssicherheit wird der Aufgabe des BSI als zentrale Meldestelle und Informationsmittler in diesem Bereich gerecht und entspricht dem Ansatz, für die Aufgaben des BSI eine möglichst große Datenbasis aufzubauen. Gleichsam sollen alle Akteure über die aktuelle Cybergefährdungslage informiert werden[228] Es müssen aber tatsächliche Anhaltspunkte dafür bestehen, dass die Daten für die Aufgaben dieser Behörden zur Sammlung und Auswertung von Informationen über Cybergefahren sowie zur Begegnung dieser Gefahren erforderlich sind. Die Hürde ist im systematischen Vergleich mit der Voraussetzung für die Übermittlung an andere Nachrichtendienste bei sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten niedriger (§ 7 Abs. 2 Nr. 2 G10 „bestimmte Tatsa-

[226] Vgl. *Denninger*, in: Lisken/ders. (Hrsg.), Handbuch des Polizeirechts, 5. Aufl. 2012, Rn. 16–34; vgl. BT-Drs. 11/4306, S. 63 (zu § 14).

[227] *Bock*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, BVerfSchG, § 19 Rn. 12.

[228] BT-Drs. 18/4654, S. 42.

chen"). Der Hintergrund ist darin zu sehen, dass aus Sicht des Gesetzgebers durch die Übermittlung keine Zweckänderung eintritt, das BSI also ohnehin beauftragt ist, Cyberangriffe zu erkennen, die auch sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht darstellen können. Andernfalls bedarf es für die Übermittlung „bestimmter Tatsachen", wie für die Übermittlung an das Bundesamt für Verfassungsschutz, da dort das Gesetz impliziert, dass die strategische Fernmeldeaufklärung grundsätzlich nicht der Aufklärung sicherheitsgefährdender oder geheimdienstlicher Tätigkeiten dient und deshalb die Übermittlung eine Zweckänderung darstellt.

Eine spezielle Übermittlung der Daten aus der SIGINT-Support-to-Cyber-Defense-(SSCD-)Strategie des BND an *ausländische* Stellen besteht mit § 7a G10. Der Gesetzgeber erkennt ausdrücklich an, dass „Cybergefahren […] Gefahren im internationalen Raum sind" und die Bundesrepublik „aufgrund der Komplexität und der internationalen Durchdringung Cyberbedrohungen nicht allein" entgegengetreten kann.[229] Die im Rahmen der strategischen Fernmeldeaufklärung gewonnenen Daten dürfen an ausländische Stellen übermittelt werden. Aus § 7a Abs. 1 S. 1 Nr. 3 G10 ergibt sich aber, dass es sich dabei um einen Austausch handelt. Das Prinzip der Gegenseitigkeit gehört zur Rechtsmäßigkeitsvoraussetzung der Datenübermittlung. Nur Staaten, die ihrerseits an ihren Erkenntnissen teilhaben lassen, sollen für einen Informationsaustausch in Betracht kommen.[230] Die Zusammenarbeit und das Zusammenlegen von Erkenntnissen im internationalen Verbund stellen das Kernelement der Strategie dar, die Systematik einer Schadsoftware zu erkennen.[231] Die Einhaltung des Gegenseitigkeitsprinzips muss mindestens mit einer bilateralen Verwaltungsvereinbarung verfestigt sein.[232] Als weiteres empfängerbezogenes Kriterium gilt, dass die Empfängerbehörde mit „nachrichtendienstlichen Aufgaben" betraut sein muss. Im europäischen Kontext kann keine so trennscharfe Unterscheidung zwischen Geheim- bzw. Nachrichtendienst und Polizei vorgenommen werden wie in Deutschland.[233] Insofern kann die Empfängerbehörde eine Stelle sein, die nach deutschem Verständnis nicht für eine Datenübermittlung des BND infrage kommt. Aufgefangen werden kann diese mögliche Friktion durch eine Zweckbindung der Daten. § 7a Abs. 4 G10 soll die Nachkontrolle einer Übermittlung

---

[229] BT-Drs. 18/4654, S. 42.

[230] BT-Drs. 16/509, S. 10.

[231] Vgl. *Schindler*, Wirtschaftsschutz – Strategien und Herausforderungen für den Bundesnachrichtendienst, Rede des BND-Präsidenten anlässlich des 11. Symposiums des Bundesamtes für Verfassungsschutz am 8. Mai 2014, online abrufbar.

[232] *Huber*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, G 10, § 7a Rn. 15.

[233] *Roggan*, in: G-10-Gesetz, 2012, § 7a Rn. 4.

ermöglichen. Allerdings ist die Folge einer Verletzung nur dadurch zu ahnden, dass zukünftig kein Austausch mehr stattfindet.[234] Wegen der hohen Anforderungen und der Zustimmungsbedürftigkeit kann ohnehin nur eine Übermittlung im Einzelfall angezeigt sein. Da § 7a Abs. 1 S. 1 Nr. 1 G10 auch die erheblichen Sicherheitsinteressen ausländischer Staaten erfasst, kann eine Übermittlung vereinzelt aber auch geboten sein.

Eine Übermittlung der Daten des BND innerhalb der Struktur der europäischen NIS-Kooperation kommt nicht in Betracht, sofern das BSI die Daten über § 7 Abs. 4a G10 vom BND erlangt und die Erkenntnisse selbst über das BSI als zuständige Stelle für die grenzüberschreitende Zusammenarbeit in die NIS-Kooperation einfließen. Ausgeschlossen ist eine Übermittlung unter den Voraussetzungen des § 7a G10 jedoch nicht unter dem Aspekt, dass an der europäischen NIS-Kooperation keine polizeilichen Stellen direkt beteiligt sind. Als nachrichtendienstliche Plattform für einen Austausch kommt daher das EU INTCEN (EU-Intelligence and Situation Centre) infrage.[235]

c) Übermittlung der im Rahmen der Ausland-Ausland-Fernmeldeaufklärung gewonnenen Daten

Mit dem 2017 in Kraft getretenen §§ 13 bis 15 BNDG wird erstmals die Kooperation des Bundesnachrichtendienstes im Rahmen der Ausland-Ausland-Fernmeldeaufklärung mit ausländischen Stellen, die ebenfalls nachrichtendienstliche Aufgaben wahrnehmen, geregelt. Nach § 13 Abs. 1 BNDG dürfen im Rahmen der Kooperation Informationen einschließlich personenbezogener Daten nach § 14 erhoben und nach § 15 ausgetauscht werden. Eine solche Kooperation ist gemäß § 13 Abs. 2 BNDG zulässig, wenn sie den Zielen des § 6 Abs. 1 Nr. 1 bis 3 BNDG dient und die Erfüllung der Aufgaben durch den Bundesnachrichtendienst ohne eine solche Kooperation wesentlich erschwert oder unmöglich wäre. Da § 6 BNDG zur Erkennung von besonderen Cybergefahren dient, ist eine Informationskooperation zur Gewährleistung einer höheren Internetsicherheit auf Grundlage von § 13 Abs. 4 Nr. 7 BNDG denkbar.[236] Auf europäischer Ebene kommt auch hier das EU Intelligence and Situation Centre für eine Kooperation in Betracht.[237] Rechtlich neuartig und vorbildlich sind die Anforderungen an die schriftliche Fixierung einer solchen Kooperation.[238] Vor Beginn

---

[234] BT-Drs. 16/509, S. 11.

[235] Siehe § 3 B. I. 2.

[236] Das Erfordernis einer Kooperation zur erfolgreichen Aufklärung anerkennend BVerfG, NJW 2016, 1781 (1784, Rn. 102).

[237] Siehe § 3 B. I. 2.

[238] *Huber*, ZRP 2016, 162 (164).

der Kooperation sind Kooperationsziele und -inhalte, Kooperationsdauer, Zweckbindung und Löschpflichten in einer Absichtserklärung niederzulegen (§ 13 Abs. 3 BNDG). Wenn die Kooperation mit ausländischen öffentlichen Stellen von Mitgliedstaaten der EU erfolgt, bedarf es der Absichtserklärung des Bundeskanzleramtes.

Nach § 26 Abs. 1 BNDG kann der Bundenachrichtendienst zum Zwecke des Austausches und der gemeinsamen Auswertung von nachrichtendienstlichen Informationen und Erkenntnissen mit ausländischen öffentlichen Stellen gemeinsame Dateien führen (§ 27 BNDG) oder sich an diesen beteiligen (§ 27 BNDG). Die jeweilige Datei muss sich nach § 28 Abs. 1 S. 2 BNDG auf bestimmte Gefahrenlagen oder bestimmte Personenkreise beziehen, die nicht den in § 5 Abs. 1 S. 3 G10 benannten Gefahrenbereichen entsprechen müssen, sondern durchaus weiter gefasst sein dürfen.[239] Es sind aber auch Cybergefahren erfasst. Die näheren Voraussetzungen sind in § 26 und § 30 BNDG genannt.

3. Besondere Zweckbindung für die Meldedaten beim BSI

Informationssysteme haben die immanente Grundtendenz, mit anderen Datenbeständen verknüpft oder in andere Informationssysteme integriert zu werden – mit dem Ziel der Bildung einer Datenbank höherer Ordnung mit potenziell neuem Informationsgehalt für einen erweiterten Kreis von Akteuren mit neuen Verwendungskontexten.[240] Der datenschutzrechtliche Grundsatz der Zweckbindung soll diese Tendenz begrenzen. Eine Norm, die den allgemeinen Austausch personenbezogener Daten aller Sicherheitsbehörden und den Abbau jeglicher Informationsgrenzen zwischen den Behörden erstrebt, unterläuft das Bestimmtheitsgebot und den Grundsatz der Zweckbindung und wäre von vorneherein verfassungswidrig.[241]

Der Grundsatz der Zweckbindung gilt allerdings nicht absolut, es bestehen Abstufungen und Grenzen. Schon früh wurde darauf hingewiesen, dass der Inhalt der Zweckbindung nicht darin besteht, die Datenverarbeitung absolut an einen Zweck zu binden.[242] Eine Lockerung der Zweckbindung ist weder verfassungsrechtlich noch datenschutzrechtlich ausgeschlossen.[243] Die für bestimmte Zwecke erhobenen personenbezogenen Daten dürfen für andere als die ursprünglich festgelegten Zwecke verarbeitet werden, sofern diese nicht unverein-

---

[239] Kritisch *Huber*, ZRP 2016, 162 (165).

[240] *Schneider*, NVwZ 2012, 65 (66).

[241] BVerfGE 133, 277 = NJW 2013, 1499, Rn. 106.

[242] *Schneider*, NJW 1984, 390 (397).

[243] BVerfGE 120, 351 = NJW 2008, 2099 Rn. 82; *Härting*, NJW 2015, 3284 (3287); vgl. aber *Heckmann*, in: Taeger/Gabel (Hrsg.), BDSG, 2. Aufl. 2013, BDSG, § 14 Rn. 22.

bar sind. Das entscheidende Kriterium für eine Weiterverarbeitung ist nach Art. 6 Abs. 4 DS-GVO die Kompatibilität. Die ursprünglichen und die neuen Verarbeitungszwecke dürfen nicht unvereinbar und müssen kompatibel sein (vgl. Art. 5 Abs. 1 lit. b DS-GVO). Eine weitere Verarbeitung vorhandener Daten ist unter den in Art. 6 Abs. 4 DS-GVO aufgeführten Konstellationen statthaft. Neben der Einwilligung des Betroffenen als Grundlage für eine Weiterverarbeitung kommen eine Rechtsnorm der Union oder eines Mitgliedstaates, die einem der zehn in Art. 23 Abs. 1 DS-GVO genannten Ziele dient, in Betracht. Zu den genannten Zielen gehört die öffentliche Sicherheit.

Die Begrenzung der Übermittlung personenbezogener Daten ergibt sich somit aus der Zweckfestlegung nach Art. 5 lit. b DS-GVO. Für eine enge Zweckbindung bedarf es daher einer besonderen Regelung.

Eine solche spezialgesetzliche Zweckbindung stellt § 8b Abs. 7 BSIG dar.[244] Soweit im Rahmen von § 8b BSIG personenbezogene Daten erhoben, verarbeitet oder genutzt werden, „ist eine über die vorstehenden Absätze hinausgehende Verarbeitung und Nutzung zu anderen Zwecken unzulässig" (§ 8b Abs. 7 BSIG).

Sachlich bezieht sich die Zweckbindung vorrangig auf die Daten, die über die Meldepflichten von Betreibern kritischer Infrastrukturen generiert werden (§ 8b Abs. 4 BSIG), da eine weitere Form der Datenerhebung von der Vorschrift nicht vorgesehen ist. Darüber hinaus bewirkt die Zweckbindungsklausel die Begrenzung der Datenverarbeitung auf die in § 8b Abs. 2 BSIG beschriebenen Zwecke. Die Aufgaben sind allerdings denkbar weit gefasst (vgl. etwa in § 8b Abs. 2 Nr. 1 BSIG die Formulierung „die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik wesentlichen Informationen zu sammeln und auszuwerten"). Da § 8b Abs. 2 Nr. 4 BSIG die Unterrichtung der Betreiber kritischer Infrastrukturen und der zuständigen Aufsichtsbehörden regelt, umfasst die Zweckbindung nicht die Übermittlung personenbezogener Daten generell. Die Übermittlung als solche wird auch nicht über die Rechtsfolgenverweisung in § 8b Abs. 7 S. 2 BSIG verboten. Durch die Verweisung finden die Vorschriften zum Umgang mit Daten des Kernbereichs privater Lebensgestaltung nach § 5 Abs. 7 S. 3 bis 8 BSIG Anwendung. Insbesondere gilt damit das Beweisverwertungsverbot für Inhalte und Umstände der Kommunikation von Personen, denen nach § 53 Abs. 1 S. 1 StPO ein Zeugnisverweigerungsrecht zusteht. Ein allgemeines Verbot der Weitergabe folgt daraus nicht.[245]

Fraglich ist indes, ob die Zweckbindung die Übermittlung von Daten an europäische Stellen der NIS-Kooperation betrifft. Eine unzulässige, da „über die

---

[244] Vgl. auch § 88 Abs. 3 S. 3 TKG.

[245] Vgl. *Buchberger*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, BSIG, § 5 Rn. 41.

vorstehenden Absätze [des § 8b BSIG] hinausgehende Verarbeitung und Nutzung“ könnte im Falle der grenzüberschreitenden Übermittlung angenommen werden, weil der Wortlaut in § 8b Abs. 2 Nr. 4 b) und c) lediglich auf Behörden des Bundes und der Länder verweist. Der Austausch personenbezogener Daten zur Erfüllung der Pflicht, im Falle von Sicherheitsvorfällen etwaigig betroffene andere Mitgliedstaaten zu unterrichten und Daten zur möglichen Abhilfe zu übermitteln (vgl. Art. 14 Abs. 5 NIS-RL bzw. Art. 16 Abs. 6 NIS-RL), steht mit diesem Verständnis der Zweckbindung im Konflikt.

Eine Lesart der Vorschrift, die auf den eigentlichen Zweck der Datenverarbeitung abstellt, steht einer grenzüberschreitenden Übermittlung dagegen nicht grundsätzlich entgegen. Betont man die Zweckbindung so, dass es darauf ankommt, dass nur die „über die vorstehenden Absätze hinausgehende Verarbeitung […] zu *anderen* Zwecken“[246] unzulässig ist, hängt die Zulässigkeit der Übermittlung lediglich davon ab, dass die Daten beim Empfänger zu Zwecken verarbeitet werden, die mit denen in § 8b BSIG kongruent sind. Das BSI müsste dann im Falle einer Übermittlung sicherstellen, dass sie ausschließlich zur Abwehr von Gefahren für die Informationstechnik, zur Analyse der Auswirkungen eines Sicherheitsrisikos für die Verfügbarkeit der kritischen Infrastrukturen sowie zur Unterrichtung von Infrastrukturbetreibern, damit diese sich schützen können, verarbeitet und genutzt werden.

II. Grenzen des Informationstransfers durch den Schutz unternehmensbezogener Daten

Der Schutz vertraulicher, sensibler und sicherheitskritischer unternehmensbezogener Daten erfordert von den Behörden eine akribische Prüfung des Geheimnisschutzrechts, die sich auf den europäischen Informationsverkehr hemmend auswirken kann.

Im europäischen Verwaltungsverfahrensrecht fehlt es an einer ausdrücklichen Regelung des Geheimhaltungsanspruchs. Als ungeschriebener Grundsatz des europäischen Verwaltungsverfahrensrechts ist er gleichwohl anerkannt.[247] Der Schutz unternehmensbezogener Daten in europäischen Informationssystemen ist im Allgemeinen dennoch weit weniger ausdifferenziert als das Datenschutzrecht.[248] Die bestehenden Schutzstrukturen ähneln nicht den aus dem

---

[246] Hervorhebung des Verfassers.

[247] *Hermann*, in: Bader/Ronellenfitsch (Hrsg.), BeckOK VwVfG, 30. Ed. 2016, § 30 Rn. 2; EuGH, C-450/06, Rn. 46; vgl. auch Art. 339 AEUV und Art. 42 Abs. 2 2. Spiegelstrich GRCh.

[248] Der Entwurf der Kommission einer Richtlinie zum Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnis) vor rechtwidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, COM(2013) 813 final, zeigt, dass ein diffe-

Datenschutzrecht bekannten Regelungstechniken. Das Schutzregime zeichnet sich vielfach nur durch punktuelle Bestimmungen aus.[249]

Der § 30 VwVfG, der Verwaltungsgeheimnisse schützt, stimmt mit europäischem Recht überein und ist auch „in Ansehung von Europarecht voll anwendbar".[250]

Das deutsche Geheimnisschutzrecht legt unabhängig von der Frage, ob Geschäftsgeheimnisse grundrechtlich dem Grundrecht auf Eigentum oder dem Grundrecht auf Berufsfreiheit zuzuordnen sind,[251] nahe, dass Geheimnisse auch in bipolaren öffentlichen Informationsbeziehungen zu schützen sind. So darf die um Amtshilfe ersuchte Behörde eine Auskunft nach § 5 Abs. 2 S. 2 VwVfG verweigern, wenn die Information nach dem Gesetz oder ihrem Wesen nach geheim gehalten werden muss.[252] Der Offenbarungsbegriff im Verwaltungsgeheimnis (§ 30 VwVfG) legt diese Wertung ebenfalls nahe. Als Offenbarung kann die Mitteilung bzw. die Bekanntmachung des Geheimnisses an einen Dritten, der das Geheimnis zuvor nicht kannte, verstanden werden.[253] Von diesem Verständnis ausgehend liegt eine Mitteilung unabhängig davon vor, ob das Geheimnis mit einem Privaten oder einer öffentlichen Stelle ausgetauscht wurde.[254]

Das Offenbaren von Unternehmensgeheimnissen setzt demnach grundsätzlich eine Befugnis voraus, die Geheimhaltungspflicht ist nur dann verletzt, wenn das Geheimnis unbefugt offenbart wird. Die Befugnis kann aufgrund der Zustimmung des betroffenen Unternehmens gegeben sein, aus einer gesetzlichen Offenbarungsbefugnis oder aus dem Ergebnis einer Güterabwägung folgen,[255] nach dem zur Wahrung höherrangiger Rechtsgüter der Allgemeinheit oder Einzelner die Offenbarung erforderlich ist.[256]

---

renzierterer und harmonisierter Schutz unternehmensbezogener Daten angestrebt ist. Die im Entstehen begriffene Kohärenz bezieht sich aber auf Maßnahmen, Verfahren und Rechtsbehelfe, die für einen zivilrechtlichen Schutz erforderlich sind (vgl. Art. 5).

[249] *Heußner*, Informationssysteme im Europäischen Verwaltungsverbund, 2007, S. 341.

[250] *Kallerhoff*, in: Stelkens/Bonk/Sachs (Hrsg.), VwVfG, 8. Aufl. 2014, § 30 Rn. 30.

[251] Siehe § 3 E. III.

[252] Vgl. *Holznagel*, Informationsbeziehungen in und zwischen Behörden, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band II, 2. Aufl. 2012, § 24, Rn. 73; *Bullinger*, NJW 1978, 2173 (2178).

[253] *Herrmann*, in: Bader/Ronellenfitsch (Hrsg.), BeckOK VwVfG, 30. Ed. 2016, § 30 Rn. 12.

[254] *Ramsauer*, in: Kopp/ders., VwVfG, 17. Aufl. 2016, § 30 Rn. 10 f.; *Herrmann*, in: Bader/Ronellenfitsch (Hrsg.), BeckOK VwVfG, 30. Ed. 2016, § 30 Rn. 13.

[255] BVerwG, DVBl. 1992, 298 (300).

[256] *David*, Inspektionen als Instrument der Vollzugskontrolle im Europäischen Verwaltungsverbund, in: Schmidt-Aßmann/Schöndorf-Haubold (Hrsg.), Der Europäische Verwaltungsverbund, 2005, S. 237 ff.; *Wettner*, Die Amtshilfe im Europäischen Verwaltungsrecht, 2005, S. 329; *Heußner*, Informationssysteme im Europäischen Verwaltungsverbund, 2007, S. 324.

Zu untersuchen ist daher, welche abwägungsleitenden Anforderungen die für den Informationsaustauch maßgebliche NIS-RL für den Vertraulichkeitsschutz vorgibt (1.) und ob besondere Schutzvorkehrungen auf nationaler Ebene den Informationsverkehr hemmen können (2.).

1. Anforderungen an den Austausch vertraulicher Informationen

Eine generalklauselartige Vertraulichkeitsregelung stellt Art. 1 Abs. 5 NIS-RL dar. Die Vorschrift beantwortet die Frage, unter welchen Voraussetzungen vertrauliche Informationen mit der Kommission und den zuständigen NIS-Behörden ausgetauscht werden dürfen. Die Voraussetzungen des Vertraulichkeitsschutzes benennt die Norm nicht. Sie verweist dafür auf Vorschriften der Union und der Mitgliedstaaten, ohne diese zumindest für die Union näher zu benennen. Durch diese Regelungstechnik bleibt es den Mitgliedstaaten überlassen, zu bestimmen, wann eine Information auf welchem Schutzniveau vertraulich zu behandeln ist. Das Schutzniveau kann dadurch insgesamt nicht unerheblich variieren. Eine solche Regelungstechnik muss die Kooperationseffizienz jedoch nicht notwendig begrenzen, wenn Unstimmigkeiten unter den Mitgliedstaaten über den Vertraulichkeitsmaßstab begrenzt bleiben.[257] Eine gewisse Kohärenz im Schutzniveau wird dadurch gesichert, dass kumulativ die Information nach Vorschriften des Unionsrechts als vertraulich geschützt sein muss („und").

Aus Art. 1 Abs. 5 S. 1 NIS-RL ergibt sich, dass die Erforderlichkeit das maßgebliche Kriterium der Abwägung ist. Vertrauliche Informationen werden mit der Kommission und den mitgliedstaatlichen NIS-Behörden „nur ausgetauscht, wenn dieser Austausch für die Anwendung dieser Richtlinie erforderlich ist. Die auszutauschenden Informationen werden auf das beschränkt, was für das verfolgte Ziel relevant und angemessen ist."

Die in dieser Regelungstechnik liegende Anforderung führt regelmäßig zu einem strikteren Informationsaustausch. Im Rahmen mitgliedstaatlicher Informationshilfe führt das Tatbestandsmerkmal „erforderlich" zunächst dazu, dass aus Sicht des um eine Auskunft ersuchenden Mitgliedstaats eine ernstliche Möglichkeit bestehen muss, dass der andere Mitgliedstaat im Besitz der Kenntnis ist. Der Blick auf die Auslegung dieses Kriteriums im steuerrechtlichen Informationsaustausch zeigt, dass zusätzliche Anforderungen abgeleitet werden können. Erforderlich ist dort ein Auskunftsersuchen erst dann, wenn die Information vom ersuchenden Staat auch nach Ausschöpfung aller eigener Auskunftsquellen nicht erreichbar ist. Die Auskunftserteilung ist nicht schon dann legitimiert, wenn das entsprechende Ersuchen aus Sicht des ersuchenden Staa-

[257] *Hombergs*, Europäisches Verwaltungskooperationsrecht auf dem Sektor der elektronischen Kommunikation, 2006, S. 265.

tes effektiver oder einfacher ist als innerstaatliche Mittel.[258] Ein Austausch von Informationen auf Grund von Anfragen „ins Blaue hinein" bzw. durch „fishing expeditions" scheidet regelmäßig aus.[259]

Daneben hat der Umfang der ausgetauschten Informationen für das verfolgte Ziel relevant und angemessen zu sein. Der Austausch von Unternehmensgeheimnissen wird damit unter die Zielvorgabe der Datenvermeidung und der Sparsamkeit gestellt.

Das CSIRTs-Netzwerk ist bereits im Ausgangspunkt darauf angelegt, schonend mit vertraulichen Informationen umzugehen. Der Informationsaustausch über Sicherheitsvorfälle bezweckt nur den Austausch von „wirtschaftlich nicht sensiblen" bzw. „nicht vertraulichen" Informationen (Art. 12 Abs. 3 lit. b und c NIS-RL). Die Schwelle der Erforderlichkeit eines Austausches schutzbedürftiger Informationen besteht für die antragsbasierte Informationshilfe nicht. Der antragsgebundene Austausch vertraulicher, sicherheitskritischer bzw. wirtschaftlich vorteilhafter Informationen wird von vorneherein unterbunden.

Die jährlichen Berichte über Meldepflichten sollen die Vertraulichkeit der Meldungen und Infrastrukturbetreiber wie Diensteanbieter wahren, indem diese möglichst zu anonymisieren sind.[260] Letztlich liegt im so vorgesehen Vertraulichkeitsschutz und Identitätsschutz ein Anreizmechanismus für die Unternehmen, die Meldepflicht tatsächlich zu erfüllen. Sie müssen nicht befürchten, Gegenstand einer Fallbesprechung zu sein.

Eine Skalierung des Schutzes von Unternehmensgeheimnissen besteht für Sicherheitslücken. Neben der Stufe der einfachen Vertraulichkeit besteht die der strengen Vertraulichkeit. Streng vertraulich zu behandeln sind insbesondere die über die Meldepflicht gemeldeten Informationen, wenn sie die Anfälligkeit von Produkten betreffen und Abhilfen gegen Sicherheitsschwachstellen noch nicht

---

[258] Vgl. zum Informationsaustausch im Steuerrecht *Schaumburg*, IStR, 3. Aufl., Rn. 19.97.

[259] Siehe FG Köln, Beschl. v. 7.9.2015 – 2 V 1375/15, IStR 2015, 835 (m. Anm. *Scholz*), Rn. 79 ff. Das Gericht hatte den weitreichenden Austausch von Steuerdaten durch das Bundeszentralamt für Steuern zur Bekämpfung des sog. „Base-Erosion and Profit Shifting" (BEPS) untersagt, weil der Informationsaustausch gegen das Steuergeheimnis aus § 30 AO verstoße. Der internationale Informationsaustausch zielte nicht auf die konkrete Besteuerung eines Unternehmens, sondern auf das Aufdecken von Besteuerungslücken und auf die Klärung der Frage, worin die gesetzlichen Ursachen der niedrigen effektiven Steuerbelastung bestünden, um durch Gesetzesänderungen Abhilfe schaffen zu können. Der Informationsaustausch war auch nicht im Wege der Amtshilfe nach § 30 Abs. 4 Nr. 2 AO und nicht aus § 117 Abs. 2 AO in Verbindung mit dem EU-Amtshilfegesetz rechtmäßig. Das Tatbestandsmerkmal der „voraussichtlichen Erheblichkeit" solle zwar einen größtmöglichen Informationsaustausch ermöglichen. Nicht gestattet seien aber Beweisausforschungen („Fishing Expeditions").

[260] Erwägungsgrund 32 NIS-RL.

veröffentlich sind.[261] Diese Vorgabe, die formell keine Bindungswirkung hat, betrifft sowohl das Verfahren des Informationsaustausches als auch die nach außen gerichtete Informationsdistribution.[262]

2. Besondere Begrenzungen

Die Zulässigkeit des Austauschs vertraulicher und sensibler Informationen ist grundsätzlich davon abhängig, ob der Austausch für die Anwendung der NIS-RL erforderlich ist. Besondere Begrenzungen ergeben sich für die ENISA (a) und die deutschen NIS-Behörden (b).

a) Begrenzungen der ENISA und allgemeine unionsrechtliche Geheimhaltungspflicht

Eine spezielle Vertraulichkeitsregelung besteht für die ENISA. Die Agentur gibt die eingehenden und verarbeiteten Informationen nicht an Dritte weiter, wenn sie auf begründetes Ersuchen ganz oder teilweise als vertraulich behandelt werden sollen (Art. 17 Abs. 1 VO [EU] Nr. 526/2013). Die Weitergabe ist durch das Erfordernis eines qualifizierten Ersuchens folglich nicht schon im Ausgangsmodus beschränkt. Die Vertraulichkeitsregelung betrifft aber auch die Weitergabe im Rahmen der NIS-Kooperation und nicht etwa nur die Weitergabe auf Informationsanfrage seitens der Öffentlichkeit. Als Dritte können alle Personen oder Stellen außerhalb der ENISA angesehen werden, also auch die CSIRTs, das CSIRTs-Netzwerk oder die Kooperationsgruppe.

Für Mitglieder der ENISA – wie im Übrigen für alle Beamte und Bedienstete der Union – gilt außerdem die personelle Geheimhaltungspflicht nach Beendigung der Amtstätigkeit, die primärrechtlich in Art. 339 AEUV verankert ist. Kenntnisse, die „ihrem Wesen nach" unter das Berufsgeheimnis fallen, dürfen nicht preisgegeben werden. Ausdrücklich sind auch Kenntnisse über Unternehmen und deren Geschäftsbeziehungen genannt. Da Art. 339 AEUV grundsätzlich alle Mitglieder der Organe der Union zur Geheimhaltung verpflichtet, ist die Überlegung nicht abwegig, die Weitergabe geschützter Informationen sowohl innerhalb als auch zwischen Organen der Union auf Art. 339 AEUV zu stützen. Denn um die Funktionsfähigkeit eines Organs oder einer Einrichtung zu wahren (*effet utile*), muss die Weitergabe einer geschützten Information mindestens insoweit zulässig sein, als ein anderes Organ oder eine andere Einrichtung, d. h. die empfangende Stelle, für die Verarbeitung der Information zuständig ist und die Kenntnis des Geheimnisses erforderlich ist. Dagegen lässt sich

---

[261] Erwägungsgrund 59 NIS-RL.

[262] Dazu § 5.

aus der allgemeinen Verschwiegenheitspflicht der Organbediensteten aber weder eine Erlaubnis noch ein Recht auf Mitteilung eines Geheimnisses herleiten.[263] Ohne eine bestimmte Offenbarungsbefugnis ist die Weitergabe an nicht zuständige Stellen oder andere Organe der Union im Grundsatz unzulässig.

b) Begrenzungen der deutschen NIS-Behörden

Hinsichtlich der Weitergabe von gewonnenen Informationen aus Untersuchungen von sicherheitsrelevanten Produkten und Systemen besteht eine besondere Begrenzung, die den europäischen Austausch betrifft (aa). Im Übrigen zeichnet sich der Vertraulichkeitsschutz durch eine geringe Regelungsdichte aus, die zu Unsicherheit führt und den Informationsverkehr hemmt (bb).

aa) Weitergabe von Erkenntnissen aus Produkt- und Systemuntersuchungen an europäische NIS-Stellen

Eine spezifische Begrenzung der Weitergabe besteht für die Erkenntnisse aus der Untersuchung von informationstechnischen Produkten und Systemen, die das BSI nach § 7a BSIG vornehmen darf.[264] Erkenntnisse sind keine personenbezogenen Daten[265] und umfassen sicherheitsrelevante Produkt- und Systeminformationen. Erfasst sind vom Begriff der Erkenntnis festgestellte Sicherheitslücken, mithin vertrauliche Unternehmensinformationen.

Dem Wortlaut nach darf das Bundesamt seine Erkenntnisse „weitergeben und veröffentlichen". Die Weitergabe unterliegt dennoch einer nicht datenschutzrechtlichen Zweckbindung. Zulässig ist die Weitergabe durch diesen Verweis („soweit dies zur Erfüllung dieser Aufgaben erforderlich ist") nur für einen definierten Aufgabenbereich.[266] Die Verweisung auf § 7a Abs. 2 S. 1 in Verbindung mit § 3 Abs. 1 S. 2 Nr. 1, 14 und 17 BSIG betrifft dabei gerade nicht die Aufgabe der Zusammenarbeit mit den zuständigen europäischen Stellen (vgl. § 3 Abs. 1 S. 2 Nr. 16 BSIG). Auch der Verweis auf die allgemeinste Aufgabe (Nr. 1), die Abwehr von Gefahren für die Sicherheit der Informationstechnik, betrifft nur die Informationstechnik „des Bundes". Im Umkehrschluss aus der

---

[263] *Brühann*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Europäisches Unionsrecht, Band 4, 7. Aufl. 2015, AEUV, Art. 339 Rn. 19; die Zulässigkeit der Weitergabe davon abhängig machend, ob die Geheimhaltung erkennbar ist, *Kotzur,* in: Grabitz/Hilf/Nettesheimer (Hrsg.), AEUV/EUV, 57. Aufl. 2015, Art. 287 Rn. 33.

[264] Siehe § 3 D. II. 1.

[265] Vgl. BT-Drs. 18/4096, S. 41.

[266] *Eckhardt*, ZD 2014, 599 (603), mit der Bemerkung, dass die Praxis allerdings zeige, dass eine Zweckbestimmung einmal vorhandener Daten und Informationen nicht lange Begehrlichkeiten bezüglich der Verwendung zu anderen Zwecken standhält.

Aufgabenkopplung ergibt sich, dass die Weitergabe der Erkenntnisse an europäische Stellen gerade nicht intendiert ist.

Für die europäische NIS-Informationskooperation stellt diese Weitergabebegrenzung eine nicht zu unterschätzende Begrenzung dar. Die Weitergabe einer Information über Sicherheitslücken in einem IT-Produkt oder -system kann unmittelbar zur europäischen Sicherheitsgewährleistung beitragen, da diese Produkte häufig global bzw. im europäischen Binnenmarkt im Verkehr sind.[267] Das Weitergabeverbot perpetuiert insofern europäische Informationsasymmetrien, die abzuschaffen Zweck der NIS-RL ist, um so das Funktionieren des Binnenmarkts zu verbessern (Art. 1 Abs. 1 NIS-RL). Beheben lässt sich die Asymmetrie zum Teil durch die Befugnis des BSI, die Erkenntnis zu veröffentlichen. Die Erkenntnis könnte so an das europäische Publikum und damit an die NIS-Stellen weitergetragen werden.[268]

bb) Geringe Regelungsdichte zur Weitergabe vertraulicher Informationen durch die NIS-Behörden

Befugnisse zur Weitergabe von Betriebs- und Geschäftsgeheimnissen sind für das BSI nicht positiv gesetzlich geregelt. Eine besondere Bestimmung ist auch nicht in den telekommunikationsrechtlichen Vorschriften zur Sicherheit vorgesehen (§§ 108 ff. TKG). Das ist umso verwunderlicher, als die telekommunikationsrechtlichen Meldungen an die Bundesnetzagentur im Gegensatz zu denen an das BSI stets die Offenbarung der Unternehmensidentität bedingen und daher tendenziell eher wirtschaftlich sensible Informationen bei der Bundesnetzagentur vorliegen.

Als Grundlage denkbar für den Austausch vertraulicher Informationen erscheint ein Rückgriff auf § 123b TKG. Die Norm erlaubt der Bundesnetzagentur die Offenbarung von vertraulichen Informationen an die Kommission und die Regulierungsbehörden anderer Mitgliedstaaten.[269] Aus dem systematischen Zusammenhang mit § 123a TKG, der allgemein die Zusammenarbeit der Bundesnetzagentur im Mehrebensystem betrifft, ergibt sich, dass vor allem die Informationskooperation im telekommunikationsrechtlichen Regulierungsverbund ermöglicht werden soll.[270] Die Norm wurde in formeller Hinsicht erst durch die

---

[267] Gegen eine Weitergabe von Informationen im Rahmen der Zusammenarbeit mit anderen Behörden *Hornung*, NJW 2015, 3334 (3338), der wegen der Sensibilität der Informationen auf die Gefahr der Industriespionage verweist.

[268] Siehe § 5 B. I. 3.

[269] BT-Drs. 17/5707, S. 85; *Schönau*, in: Geppert/Schütz (Hrsg.), BeckTKG, 4. Aufl. 2013, § 123a Rn. 8.

[270] Zum Hintergrund der spannungsgeladenen Kooperation *Schönau*, in: Geppert/Schütz (Hrsg.), BeckTKG, 4. Aufl. 2013, § 123a Rn. 1; vgl. auch *Kurth*, MMR 2009, 818 (818 ff.), der

Schaffung des Gremiums Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) notwendig.[271] Dass weder die Rollenbeschreibung noch die Aufgabenzuweisung des GEREK auf eine Funktion in der Gewährleistung der Sicherheit von Netzen und Informationssystemen hinweisen,[272] spricht dagegen, § 123b TKG als Grundlage in der europäischen NIS-Kooperation heranzuziehen. Allerdings muss § 123b TKG ausgehend vom Wortlaut nicht notwendig im Zusammenhang mit der GEREK gelesen werden. Wenn § 123b Abs. 2 TKG der Bundesnetzagentur erlaubt, ihr übermittelte Informationen der nationalen Regulierungsbehörde eines anderen Mitgliedstaats zur Verfügung zu stellen, „damit diese […] ihre Verpflichtungen aus dem Recht der Europäischen Union erfüllen kann", dann betrifft die Befugnis grundsätzlich auch Informationen zur Sicherheit von Telekommunikationsinfrastrukturen. Art. 8 Abs. 4 lit. f RL 2009/140/EG weist die Sicherstellung der Gewährleistung der Integrität und Sicherheit der öffentlichen Kommunikationsnetze als politisches Ziel und regulatorischen Grundsatz den nationalen Regulierungsbehörden zu. Aus den sicherheitsbezogenen Vorschriften in Art. 13a und 13b RL 2009/140/EG ergeben sich Pflichten für die Regulierungsbehörden, insbesondere zur Durchsetzung der Sicherheitspflichten. Demzufolge kann die Bundesnetzagentur vertrauliche Informationen mit Behörden anderer Mitgliedstaaten austauschen. Der mögliche Anwendungsbereich ist jedoch gering, da die Befugnis für das BSI oder die CSIRTs gerade nicht gilt. Überdies setzt der Informationsaustausch auch auf Grundlage von § 123b TKG einen begründeten Antrag voraus. Das strukturelle Problem bei den zuständigen Behörden ist aber gerade die Unkenntnis, sodass regelmäßig weder Anlass für einen Antrag besteht noch dieser begründet werden kann.

Ein vergleichender Blick auf andere Informationsaustauschregime im europäischen Kartellrecht macht deutlich, dass sich das europäische NIS-Recht durch eine verhältnismäßig geringe Regelungsdichte hinsichtlich des Vertrau-

---

Meinungsverschiedenheiten am exemplarischen Vertragsverletzungsverfahren der Kommission gegen die Bundesrepublik Deutschland wegen Verstoßes gegen Notifizierungspflichten erörtert.

[271] Etablierung des GEREK im Januar 2010 durch die unmittelbar anwendbare VO (EG) Nr. 1211/2009 vom 25.11.2009, ABl. EU Nr. L 337 v. 18.12.2009, S. 1, zur Errichtung des neuen Gremiums Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) und des Büros.

[272] Art. 2 und 3 VO (EG) Nr. 1211/2009. Vor der Schaffung des GEREK hatte die Kommission zunächst weitergehende Pläne und schlug vor, eine *European Electronic Communications Authority* (*EECMA*) zu schaffen. Diese sollte über aufsichtsrechtliche, organisatorische und gestalterische Kompetenzen verfügen und eine Aufsichtsrolle in der Netz- und Informationssicherheit wahrnehmen. Der Vorschlag konnte sich nicht durchsetzen und so ist die GEREK-VO eine Kompromisslösung. Siehe *Attendorn*, CR 2011, 721 (722 m. w. N.).

lichkeits- und Geheimnisschutzes auszeichnet. Die Zusammenarbeit der europäischen Kartellbehörden im European Competition Network verfolgt Zwecke, die auch denen der NIS-Kooperation entsprechen. Der Informationsaustausch soll die beschränkten Ermittlungsmöglichkeiten der nationalen Kartellbehörden, die sich vor allem aus der territorialen Begrenzung der jeweiligen nationalen Zuständigkeit ergeben, kompensieren.[273] Der Netzwerk der Kartellbehörden dient als wichtige Erkenntnisquelle im dezentralen Vollzug des Kartellrechts im Mehrebenengeflecht der Union.[274] Der bedeutenden Problematik des Schutzes von Betriebs- und Geschäftsgeheimnissen trägt bereits auf Ebene des Sekundärrechts Art. 12 VO 1/2003 Rechnung. Diese Vorgabe konkretisiert § 50a GWB und stellt die Befugnis zum umfassenden Austausch rechtlicher und tatsächlicher Informationen dar.[275] Positiv geregelt sind dabei nicht nur die allgemeine Befugnis und der Umfang des Informationsaustausches, sondern auch gegenstandsbezogene Verwertungsbeschränkungen und solche zum Schutz von Verteidigungsrechten. So ist die Verwertung der Informationen gegenstandsbezogen an die Anwendung von Art. 101 und 102 AEUV gebunden. Gleichzeitig haben die Kommission und die nationalen Behörden einen Katalog von Verwertungsbeschränkungen bei der Verhängung von Sanktionen zu beachten.[276] Art. 28 Abs. 2 VO 1/2003 statuiert ein Weitergabeverbot und betrifft unmittelbar alle Behörden und alle im Netzwerk ausgetauschten Informationen. Die Vorschrift gewährleistet den Außenschutz von Berufs- und Geschäftsgeheimnissen im Netzwerk. Aufgrund des Vorrangs des Unionsrechts geht das Weitergabeverbot nationalen Regelungen in Bezug auf ausgetauschte Dokumente vor.

Beide Regelungsarrangements, das telekommunikationsrechtliche wie das kartellrechtliche, weisen eine höhere Dichte an Regelungen zum Vertraulichkeitsschutz auf. Im NIS-Bereich ist das Schutzniveau weitgehend von den Regulierungsansätzen und Verständnissen von vertraulichen Informationen abhängig. Unterschiede kann es in den Mitgliedstaaten insbesondere bei der Frage geben, ob besondere Sicherheitsschwachstellen als zu schützendes Unternehmensgeheimnis zu bewerten sind. Solange ein harmonisiertes Verständnis unionsrechtlich nicht vorgezeichnet wird und solange keine den aufgeführten Refe-

---

[273] Vgl. Ausführung in BGH, NJW 2004, 3711 (3714).

[274] *Kment*, Grenzüberschreitendes Verwaltungshandeln, 2010, S. 291; *Gussone*/*Michalczyk*, EuZW 2011, 130 (130 ff.); Erwägungsgrund 16 VO (EG) Nr. 1/2003.

[275] *Rehbinder*, in: Immenga/Mestmäcker, GWB, 5. Aufl. 2014, § 50a Rn. 7; vgl. für Art. 12 VO (EG) 1/2003 *Vollrath*, in: von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht, Band 4, 7. Aufl. 2015, VO (EG) 1/2003, Art. 12, Rn. 6.

[276] Verfassungsrechtlich begründete Verwertungsverbote sind nach § 50a Abs. 3 S. 2 GWB zu beachten. Informationen, die in einem ausländischen Verfahren erhoben wurden, können im Bußgeldverfahren verwertet werden. Art. 12 VO (EG) Nr. 1/2003 geht von einem in der EU vergleichbaren Schutzniveau aus, Erwägungsgrund 16 der VO.

renzgebieten entsprechend differenzierten, nationalen Befugnisse vorgegeben sind, ist der Austausch mit Unsicherheit behaftet. Diese Unsicherheit hat eine begrenzende Wirkung auf den Informationsaustausch.[277] Eine Zustimmung des Betroffenen mag im Einzelfall vorliegen. Regelmäßig haben Unternehmen jedoch keinen intrinsischen Anreiz, Geheimnisse, zumal transnational, zu teilen. Auf einzelfallabhängigen Abwägungsentscheidungen kann perspektivisch kein europäisches NIS-Informationsaustauschsystem beruhen, das operabel sein möchte.

III. Grenzen des Informationstransfers durch Organisationsrecht

Begrenzungen für den Informationsaustausch im Bereich der Netz- und Informationssicherheit können sich des Weiteren aus dem Organisationrecht ergeben. Die Verdichtung der informationellen Zusammenarbeit in Fusionszentren wie dem Nationalen Cyber-Abwehrzentrum wirft die Frage nach der Vereinbarkeit mit dem sicherheitsbehördlichen Trennungsgebot auf (1.). Die fehlende organisationrechtliche Unabhängigkeit der NIS-Behörde lässt den Vorbehalt anmelden, informationelle Entscheidungen über die Weitergabe von Informationen fielen zulasten der Netz- und Informationssicherheit aus (2.).

1. Trennungsgebot und Informationsaustausch im Nationalen Cyber-Abwehrzentrum

Die Kooperation verschiedener Sicherheitsbehörden im Nationalen Cyber-Abwehrzentrum (NCAZ) ruft Bedenken hinsichtlich der Vereinbarkeit mit dem sicherheitsbehördlichen Trennungsgebot hervor.[278]

Das NCAZ steht in der Sicherheitsgewährleistung für eine konzeptionell neue Form der Zusammenarbeit in Gestalt eines informellen und informationellen Netzwerks. Die Einrichtung des NCAZ bettet sich ein in eine Entwicklung des Ausbaus der Sicherheitsarchitektur im Zuge der intensivierten Bekämpfung des internationalen Terrorismus und der organisierten Kriminalität. Es zeichnet sich eine allgemeine Tendenz zur Zentralisierung in der Aufgabenwahrneh-

---

[277] Im Zusammenhang mit der Einführung des Cybersecurity-Information-Sharing-Systems in den USA *Nolan*, Cybersecurity and Information Sharing: Legal Challenges and Solutions, Congressional Research Service, 2015, S. 36.

[278] Siehe zum NCAZ § 3 B. II. 5; zur Vereinbarkeit mit dem institutionellen Gesetzesvorbehalt *Linke*, DÖV 2015, 128 (132 f.); vgl. zum Gemeinsamen Terrorismusabwehrzentraum (GTAZ), *Weisser*, NVwZ 2011, 142 (144); *Schoch*, Polizei- und Ordnungsrecht, in: ders. (Hrsg.), Besonderes Verwaltungsrecht, 15. Aufl. 2013, Kap. 2, Rn. 52; *Rathgeber*, DVBl. 2013, 1009 (1016); allgemeiner *Bäcker/Giesler/Harms/Hirsch/Kaller/Wolff*, Bericht der Regierungskommission zur Überprüfung der Sicherheitsgesetzgebung in Deutschland, 2013, S. 174 ff.

mung und eine Verlagerung der Aufgaben und Eingriffsbefugnisse weiter in das Vorfeld der Gefahrenabwehr ab.[279]

Das NCAZ verdichtet die informationelle Zusammenarbeit. Am NCAZ sind sowohl Polizeibehörden (Bundeskriminalamt) als auch Nachrichtendienste (Bundesamt für Verfassungsschutz und Bundesnachrichtendienst), darunter aus dem militärischen Bereich der Militärischer Abschirmdienst, beteiligt. Mit dem IT-Sicherheitsgesetz wurde die Rolle des NCAZ indirekt aufgewertet, da das BSI und das Bundeskriminalamt erweiterte Kompetenzen hinsichtlich der Informationsgenerierung zugewiesen bekommen haben und so mehr Informationen im NCAZ einbringen können. Das so ausgestaltete NCAZ könnte gegen das Trennungsprinzip insbesondere in informationeller Hinsicht verstoßen.

a) Sicherheitsbehördliches Trennungsgebot

Das Trennungsgebot in der sicherheitsbehördlichen Datenverarbeitung findet seine historische Erklärung in der Rolle der Sicherheitsdienste vor der Bildung der Bundesrepublik Deutschland. Während der nationalsozialistischen Gewalt- und Willkürherrschaft hatte die „Geheime Staatspolizei" (Gestapo) sowohl polizeiliche also auch nachrichtendienstliche Befugnisse. Diese doppelte Befugnis erwies sich als besonders fatal, da so die Gestapo politische Gegner systematisch überwachen und verfolgen konnte.[280] Die alliierten Vereinigten Staaten von Amerika, Großbritannien und Frankreich setzten in der Folge durch, Polizei und Nachrichtendienste sowohl in ihrer Funktion als auch in ihren Befugnissen zu trennen.[281]

Das Trennungsgebot findet im Gesetz eine organisatorische, aufgabenbezogene und eine befugnisbezogene Ausprägung. Das einfachgesetzliche Trennungsgebot steht dem NCAZ nicht entgegen.

In organisatorischer Hinsicht ist eine personelle Verflechtung grundsätzlich unzulässig. Das Trennungsgebot sieht einfachgesetzlich in den Errichtungsgesetzen für die Nachrichtendienste vor, dass diese keiner „polizeilichen Dienststelle […] angegliedert werden" (§ 2 Abs. 1 S. 2 BVerfSchG, § 1 Abs. 1 S. 2 BNDG, § 1 Abs. 4 MADG). Das NCAZ verletzt diese Vorgaben nicht. Das Bundeskriminalamt ist lediglich lose durch Verbindungsbeamten assoziiert. Keiner der Beamten verfügt über eine Doppelzuständigkeit, ein Subordinationsverhältnis wird nicht hergestellt. Im Übrigen fehlt dem NCAZ schon die Behördenqua-

---

279 *Roggan*, NJW 2009, 257 (262); *Dombert/Räuker*, DÖV 2014, 414 (420).

280 *Petri*, Sicherheitsbehördliche Datenverarbeitung, in: Schmidt/Weichert (Hrsg.), Datenschutz, 2010, S. 125 (Fn. 2).

281 *Petri*, Sicherheitsbehördliche Datenverarbeitung, in: Schmidt/Weichert (Hrsg.), Datenschutz, 2010, S. 115.

lität. Weder verfügt es über eine organisatorische Eigenständigkeit, da es beim BSI angesiedelt ist, noch verfolgt es eine nach außen gerichtete Verwaltungstätigkeit. Sofern im interbehördlichen Datenaustausch Grundrechte von Grundrechtsberechtigten berührt werden, so ist jedenfalls nicht das NCAZ selbst übermittelnde oder empfangende Stelle.[282]

Unvereinbar mit dem Trennungsprinzip wäre ferner eine Aufgabenvermischung im NCAZ. Die Aufgaben der Behörden sind grundsätzlich zu trennen. Aufgaben der Gefahrenabwehr und der Strafverfolgung sind von der nachrichtendienstlichen Vorfeldaufklärung zu separieren.[283] Soweit im NCAZ ein Austausch über den eigenen Aufgabenkreis betreffende Fragen und Sachverhalte stattfindet, liegt darin keine rechtswidrige Ausdehnung der Aufgabenzuweisungen. Die Schwelle wäre wohl dann übertreten, wenn die beteiligten Polizeibehörden nicht mehr nur für die Gefahrenabwehr und Strafverfolgung zuständig wären, sondern auch für Aufgaben im nachrichtendienstlichen, vorfeldbezogenen Aufgabenspektrum und so die Zusammenarbeit über den koordinativ-kooperativen Informationsaustausch hinausginge. In der Behördenkooperation liegt auch kein gegen Art. 35 Abs. 1 GG verstoßendes Zusammenwirken. Eine verstetigte Amtshilfe kann problematisch sein, wenn Zuständigkeiten und Kompetenzen nicht nur situativ und punktuell überbrückt, sondern dauerhaft umgangen werden.[284] Im NCAZ verbleibt aber jede Behörde im eigenen Zuständigkeitsbereich, die Kooperation findet in eigenen Angelegenheiten statt. Dagegen hat Amtshilfe einen altruistischen Charakter.[285]

Grundlegendste Ausprägung des Trennungsgebots ist die befugnisbezogene Trennung. Nachrichtendienste dürfen gemäß § 8 Abs. 3 BVerfSchG, § 2 Abs. 3 BNDG und § 4 Abs. 2 MADG weder über polizeiliche Befugnisse, über kompensatorische Amtshilfeansprüche noch über Weisungsrechte verfügen. Jedenfalls sollen den Nachrichtendiensten damit nicht die Befugnisse einer Exekutivbehörde zustehen[286] bzw. sie dürfen keine polizeilichen Zwangsbefugnisse aufweisen und mithin keine Vernehmungen, Durchsuchungen oder Beschlagnahmen durchführen oder anderen Zwang ausüben.[287] Demgegenüber haben Polizei- und Strafverfolgungsbehörden Vollzugsbefugnisse, weil sie grundsätzlich dem

---

[282] Vgl. *Weisser*, NVwZ 2011, 142 (145).

[283] BVerfGE 133, 277 (325 ff.).

[284] Vgl. BVerfGE 63, 1 (32); BVerfG, NVwZ 2011, 1254 (1255); *Pieroth*, in: Jarass/Pieroth (Hrsg.), GG, 13. Aufl. 2014, Art. 35 Rn. 4.

[285] Im Ergebnis auch *Linke*, DÖV 2015, 128 (135); *Müller-Terpitz*, Sicherheit im E-Government, in: Borges/Schwenk (Hrsg.), Daten- und Identitätsschutz in Cloud Computing, E-Government und E-Commerce, 2012, S. 169 (179).

[286] Zum BVerfSchG BT-Drs. 1/924, S. 3 f.

[287] BVerfG, NJW 2011, 2417 (2420).

Bürger mit „offenem Visier" gegenübertreten. Eine Geheimpolizei ist nicht vorgesehen.[288]

Es ist nicht ersichtlich, dass dem NCAZ als Einrichtung Befugnisse übertragen werden, die dem Trennungsprinzip widersprächen. Im NCAZ werden den Nachrichtendiensten weder Zwangsbefugnisse übertragen noch wird den Fach- und Polizeibehörden Zugriff auf nachrichtendienstliche Befugnisse gewährt.[289] Eine Weisungsbefugnis des koordinierenden Cybersicherheitsrates gegenüber dem NCAZ wäre schon aufgrund der fehlenden Behördeneigenschaft nicht möglich.[290] Vor diesem Hintergrund besteht zwar ein Spannungsverhältnis zwischen dem Bedürfnis nach Informationsaustausch und Vernetzung der Sicherheitsbehörden und dem Trennungsgebot. Die konkrete Verwaltungskooperation im NCAZ verstößt jedoch nicht gegen die befugnisrechtliche Ausformung des Trennungsgebots.[291]

b) Reichweite des informationellen Trennungsprinzips

Gegen den Informationsaustausch im NCAZ könnte das Bestehen eines informationellen Trennungsgebots angeführt werden. Demzufolge müssten auch die jeweils generierten Informationen getrennt bleiben. Eine einfachgesetzliche Ausgestaltung eines solchen Gebots besteht nicht. Vielmehr erlauben die fachgesetzlichen Übermittlungsvorschriften wie § 20 Abs. 1 S. 2 BVerfSchG, § 9 Abs. 3 BNDG und § 11 Abs. 2 MADG den Nachrichtendiensten, im Vorfeld gesammelte Erkenntnisse über erhebliche Gefahren mit den Polizeien zu teilen. Der zulässige Informationsaustausch vermeidet sinnwidrige Situationen. Es wäre absurd, wenn die Nachrichtendienste (spontan) Erkenntnisse über konkrete, schwerwiegende Gefahren hätten, die sie nicht an Polizeien und Strafverfolgungsbehörden weitergeben dürften.[292] Ein striktes informationelles Trennungsgebot kann es nicht geben. Sinnvoll erscheint es dagegen, das Trennungsgebot als interpretative Leitlinie für den Informationsaustausch heranzuziehen. Das Trennungsgebot soll den allwissenden Überwachungsstaat verhindern. Entsprechend dieser Ratio ist es richtig, das Trennungsgebot unter dem Aspekt

---

[288] *Petri*, Sicherheitsbehördliche Datenverarbeitung, in: Schmidt/Weichert (Hrsg.), Datenschutz, 2010, S. 117; zu den zunehmenden verdeckten und heimlichen Ermittlungsmethoden *Schwabenbauer*, Heimliche Grundrechtseingriffe, 2013, S. 26 ff.

[289] *Linke*, DÖV 2015, 128 (137).

[290] Vgl. BT-Drs. 17/5694, S. 5.

[291] Vgl. allgemein auch *Bull*, Trennungsgebot und Verknüpfungsbefugnis – Zur Aufgabenteilung der Sicherheitsbehörden, in: Hendler/Ibler/Soria (Hrsg.), „Für Sicherheit, für Europa", FS Götz, 2005, S. 341 (355 f.).

[292] *Zöller*, Informationssysteme und Vorfeldmaßnahmen von Polizei, Staatsanwaltschaft und Nachrichtendiensten, 2002, S. 309.

des Datenschutzes zu beleuchten.[293] Komplexe Angriffe auf die Netz- und Informationssysteme orientieren sich indes nicht entlang der Behördenzuständigkeit. Ein Informationsaustausch über Sachinformationen muss erlaubt sein. Der intensiven und effektiven Zusammenarbeit von Nachrichtendiensten, Polizei, Strafverfolgungsbehörden und militärischen Einheiten zu Analysezwecken steht allerdings auch bei Rückbesinnung auf die ursprüngliche Funktion des Trennungsgebots im Grundsatz nichts im Wege. Das Bundesverfassungsgericht geht in diesem Zusammenhang im Übrigen nur von einem aus dem Grundrecht auf informationelle Selbstbestimmung abzuleitenden informationellen Trennungs*prinzip* aus.[294] Danach dürfen Daten zwischen den Nachrichtendiensten und Polizeibehörden grundsätzlich nicht ausgetauscht werden. Einschränkungen der Datentrennung sind aber zulässig, wenn sie zur operativen Aufgabenwahrnehmung erfolgen. Der Austausch zwischen Nachrichtendiensten und Polizeibehörden muss jedoch einem herausragenden öffentlichen Interesse dienen. Dieser schwerwiegende Eingriff muss durch hinreichend konkrete und qualifizierte Eingriffsschwellen auf der Grundlage normenklarer gesetzlicher Regelungen gesichert sein, wobei die Eingriffsschwellen zur Generierung von Daten nicht unterlaufen werden dürfen.[295]

Im NCAZ sollen personenbezogene Daten ohnehin nicht verarbeitet werden, eine eigene Datei legt das NCAZ nicht an. Sollte ausnahmsweise ein Austausch personenbezogener Daten erforderlich sein, hat dieser ausschließlich zwischen den jeweils beteiligten Behörden und Stellen auf der Grundlage der für die jeweilige Behörde geltenden Gesetze und Vorschriften stattzufinden.[296] Perspektivisch wäre der Austausch personenbezogener Daten im NCAZ auf Grundlage der gebotenen spezifischen Rechtsgrundlage jedenfalls zum Schutz der Informationstechnik kritischer Infrastrukturen rechtfertigungsfähig. Deren Ausfall oder Beeinträchtigung kann bei erheblichen Versorgungsengpässen das herausragende öffentliche Interesse am Informationsaustausch begründen. Problematisch wäre der automatische Zugriff auf behördenfremde Daten.[297] Sobald eine automatisierte oder gar unbegrenzte Zugriffsmöglichkeit auf personenbezogene Daten vorhanden ist, kann darin eine selbstständig zu bewertende Eingriffsqualität zu sehen sein, deren Ausmaß nicht mehr von den Übermittlungsvorschrif-

---

[293] *Nehm*, NJW 2004, 3289 (3294 f.): „Informationelle Aspekte des Datenaustauschs sind nicht Bestandteil des Trennungsgebots. […] Das Trennungsgebot […] hat […] seine unmittelbare verfassungsrechtliche Bedeutung verloren." Vgl. *Gärditz*, JZ 2013, 633 (634).

[294] BVerfGE 133, 277 (329).

[295] BVerfGE 133, 277 (329).

[296] BT-Drs. 17/5694, S. 3; siehe zu den Rechtsgrundlagen § 4 C. I. 2.

[297] Vgl. *Würtenberger*, Polizei- und Ordnungsrecht, in: Ehlers/Fehling/Pünder (Hrsg.), Besonderes Verwaltungsrecht, Band 3, 3. Aufl. 2013, § 69 Rn. 93; *Zöller*, JZ 2007, 763 (770 f.).

ten gedeckt sein dürfte. Diese Form der verstetigten Kooperation wäre auf Grundlage von Kooperationsvereinbarungen, wie sie für das NCAZ bestehen, nicht zu rechtfertigen.

Ein umfassendes informationelles Trennungsgebot ist im Ergebnis nicht zu begründen. Der Austausch allgemeiner Kenntnisse und von Informationen über Zielrichtungen und Motivationen von Angriffen, Auswertungen über die Auswirkungen von Angriffen oder über Sicherheitsschwachstellen im NCAZ ist zulässig. Für den Austausch personenbezogener Daten gilt ein informationelles Trennungsprinzip. Der Austausch solcher Daten zwischen Nachrichtendiensten und Polizei muss einem herausragenden öffentlichen Interesse dienen. Insofern sind für den Informationsaustausch des Bundesnachrichtendiensts mit dem BSI auf Grundlage von § 7 G10 geringe Anforderungen zu stellen, da das BSI von keinen Vollzugs- und Zwangsbefugnissen Gebrauch machen darf. Gleichwohl darf für den Austausch mit dem BSI nicht das befugnisbezogene Trennungsgebot unterlaufen werden. Insgesamt steht weder das Trennungsgebot noch das Trennungsprinzip dem NCAZ in seiner konkreten Gestalt entgegen.

2. Unabhängigkeit der NIS-Behörde

Wesentliche organisationsrechtliche Bedingungen wie die Leitungsstruktur, Weisungsgebundenheit sowie Fach- und Rechtskontrolle haben Bedeutung für die informationsverwaltungsrechtlichen Prozesse. Sie beeinflussen die Wissensproduktion, den Informationsaustausch sowie die Ermessensausübung im staatlichen Informationshandeln. Zu untersuchen ist daher, ob eine fehlende institutionelle Unabhängigkeit der NIS-Behörden Einfluss auf die Gewährleistung der Netz- und Informationssicherheit hat (a). Die Debatte der Unabhängigkeit der Datenschutzaufsicht hat die Frage der grundsätzlichen Zulässigkeit der Unabhängigkeit von Behörden geklärt (b). Die sachliche Rechtfertigung der Unabhängigkeit der NIS-Behörden ist aber, auch wenn die Unabhängigkeit ihre Position als Wissensakteur zu stärken vermag, nicht zuletzt nach dem Verständnis der Schutzziele der Netz- und Informationssicherheit selbst fraglich (c).

a) Stärkung der technischen Sicherheit durch Neutralität

Die Frage der Unabhängigkeit der NIS-Behörde stellt sich nicht so sehr für die ENISA, da es sich bei ihr um eine weitgehend verselbstständigte und unabhängige Unionsagentur handelt.[298] Dagegen ist das BSI gemäß § 1 S. 2 BSIG eine dem Bundesministerium des Innern (BMI) untergeordnete Behörde. Die durch das Unterordnungsverhältnis gegebene Fach- und Rechtsaufsicht des BMI kann

[298] Art. 11 Abs. 1 VO (EU) Nr. 526/2013.

zu Weisungen führen, die den Schutzzielen der Netz- und Informationssicherheit gegenläufig sind.

In der Sicherheitsdebatte ist vorgebracht worden, dass die Doppelrolle des BSI zu Zielkonflikten führe, da sie auf der einen Seite als zivile, präventive Sicherheitsbehörde für Bürger und Unternehmen fungiere und auf der andern Seite zugleich als Fachbehörde andere Sicherheitsbehörden aus anderen Geschäftsbereichen des BMI unterstütze.[299] Dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme werde nicht entsprochen, wenn das BSI in Beratungs- und Mitgestaltungsfunktion an der Entwicklung im E-Government wie der DE-Mail als Standard für die Behördenkommunikation mitwirke und eine sichere Ende-zu-Ende-Verschlüsselung lediglich als unverbindliche Option vorsehe, damit anderen Sicherheitsbehörden der Zugriff auf die E-Mail-Kommunikation ermöglicht werde.[300] Die Glaubwürdigkeit würde zudem leiden, wenn das BSI das Bundeskriminalamt bei der Entwicklung einer bundeseigenen fernforensischen Software (Remote Forensic Software, sog. „Bundestrojaner") unterstütze, da etwaige Instrumente den Zugriff auf fremde informationstechnische Systeme unter Verletzung der Schutzziele der Netz- und Informationssicherheit, nämlich der Integrität und Vertraulichkeit, ermöglichen.[301] Da das BSI vormals als Zentralstelle für das Chiffrierwesen dem Bundesnachrichtendienst unterstellt war,[302] sei es überdies dem Vertrauen abträglich, dass das BSI bei privaten Sicherheitsunternehmen nicht nur Informationen über Schwachstellen, sondern auch über kritische Sicherheitslücken (Zero-Day-Exploits) erwerbe.[303] Die Zusammenarbeit mit Nachrichtendiensten, die nicht wie das BSI zivil und präventiv, sondern offensiv und zum Teil militärisch ausgerichtet seien, stelle einen nicht auflösbaren Interessenkonflikt dar.[304]

---

[299] *Schiller*, Stellungnahme zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme, A-Drs. 18(4)284 C, S. 6 f.; *Neumann*, Stellungnahme zum IT-Sicherheitsgesetz, A-Drs. 18(24)11, S. 8.

[300] Neumann, E-Government-Gesetz: Bundesregierung will Verschlüsselungsstandards senken, Netzpolitik.org vom 19.03.2013.

[301] *Meister*, Geheime Kommunikation: BSI programmierte und arbeitete aktiv am Staatstrojaner, streitet aber Zusammenarbeit ab, Netzpolitik.org vom 16.03.2015. Dass das BSI aktiv das Bundeskriminalamt bei der Entwicklung unterstützte, ergibt sich aus der Antwort des BSI auf eine Informationsanfrage nach § 1 IFG selbst, siehe Antwort des BSI vom 08.04.2015, Az. B21-010 03 05/001, abrufbar unter: https://fragdenstaat.de/anfrage/zusammenarbeitsverbot-bsibka/.

[302] Siehe § 3 B. II. 1. a).

[303] *Schulski-Haddouti*, Crypto Wars 3.0: Neuorganisation des BSI gefordert, Heise Online vom 28.01.2015.

[304] Vgl. BT-Drs. 17/14797, S. 5; Bernhardt/Ruhmann, IT-Sicherheit nach dem neuen IT-Sicherheitsgesetz, Beitrag zur Sommerakademie „Vertrauenswürdige IT-Infrastruktur – ein unerreichbares Datenschutzziel", 31.08.15; *Rötzer*, NSA, BND, BSI und Verfassungsschutz

Die informationsverwaltungsrechtliche These kann daher lauten, dass eine unabhängige, weisungsfreie NIS-Behörde ihr Ermessen eher dahingehend ausübt, Informationen im Rahmen der europäischen NIS-Kooperation weiterzuleiten oder Kenntnisse von IT-Schwachstellen nicht mit anderen (ausländischen) Nachrichtendiensten, Polizeibehörden oder sonstigen Stellen zu teilen, damit diese die Informationen nicht bei gleichzeitigem Verstoß gegen die Schutzziele der Netz- und Informationssicherheit für ihre Aufgabenerfüllung ausnutzen. Denn eine unabhängige NIS-Behörde müsste auf Interessen anderer Sicherheitsbehörden, die für ihre Aufgabenerfüllung auf das Ausnutzen von Sicherheitslücken angewiesen sind und insofern ein gewisses Interesse an einer nicht umfassenden Netz- und Informationssicherheit haben, keine Rücksicht nehmen und könnte Entscheidungen über den Informationsaustausch primär an den Schutzzielen der Netz- und Informationssicherheit (vgl. Art. 4 Nr. 2 NIS-RL) ausrichten. Am Beispiel des BSI würde dies bedeuten, dass das aufsichtführende BMI dem BSI den Austausch von Erkenntnissen über kritische Sicherheitslücken mit anderen europäischen Stellen nicht etwa deshalb untersagen kann, weil diese Sicherheitslücken für Operationen des Bundesnachrichtendienstes, des Bundesamtes für Verfassungsschutz oder des Bundeskriminalamtes von strategischer Bedeutung sind.

b) Unionsrechtliche Zulässigkeit weisungsfreier Räume

Gegen die Unabhängigkeit von NIS-Behörden ließe sich von vorneherein einwenden, dass Behörden mit Eingriffsbefugnissen nicht außerhalb der demokratischen Legitimation handeln dürften. Diese erste organisationsrechtliche Konfliktlinie in der Frage der Zulässigkeit weisungsfreier Räume lässt sich am Beispiel der Unabhängigkeit der Datenschutzaufsicht untersuchen, der ohnehin eine gewichtige Rolle in der Gewährleistung der Internetsicherheit zukommt.[305]

Die Aufsichtsbehörden handeln bei der Ausübung ihrer Befugnisse „völlig unabhängig“ (Art. 52 Abs. 1 DS-GVO). Die Unabhängigkeit ist verfassungsrechtlich in Art. 8 Abs. 1 GRCH in Verbindung mit Art. 6 Abs. 1 EUV und in Art. 16 Abs. 2 UAbs. 1 S. 2 AEUV verankert. Was der materielle Inhalt administrativer Unabhängigkeit ist, musste durch die Große Kammer des Europäische Gerichtshof erst geklärt werden, nachdem gegen die Bundesrepublik Deutschland ein Vertragsverletzungsverfahren eingeleitet worden war, weil es die Da-

---

unter einer Decke, Telepolis vom 20.06.2014; vgl. am Beispiel der US-amerikanischen National Security Agency *Bambauer*, Sharing Shortcomings, Loyola University Chicago Law Journal Vol. 47 (2015), 465 (477): „Vulnerability information can be used to advance only one of [the two NSA's missions]“.

[305] § 3 B. II. 2.

tenschutzaufsichtsbehörden staatlicher Aufsicht unterwarf.[306] Die Bundesrepublik Deutschland verstand Unabhängigkeit im Sinne der funktionellen Unabhängigkeit, die sich in der Nichtbeeinflussung des Entscheidungsprozesses manifestiere.[307] Aufgrund der den Datenschutzbehörden verliehenen Befugnisse handele es sich um eine Eingriffsverwaltung. Das Gebot der demokratischen Legitimation verlange eine Weisungsgebundenheit der Datenschützer gegenüber der Regierung.

Der Gerichtshof legte den Begriff als institutionelle Unabhängigkeit aus.[308] Diese ist bei einer eigenständigen, rechtlich begründeten Organisation gegeben, die grundsätzlich keiner Rechts- und Fachaufsicht unterliegt.[309] Eine staatliche Aufsicht „gleich welcher Art" sei mit der Unabhängigkeit unvereinbar. Das Erfordernis der Objektivität und Unparteilichkeit sei nur durch Schutz vor „jeglicher Einflussnahme von außen", d. h. auch seitens des Staates, erfüllt.[310] Es reiche mithin die „bloße Gefahr" einer Einflussnahme, da es einen „vorauseilenden Gehorsam" der Datenschutzaufsicht im Hinblick auf die Entscheidungspraxis geben könne.[311]

Die Unabhängigkeit einer Behörde birgt demnach das demokratietheoretische Probleme der nach Art. 2 EUV gebotenen Legitimation öffentlicher Stellen. Die Legitimationssubjekte müssen Regeln und Herrschaft akzeptieren.[312] Das konventionelle deutsche Verständnis geht von einem grundsätzlichen Verbot ministerialfreier Räume aus, demzufolge jeder Amtsträger dergestalt sachlich-inhaltlich legitimiert sein muss, dass sich die Legitimationskette über die Ingerenzbefugnisse der Exekutive und insbesondere durch die Instrumente der Rechts- und Fachaufsicht realisiert.[313] Das Bundesverfassungsgericht ließ jedoch ministeri-

---

306 EuGH, C-518/07, Rn. 1.

307 EuGH, C-518/07, Rn. 16; *Tinnefeld/Buchner/Petri*, Einführung in das Datenschutzrecht, 2012, S. 429; vgl. *Bredt*, Die demokratische Legitimation unabhängiger Institutionen, 2006, S. 32, der darunter formal die „sachliche Unabhängigkeit" versteht; anders: *Ehmann/Helfrich*, EG-DSRL, 1999, Art. 28 Rn. 4: „keinerlei Weisung".

308 EuGH, C-518/07, Rn. 32, 33; *Petri*, in: Simitis (Hrsg.), BDSG, 8. Aufl. 2014, § 38 Rn. 7; *Hillenbrand-Beck*„ in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, Kap. 5.4, Rn. 26.

309 *Bredt*, Die demokratische Legitimation unabhängiger Institutionen, 2006, S. 29.

310 EuGH, C-518/07, Rn. 25, 30.

311 EuGH, C-518/07, Rn. 36.

312 Vgl. *Würtenberger*, Legitimität, Legalität, in: Brunner/Conze/Kosselleck (Hrsg.), Geschichtliche Grundbegriffe, Band 3, 1982, S. 677 (678 f.); ferner *Wiedemann*, Unabhängige Verwaltungsbehörden und die Rechtsprechung des Bundesverfassungsgerichts zur demokratischen Legitimation, in: Masing/Marcou (Hrsg.), Unabhängige Regulierungsbehörden, 2010, S. 39 (40).

313 BVerfGE 107, 59 (87 f.); *Klein*, Die verfassungsrechtliche Problematik des ministerialfreien Raumes, 1974, S. 47 f.; *Möllers*, Gewaltengliederung – Legitimation und Dogmatik im nationalen und internationalen Rechtsvergleich, 2005, S. 121.

alfreie Räume in verselbstständigten Verwaltungseinheiten für Angelegenheiten zu, die nicht von einem solchen politischen Gewicht sind, dass sie der Regierungsverantwortung entzogen werden können.[314] Wie sich aus Art. 23 GG ergibt, müssen Gehalte von Unionsgrundsätzen nicht immer den Vorgaben der Mitgliedstaaten entsprechen. Die deutsche Verfassungsordnung ist grundsätzlich offen für neue organisationsrechtliche Ansätze. Die Bestimmung des unionsrechtlichen Demokratiegehalts fordert ihrem Charakter nach zwar eine rechtvergleichende Untersuchung, sie kann aber gleichwohl autonom ausgelegt werden.[315] Nicht zuletzt lässt auch das Unionsrecht mit der Meroni-Doktrin[316] grundsätzlich keine ungesteuerte Herausbildung unabhängiger „Cluster unbeantworteter Selbstherrschaft der Verwaltung" zu und setzt Formen demokratischer Zurechnungs- und Verantwortungszusammenhänge auf allen Ebenen voraus.[317] Der Grundsatz der Demokratie bedeutet aber nicht, dass es außerhalb des „klassischen hierarchischen Verwaltungsaufbau[s]" keine öffentlichen Stellen geben könne, die von der Regierung mehr oder weniger unabhängig sind.[318]

Die volle Unabhängigkeit einer Behörde ist also grundsätzlich zulässig, wenn sie aus sachlichen Gründen gerechtfertigt werden kann.

c) Sachliche Rechtfertigung der Unabhängigkeit

Sachliche Gründe zur Rechtfertigung organisationsrechtlicher Unabhängigkeit können epistemischer Natur sein (aa). Die Prämissen der Argumente für eine Unabhängigkeit von Behörden können allerdings bezweifelt werden (bb). Als rechtliche Gestaltungsoption, die dem unionsrechtlichen Wirksamkeitsgebot der NIS-RL entspräche, kommt die Veröffentlichung von Weisungen in Betracht (cc).

aa) Stärkung der Wissensfunktion durch Unabhängigkeit

Die unter dem Etikett New Public Management vorgeschlagene neue Verwaltungsstrategie beruhte auf der Annahme, dass das monistische Modell des Verwaltungsaufbaus der Aufgabenkomplexität der modernen Gesellschaft nicht gerecht werde und nicht adäquat auf die voranschreitende Ausdifferenzierung reagieren könne.[319] Übergeordnete Zielsetzung der Agenda des New Public

---

[314] BVerfGE 9, 268 (282); vgl. BVerfGE 111, 333 (354) in Bezug auf Art. 5 Abs. 3 S. 1 GG.

[315] BVerfGE 123, 267 (Rn. 266); *Wendel*, Permeabilität im europäischen Verfassungsrecht, 2011, S. 347; *Görisch*, Demokratische Verwaltung durch Unionsagenturen, 2009, S. 111.

[316] EuGH, C-9/56 – Meroni/Hohe Behörde, Slg. 1958, S. 9 (44, 2. Abs.).

[317] *Gärditz*, AöR 135 (2010), 251 (277).

[318] EuGH, C-518/07, Rn. 42; vgl. *Balthasar*, ZÖR 2012, 5 (37); *Spiecker gen. Döhmann*, JZ 2010, 787 (789).

[319] *Rittner*, JZ 2003, 641 ff.; *Shirvani*, DÖV 2008, 1 (4 ff.).

Managements war die Entflechtung von Politik und Verwaltung durch Hierarchieabbau und Dezentralisierung.[320] Die Modellannahme, dass die Gesamtheit aller Bürger chancengleich Input zu allen politischen Entscheidungsprozessen geben könne, wurde als zu idealistisch empfunden, und es entstand das Bedürfnis nach einem komplexeren, pluralistischen Legitimationskonzept, in dem zwar das Parlament den Platz eines festen Bausteins im „Legitimationsmosaik" einnimmt, seine Legitimationsrolle aber relativiert wird.[321] Eine neue Demokratiedogmatik reagiert auf diese Verwaltungsrationalitäten und Heterarchisierung der Verwaltungsorganisation, indem sie das traditionelle Legitimationskonzept ergänzt oder modifiziert.[322]

Als Ergänzung komme eine Output-Legitimation in Betracht. Bei diesem aus der Politikwissenschaft übernommenen normativen Begriff geht es zunächst um die wünschbare Qualität von Entscheidungen, die die realisierten Outputs aufgenommener Inputs (artikulierte Interessen) darstellen.[323] Die Kategorie der Effizienz spielt insofern eine Rolle, als die Lockerung parlamentarischer Rückbindung durch Repräsentation für zulässig erachtet wird, soweit dies eine bessere Aufgabenwahrnehmung ermögliche (effiziente, post-parlamentarische Demokratie).[324] Die Erreichung größtmöglicher Verwaltungseffizienz wird in der Ablösung des traditionellen hierarchischen Governments zugunsten einer flachen, netzwerkartigen Governance gesehen.

Für die Frage der Qualität behördlichen Handelns kann auch ein epistemischer Maßstab angelegt werden. Die Unabhängigkeit der Zentralbanken im Europäischen System der Zentralbanken (ESZB) und von Unionsagenturen wird insbesondere damit gerechtfertigt, dass dadurch weniger opportunitätsgetriebene und eher wissensbasierte, sachorientierte Entscheidungen getroffen werden.

---

[320] *Groß*, Die Verwaltungsorganisation als Teil organisierter Staatlichkeit, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band I, 2. Aufl. 2012, § 13, Rn. 31.

[321] Pointiert *Shapiro*, Independent Agencies, in: Craig/de Búrca (Hrsg.), The Evolution of EU Law, 2011, S. 113: „No one longer believes that government is likely to run things well."

[322] Vgl. *Pernice*, Soll das Recht der Regulierungsverwaltung übergreifend geregelt werden?, in: Ständige Deputation des Deutschen Juristentages (Hrsg.), Verhandlungen 66. DJT 2006, Band II/1, 2006, O 85 (O 133); *Pöcker*, VerwArch 99 (2008), 380 (383).

[323] Grundlegend *Scharpf*, Governing in Europe, Nachdr. der Aufl. von 1999, 2002, S. 16 f., 20; *Trute*, Die demokratische Legitimation der Verwaltung, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts 2012, Band I, 2. Aufl. 2012, § 6, Rn. 53.

[324] *Görisch*, Demokratische Verwaltung durch Unionsagenturen, 2009, S. 318 ff.; *Jestaedt*, Demokratieprinzip und Kondominialverwaltung, 1993, S. 590 ff.; vgl. zum Effizienzgedanken *Everson*, ELJ 1995, 180 (182 f.); *Eidenmüller*, Effizienz als Rechtsprinzip, 4. Aufl. 2015.

Die Zentralbanken dürfen gemäß Art. 130 AEUV keine Weisungen von Unionsstellen oder mitgliedstaatlichen Stellen entgegennehmen oder solche einholen.[325] Eine Beeinflussung der Beschlussorgane darf ebenfalls nicht stattfinden. Zur Rechtfertigung wird ökonomisch die Zeitinkonsistenztheorie angeführt, die mit der Zentralbankunabhängigkeit eine höhere Glaubwürdigkeit und als Folge wiederum die Erwartung einer niedrigeren Inflationsrate verknüpft.[326] Die Unabhängigkeit soll aber auch vor „jedem politischen Druck" bewahren, „damit sie die für ihre Aufgaben gesetzten Ziele durch die unabhängige Ausübung der spezifischen Befugnisse" wirksam verfolgen kann.[327] In der Sache sah das Bundesverfassungsgericht im Maastricht-Urteil den Zweck, das Währungswesen dem Zugriff von Interessengruppen und der an einer Wiederwahl interessierten politischen Mandatsträger zu entziehen, ebenfalls als gerechtfertigt an.[328] Die nunmehr in Art. 88 S. 2 GG normierte Unabhängigkeit erkannte das Gericht als eine mit Art. 79 Abs. 3 GG vereinbare Modifikation des Demokratieprinzips an.[329] Die Autonomie bezweckt somit letztlich eine Entpolitisierung zur Sicherstellung der sachrichtigen Entscheidung.

Bei den Unionsagenturen lässt sich in der Begründung der Unabhängigkeit die epistemische Dimension noch deutlicher erkennen. Für die Unabhängigkeit der von der Linienorganisation der Staatsverwaltung losgelösten und hauptsächlich in die polyzentrische Verwaltung eingebundenen Unionsagenturen wird neben der Trennung von kurzfristigen politischen Zyklen das Generieren von Expertise genannt.[330] So soll etwa die ENISA „als Bezugspunkt fungieren und durch die Unabhängigkeit, die Qualität ihrer Beratung und der verbreiteten Informationen" Vertrauen schaffen.[331] Der Aspekt einer unabhängigen und damit qualitativ besseren Sachentscheidung spielt auch bei den Regulierungsbehörden im Telekommunikationsrecht eine Rolle. Die Mitgliedstaaten haben nach Art. 3 Abs. 3 lit. a RL 2002/21/EG[332] dafür Sorge zu tragen, dass die Behörden Befugnisse für die Vorabregulierung des Markts oder für die Beilegung von Streitigkeiten zwischen Unternehmen unparteiisch und transparent aus-

---

325 Vgl. *Zilioli/Selmayr*, CMLR 2000, 591 (624 ff.).

326 Vgl. *Dutzler*, Der Staat 41 (2002), 495 (514).

327 EuGH, C-11/00, Rn. 134.

328 BVerfGE 89, 155 (207); *Pernice*, Das Ende der währungspolitischen Souveränität Deutschlands und das Maastricht-Urteil des BVerfG, in: Due/Lutter/Schwarze (Hrsg.), FS Everling, Band II, 1995, S. 1057 (1068).

329 BVerfGE 89, 155 (207 f.); siehe auch *Pernice*, in: Dreier (Hrsg.), GG, Band III, 2. Aufl. 2008, Art. 88 Rn. 26.

330 *Wentzel*, DÖV 2010, 763 (766); *Kommission*, Mitteilung über Rahmenbedingungen für die europäischen Regulierungsagenturen, KOM (2002) 718 vom 11.12.2002, S. 15.

331 Erwägungsgrund 18 VO (EU) Nr. 526/2013.

332 Art. 1 Nr. 3 b) der RL 2009/140/EG zur Änderung der RL 2002/21/EG.

üben. Bei der Durchführung ihrer Aufgaben sollen die Behörden vor äußerer Einflussnahme und politischem Druck geschützt werden, „die sie an der unabhängigen Beurteilung der von ihnen bearbeiteten Angelegenheiten hindern könnten."[333] Gleichgelagert fällt die Argumentation bei einem rechtsvergleichenden Blick für die *autorités administratives indépendantes* (AAI), die in Frankreich zu einem neueren Typus „unabhängiger Verwaltungsbehörde" gehören und als deren Prototyp die französische Datenschutzbehörde Commission Nationale de l'informatique et des libertés (CNIL) gilt.[334] Die angestrebte Unparteilichkeit soll dazu dienen, Informationen möglichst objektiv zu sammeln und weiterzuleiten, Diskussionen anzuregen, widerstreitenden Interessen Raum zu geben und diese in Einklang zu bringen.[335]

Im Ergebnis wird einer Behörde rechtliche Unabhängigkeit eingeräumt, damit sie Aufgaben effektiver wahrnehmen kann, wenn sie keinerlei Einfluss von Seiten anderer staatlicher Stellen unterliegt. Effektivität im Zusammenhang einer unabhängigen NIS-Behörde hieße mehr Freiraum für den Austausch von Informationen und damit im Ergebnis weniger Informationsbegrenzung. Normativ angeknüpft werden kann diese These an Art. 8 Abs. 5 NIS-RL. Danach haben die Mitgliedstaaten zu gewährleisten, dass die zuständigen Behörden mit angemessenen Ressourcen ausgestattet sind, „damit sie die ihnen übertragenen Aufgaben wirksam und effizient wahrnehmen können und die Ziele dieser Richtlinie somit erreicht werden". Ausgewiesenes Ziel ist es gemäß Art. 1 Abs. 1 NIS-RL, ein „hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen in der Union zu erreichen." Auf dieses Ziel der Richtlinie sind die Mitgliedstaaten gemäß Art. 288 Abs. 3 AEUV verpflichtet.

Den Mitgliedstaaten ist die Wahl der Form und der Mittel überlassen. Würde im Sinne wirksamer Informationsflüsse die Unabhängigkeit der NIS-Behörden gefordert, kann nicht von vorneherein dagegen ein allgemeiner Grundsatz der organisationsrechtlichen Autonomie der Mitgliedstaaten angeführt werden. Die institutionelle Autonomie der Mitgliedstaaten und die verfassungsmäßigen Verpflichtungen der Mitgliedstaaten sind zwar Schutzgut des Verhältnismäßigkeitsgrundsatzes von Art. 5 Abs. 4 EUV.[336] Die Autonomie kann jedoch nur

---

[333] Erwägungsgrund 13 RL 2009/140/EG.

[334] *Vilain*, Demokratische Legitimität und Verfassungsmäßigkeit unabhängiger Regulierungsbehörden, in: Masing/Marcou (Hrsg.), Unabhängige Regulierungsbehörden, 2011, S. 9 (11).

[335] Vgl. Bericht des Conseil d'Etat, Réflexions sur les autorités administratives indépendantes, Études et documents du Conseil d'Etat (EDCE) Nr. 52, 2001, S. 427 ff.; *Lombard*, Warum bedient man sich im Bereich der Wirtschaft unabhängiger Behörden?, in: Masing/Marcou (Hrsg.), Unabhängige Regulierungsbehörden, 2010, S. 143 (145).

[336] *Bast/von Bogdandy*, in: Grabitz/Hilf/Nettesheim (Hrsg.), AEUV/EUV, 57. Aufl. 2015, EUV, Art. 5 Rn. 66.

unter vollständiger Beachtung der in einer Richtlinie festgelegten Ziele und Pflichten ausgeübt werden.[337] Eine die Wirksamkeit des Unionsrechts gewährleistende Organisation mitgliedstaatlicher Behörden kann zur Mitwirkungspflicht der Mitgliedstaaten nach Art. 4 Abs. 3 EUV gezählt werden.[338]

bb) Verfassungsrechtliche Einwände gegen organisationsrechtliche Unabhängigkeit

Die Prämissen der Überlegung über eine unabhängige NIS-Behörde können allerdings bezweifelt werden.

Aus dem Gewaltenteilungsprinzip folgt, dass Gewalt gegenseitig kontrolliert, gehemmt und gemäßigt werden muss.[339] Dieses Prinzip ist Ausfluss der anthropologischen Einsicht der Fehlbarkeit von Amtswaltern. Es stellt sich also die Frage, wie eine Behörde kontrolliert werden soll, die selbst über eine nicht unerhebliche Menge an sicherheitskritischen Informationen und sensiblen Daten verfügt und damit über ein erhebliches Einflusspotenzial. Erkenntnisse aus der Regulierungsökonomie deuten darauf hin, dass politisch unabhängige Behörden eigene „Interessen- und Abhängigkeitsstrukturen" entwickeln können, die mit dem Maßstab selbsterzeugter Expertise unvereinbar sind (sog. *regulatory capture*).[340] Die Annahme, dass eine unabhängige Behörde stets völlig frei von ökonomischen Interessen ist bzw. diesen nicht ausgesetzt ist, erscheint im Lichte der der NIS-Behörde zustehenden Befugnisse zur Durchsetzung der Sicherheitspflichten (vgl. Art. 15 Abs. 1 und Art. 17 NIS-RL) überdies nicht haltbar.

Ein Wegfall von Weisungsbefugnissen und die Neutralisierung staatlicher Machtbefugnisse zur Versachlichung von Entscheidungen können zwar eine Entpolitisierung des Handelns bewirken. Die Berufung auf die Neutralität ist aber nicht erhaben über den Zweifel daran, selbst Ergebnis eines ephemeren rechtspolitischen Zeitgeists zu sein.[341] Eine bestimmte Interpretation des Rechts auf „gute Verwaltung" im Sinne von Art. 41 GRCh und entsprechend Art. 298

[337] EuGH, C-82/07, Rn. 24.

[338] *Kugelmann*, VerwArch 98 (2007), 78 (80).

[339] *Montesquieu*, De l'esprit des lois, 1748, XI, Satz 5: „C'est une expérience éternelle que tout homme qui a du pouvoir est porté à en abuser; il va jusqu'à ce qu'il trouve des limites."

[340] Dazu *Viscusi*/*Harrington*/*Vernon*, Economics of Regulation and Antitrust, 4. Aufl. 2005, S. 379 f.; vgl. *Schuppert*, Die Erfüllung öffentlicher Aufgaben der verselbständigten Verwaltungseinheiten, 1981, S. 341: „Clientele Capture"; *Möllers*, Gewaltengliederung – Legitimation und Dogmatik im nationalen und internationalen Rechtsvergleich, 2005, S. 122.

[341] Gleiches gilt auch für die wirtschaftliche Erkenntnis; vgl. für die „goal independence" der ESZB, *Herdegen*, CMLR 1998, 9 (15): „Economic wisdom is what economic science in a given moment suggest as economically sound. Freezing institutional rules and substantive principles on this basis implies an obvious risk which is inherent in all dictates of economic wisdom: subsequent falsification […]."

AEUV birgt die Gefahr, dass Teilinteressen zum Interesse des Ganzen und damit zum Gemeinwohl aufgewertet werden.[342] Das Argument der Expertise beruht nicht zuletzt auf der Annahme der Möglichkeit freien und unpolitischen wissenschaftlichen Expertenwissens. Diese Voraussetzung ist in der Wissenschaftstheorie ohnehin mittlerweile schon im Rückzug begriffen.[343] Wird aber die geforderte Unparteilichkeit daran bemessen, wie sie ein Allgemeininteresse absichern oder berücksichtigen kann, dann ist eigentlich die Verwaltung umso unparteiischer, je stärker sie politisch rückgebunden ist an eine Institution, die selbst durch demokratische Wahlen legitimiert ist.[344]

Die Frage der Unabhängigkeit der NIS-Behörde kann letztlich selbst als politische Frage angesehen werden. Bei der Beantwortung derartiger Fragen kann das Recht in Ermangelung klarer Maßstäbe für eine angemessene Sachbefassung funktionell überfordert werden. Dies spricht für eine Zurückhaltung beim Treffen von Aussagen. Diesem Ansatz soll hier gefolgt werden. Im Übrigen folgt auch aus dem Begriff der Netz- und Informationssicherheit nicht, die NIS-Behörde institutionell unabhängig auszugestalten.

Die Prüfung der Unabhängigkeit der Datenschutzaufsicht durch den Europäischen Gerichtshof war zulässig, weil das Primärrecht die Unabhängigkeit vorgibt (Art. 8 Abs. 1 GRCH, Art. 16 Abs. 2 UAbs. 1 S. 2 AEUV). Dagegen ist die Unabhängigkeit der NIS-Behörde weder ein Gebot von Verfassungsrang, noch folgt sie aus dem Sekundärrecht. Art. 8 Abs. 5 NIS-RL verpflichtet die Mitgliedstaaten auf das Ziel, die NIS-Behörden so auszustatten, dass diese wirksam ihre Pflichten erfüllen können. Zum Erreichen dieses Ziels ist die Unabhängigkeit, anders als in Art. 52 DS-GVO für die Datenschutzaufsicht, gerade nicht gefordert.

Sie kann auch nicht aus den Schutzzielen der Netz- und Informationssicherheit abgeleitet werden, die zu erreichen die Mitgliedstaaten verpflichtet sind. Bereits in der Begriffsbestimmung wird der Begriff der Sicherheit verstanden als „die Fähigkeit von Netz- und Informationssystemen, auf einem bestimmten Vertrauensniveau alle Angriffe abzuwehren“ (Art. 4 Nr. 2 NIS-RL). Ebenso zielt die NIS-RL als solche nicht auf die Gewährleistung größtmöglicher Sicherheit, sondern auf ein „hohes gemeinsames Sicherheitsniveau“ (Art. 1 Abs. 1 NIS-RL). Die Begriffsbestimmung setzt das Ziel der Sicherheit nicht absolut und lässt Raum für die Verfolgung anderer rechtsstaatlicher Zwecke, auch wenn

---

[342] Vgl. *Waechter*, Geminderte demokratische Legitimation staatlicher Institutionen im parlamentarischen Regierungssystem, 1994, S. 253, 255.

[343] Nachweise bei *Möllers*, Gewaltengliederung – Legitimation und Dogmatik im nationalen und internationalen Rechtsvergleich, 2005, S. 122 (Fn. 154).

[344] *Lombard*, Warum bedient man sich im Bereich der Wirtschaft unabhängiger Behörden?, in: Masing/Marcou (Hrsg.), Unabhängige Regulierungsbehörden, 2010, S. 143 (145).

darauf gestützte Maßnahmen die Schutzziele der Netz- und Informationssicherheit durch den heimlichen Zugriff auf ein informationstechnisches System bei Ausnutzen einer Sicherheitslücke oder über die Installation eines Spähprogramms verletzen. Ein solcher Zweck kann die effektive Strafverfolgung sein. Die vollständige Wahrheitsermittlung im Strafverfahren und die wirksame Aufklärung gerade schwerer Straftaten ist ein wesentlicher Auftrag in einem rechtsstaatlichen Gemeinwesen.[345] Wenn das BSI an der technischen Überprüfung fernforensischer Software mitwirkt und es unterlässt, über den Schutz dagegen zu informieren, so dient dies nicht zuletzt der Erfüllung der Auflagen, die das Bundesverfassungsgericht in seinem Urteil zur Online-Durchsuchung an eine solche staatliche Software aufstellte. Selbst ohne konkrete Missbrauchsabsicht von den Mitarbeitern der Behörden stellt bereits das Vorhandensein einer solchen Einrichtung eine Schwächung der IT-Sicherheit dar.[346] Es ist daher sogar rechtlich geboten, dass das BSI die IT-Sicherheit einer solchen staatlichen Software prüft. Das gleiche trifft für Sicherheitsinformationen zu, die gleichsam für Nachrichtendienste von Bedeutung sind. Auch hier ist das Interesse an der Informationsweitergabe durch die NIS-Behörde an andere europäische oder mitgliedstaatliche NIS-Behörden zum Zweck der Gewährleistung der Netz- und Informationssicherheit nicht von vorneherein höher zu bewerten als das Interesse der Nachrichtendienste an ihrer Aufgabenerfüllung, für die sie auf strategische Informationen über Schwachstellen in informationstechnischen Systemen angewiesen sind.

cc) Veröffentlichung von Weisungen als Gestaltungsoption

Um ein wirksames informationsverwaltungsrechtliches Handeln im Sinne der Netz- und Informationssicherheit zu gewährleisten, kommt als Gestaltungsoption die Transparenz von Weisungen in Betracht, wie dies § 117 TKG für die Bundesnetzagentur vorsieht. Die Behörde ist zwar eine selbstständige Bundesoberbehörde im Geschäftsbereich des Bundesministeriums für Wirtschaft und Technologie, § 1 S. 2 BEGTPG.[347] Da § 117 TKG ausdrücklich die Weisungsmöglichkeit einschließt, wird angenommen, dass das Ministerium als übergeordnete oberste Bundesbehörde im Wege der Rechts- und Fachaufsicht mit (Einzel-)Weisungen tätig werden kann.[348] Allerdings sind die erteilten Weisungen

---

[345] BVerfGE, 129, 208 (260).

[346] BVerfGE 120, 274 (325 f.).

[347] Gesetz über die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen vom 7. Juli 2005 (BGBl. I S. 1970, 2009), das zuletzt durch Art. 2 des Gesetzes vom 26. Juli 2011 (BGBl. I S. 1554) geändert worden ist.

[348] *Geppert*, in: ders./Schütz (Hrsg.), BeckTKG, 4. Aufl. 2013, § 117 Rn. 1 f.

nach § 117 TKG bzw. § 61 EnWG zu veröffentlichen. Es wird angenommen, dass dieses Transparenzerfordernis das zuständige Bundesministerium weitgehend davon abhält, von seiner Befugnis Gebrauch zu machen.[349] Insofern ist die Bundesnetzagentur nicht *de jure*, aber zumindest *de facto* weisungsfrei, ohne dass die Kontrollmöglichkeit als Basis demokratischer Legitimation entfällt.[350]

IV. Informationsverweigerungsrecht der Mitgliedstaaten zur Wahrung wesentlicher Sicherheitsinteressen

Die mit der Informationskooperation verfolgten Anliegen können mit den legitimen Sicherheitsinteressen der Mitgliedstaaten in einem Spannungsverhältnis stehen. Dieses in Informationsbeziehungen auszugleichen ist Zweck des Art. 346 AEUV, der den Mitgliedstaaten nach Abs. 1 lit. a ein Auskunftsverweigerungsrecht gewährt.[351] Dieses Recht ist als „praktisch nicht sehr bedeutsam" bezeichnet worden.[352] Im europäischen NIS-Informationsaustausch kann das Auskunftsverweigerungsrecht ein zentraler Hebel sein, den Informationsaustausch zu beschränken.

Die Mitgliedstaaten können sich mit Art. 346 Abs. 1 lit. a AEUV auf einen Rechtfertigungsgrund berufen, der dazu berechtigt, bei Vorliegen der Voraussetzungen zur Wahrung ihrer wesentlichen Sicherheitsinteressen sich über die Verpflichtungen und die Prinzipien des Unionsrechts begrenzt hinwegzusetzen.[353] Für die Gemeinsame Außen- und Sicherheitspolitik bestehen mit dem Kohärenzgebot des Art. 21 Abs. 3 UAbs. 2 EUV eigene konflikthemmende Regelungen. Die Integration der GASP in das Unionsrecht und die Verzahnung der Wirtschafts- mit der Sicherheitspolitik (inkl. der verteidigungsrelevanten In-

---

[349] *Hermes*, Abhängige und unabhängige Verwaltungsbehörden, in: Masing/Marcou (Hrsg.), Unabhängige Regulierungsbehörden, 2010, S. 53 (77).

[350] *Ludwigs*, Die Verwaltung 44 (2011), 41 (43); *Masing*, Unabhängige Behörden und ihr Aufgabenprofil, in: Masing/Marcou (Hrsg.), Unabhängige Regulierungsbehörden, 2010, S. 181 (197). Dass die Bundesnetzagentur nicht *de jure* weisungsfrei ist, verstößt aber gegen die „völlige Unabhängigkeit" des Bundesbeauftragten für Datenschutz und Informationsfreiheit, weil dieser sich an die Bundesnetzagentur wenden muss (§ 115 Abs. 4 TKG), um datenschutzrechtliche Sanktionen gegen Unternehmen zu bewirken, *Thomé*, VUR 2015, 130 (133); *Schaar*, MMR 2014, 641 (642).

[351] GA Mazák, Rs. C-337/05, Rn. 56. Die kumulative Berufung auf andere Sicherheitsvorbehalte des Primärrechts wie Art. 35, 45 Abs. 3, 2, 62, 65 und 72 AEUV wäre möglich. Diese betreffen aber nicht vorrangig den Austausch von Informationen.

[352] So *Jaeckel*, in: Grabitz/Hilf/Nettesheim (Hrsg.), AEUV/EUV, 57. Aufl. 2015, AEUV, Art. 346 Rn. 16.

[353] Vgl. EuGH, Rs. C-414/97, Rn. 21 ff.; *Jaeckel*, in: Grabitz/Hilf/Nettesheim (Hrsg.), AEUV/EUV, 57. Aufl. 2015, AEUV, Art. 346 Rn. 3.

dustrien) machte weitergehende Konfliktlösungsmechanismen erforderlich. Art. 346 AEUV ermöglicht den Mitgliedstaaten unilaterale Schutzmaßnahmen.

Als Ausnahme ist die Vorschrift bei systematischer Betrachtung eng auszulegen.[354] Dies betrifft zum einen die Funktion der Vorschrift als auch die Last der Obliegenheit der Mitgliedstaaten. Der Vorschrift ist kein Kompetenzvorbehalt zu entnehmen.[355] Die Vorschrift wirkt auch nicht als Regelungsvorbehalt, sodass alle Maßnahmen im Bereich der Netz- und Informationssicherheit im Rahmen der Kompetenzen möglich sind. Den Mitgliedstaaten wird lediglich eine Derogationsbefugnis gewährt.[356] Die Bestimmung beinhaltet schließlich keinen allgemeinen Vorbehalt der Außen- und Sicherheitspolitik zugunsten der Mitgliedstaaten.[357]

Das Recht, Informationen zurückhalten zu können, setzt zunächst Auskunftspflichten voraus. Damit sind die bereits beschriebenen Pflichten zur Übermittlung von Informationen gemeint, also primärrechtlich insbesondere der Grundsatz aus Art. 4 Abs. 3 EUV und die Auskunftspflicht gemäß Art. 337 AEUV, aber auch die sekundärrechtlichen Bestimmungen,[358] folglich auch die zur Gestaltung der NIS-Kooperation.[359] Umfasst sind die Informationspflichten vorrangig gegenüber der Union, es kommen aber ebenso Informationspflichten gegenüber anderen Mitgliedstaaten und sogar gegenüber Einzelnen sowie der Öffentlichkeit in Betracht.[360]

Die Mitgliedstaaten sind nur unter bestimmten Voraussetzungen durch Art. 346 AEUV berechtigt, sich zur Wahrung wesentlicher Sicherheitsinteressen über die Verpflichtungen und Prinzipien des Unionsrechts hinwegzusetzen.[361] Den Mitgliedstaaten kommt eine Einschätzungsprärogative („seines Erachtens") bei der Bestimmung der Sicherheitsinteressen und bei der Frage zu, ob diese beeinträchtigt oder gefährdet sind.[362] Stark in die Vorschrift hinein

---

354 Vgl. EuGH, Rs. C-38/06, Rn. 63.

355 *Kokott*, in: Streinz (Hrsg.), EUV/AEUV, 2. Aufl. 2012, AEUV, Art. 346 Rn. 1.

356 *Kokott*, in: Streinz (Hrsg.), EUV/AEUV, 2. Aufl. 2012, AEUV, Art. 346 Rn. 3.

357 EuGH, C-337/05, Rn. 42 ff. – Kommission/Italien; *Eikenberg,* ELR 25 (2000), 117 (119).

358 *Dittert*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Europäisches Unionsrecht, Band 4, 7. Aufl. 2015, AEUV, Art. 346 Rn. 9; NIS-RL, Erwägung 8.

359 Während der Kommissionsentwurf der NIS-RL Art. 346 AEUV das Primärrecht nur deklaratorisch in Erwägungsgrund 8 nannte, verweist die Richtlinie bereits in den allgemeinen Bestimmungen in Art. 1 auf dieses.

360 *Kokott*, in: Streinz (Hrsg.), EUV/AEUV, 2. Aufl. 2012, AEUV, Art. 346 Rn. 6.

361 Vgl. EuGH, Rs. C-414/97, Rn. 21 ff.; *Jaeckel*, in: Grabitz/Hilf/Nettesheim (Hrsg.), AEUV/EUV, 57. Aufl. 2015, AEUV, Art. 346 Rn. 3.

362 *Wegener*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, 4. Aufl. 2011, AEUV, Art. 346 Rn. 3; *Jaeckel*, in: Grabitz/Hilf/Nettesheim (Hrsg.), AEUV/EUV, 57. Aufl. 2015, AEUV, Art. 346 Rn. 3.

wirkt Art. 4 Abs. 2 S. 2 und 3 EUV. Die Union trifft für bestimmte Schutzgüter eine Achtungsverpflichtung, zu denen in der Staatsfunktionengarantie auch der Schutz der nationalen Sicherheit gehört. Die Rechtmäßigkeit der Auskunftsverweigerung unterliegt der gerichtlichen Kontrolle des Gerichtshofs nach Art. 348 Abs. 2 S. 2 AEUV unter Ausschluss der Öffentlichkeit. Das vorgesehene Konsultationsverfahren mit der Kommission macht deutlich, dass die Wettbewerbsbedingungen auf dem Binnenmarkt möglichst unverfälscht bleiben sollen. Es obliegt dem Mitgliedstaat zu beweisen, dass die Verweigerung der Wahrung der Sicherheitsinteressen dient. Der pauschale Hinweis auf Sicherheitsinteressen genügt dabei nicht.[363] Vor allem muss der verweigernde Mitgliedstaat glaubhaft machen, warum zu befürchten ist, dass die unbefugte Weitergabe der NIS-relevanten Informationen an Dritte zu befürchten ist.

Von dem Begriff der Sicherheitsinteressen ist sowohl die äußere als auch die innere Sicherheit erfasst.[364] Ob eine Information die Abwehr einer Bedrohung von außen betrifft, die gegen den Staat und seine Entwicklungsfähigkeit gerichtet ist, oder ob eine Gefahr ihren Ursprung innerhalb eines Staates hat, lässt sich kaum oder nur mit starken forensischen Mitteln beurteilen. Informationen über Schwachstellen in Netz- und Informationssystemen können gerade bei kritischen Infrastrukturen sowohl militärisch als auch terroristisch ausgenutzt werden. Ausgeschlossen sind zumindest solche Maßnahmen und Aussageverweigerungen als nicht gerechtfertigt, die wirtschaftspolitisch motiviert sind oder finanzielle Ziele verfolgen.[365]

Art. 346 AEUV erweist sich damit als Flaschenhals für die Begrenzung von Informationsflüssen in der europäischen NIS-Kooperation. Das Zusammenspiel von Art. 4 Abs. 2 S. 2 EUV und Art. 346 AEUV weist den Mitgliedstaaten ein weites Ermessen bei der Anwendung der Norm zu. Die Ausübung des Rechts unterliegt aber dem unionsrechtlichen Grundsatz der Verhältnismäßigkeit und ist gerichtlich überprüfbar. Insgesamt steht Art. 346 AEUV einem digitalisierten, automatisierten und integrierten Informationsaustausch nicht strukturell entgegen. Die Mitgliedstaaten müssen die Verweigerung im Einzelfall begründen und können den Austausch nicht pauschal unter Verweis auf Art. 346 AEUV blockieren. Das mitgliedstaatliche Bedürfnis, von Art. 346 AEUV Gebrauch machen zu können, setzt die Prüfung der Informationen voraus, was tendenziell den Informationsaustausch entschleunigt.

---

[363] GA Mazák, Schlussanträge in der Rs. C-337/05, Rn. 58.

[364] EuGH, C-285/98, Rn. 17.

[365] *Jaeckel*, in: Grabitz/Hilf/Nettesheim (Hrsg.), AEUV/EUV, 57. Aufl. 2015, AEUV, Art. 346 Rn. 15.

D. Zwischenergebnis

Der unionsweite Austausch der generierten und ausgewerteten Informationen ist als zentrale Funktionsbedingung für die europäische Internetsicherheit zu nennen. Die Kooperation ist auf Zusammenarbeit und den Austausch von Informationen ausgerichtet und demnach als Lernverbund angelegt. Die Informationskooperation zur Gewährleistung der Sicherheit von Netzen und Informationssystemen erfüllt eine Kompensations- eine Sicherheits- und eine Auffangfunktion. Sie kompensiert vor allem den grenzüberschreitenden Charakter der Sicherheitsgefahren, die Internetinfrastrukturen und -dienste beeinträchtigen können. Gefahren auf europäischer Ebene ergeben sich insbesondere aus der Interdependenz der Infrastrukturen. Insofern kann Zusammenarbeit fehlende nationale Vollzugskompetenzen und -instrumente kompensieren. Sie fungiert als Sicherheitsnetz, weil Strukturen geschaffen werden, die den Mitgliedstaaten einen Austausch über sicherheitsrelevante Informationen ermöglichen und so das Ergreifen von Schutzmaßnahmen erlauben. Eine Auffangfunktion übernimmt die Informationskooperation insofern, als NIS-Akteure aus einem Mitgliedstaat auf einen größeren Wissenstand zurückgreifen können. Auf Eingriffsbefugnisse im eigentlichen Sinne kann die europäische Verwaltung allerdings nicht zurückgreifen.

Der europäische Informationsaustausch ist organisatorisch entlang der aus der IT-Sicherheit bekannten Strukturprinzipien zur Gefahrenabwehr Detektion, Prävention und Reaktion ausgestaltet. Die strategische Kooperation, die über die NIS-Kooperationsgruppe stattfindet, ist den ersten beiden Kategorien zuzuordnen, die operative Kooperation durch das CSRITs-Netzwerk bezweckt eine koordinierte Reaktion auf Sicherheitsvorfälle. Betonung findet auf europäischer Ebene der Austausch von Wissen, Erfahrung und bewährten Praktiken, der es erlaubt, sowohl nationale als auch europäische Kapazitäten aufzubauen. Realisiert wird dieser Austausch informell oder im Wege von Berichts- und Konsultationspflichten. Konsultationspflichten tragen dem Umstand Rechnung, dass die Gewährleistung der Netz- und Informationssicherheit mit besonders instabilen Wissensverhältnissen umgehen muss und prozedurale Strukturen die situationsangepasste Weiterentwicklung der Informationen ermöglichen müssen. Die formalisierten Wissensaustauschverfahren dienen als „Osmose“ zum einen dem Rückgriff auf die besondere Fachkunde anderer Behörden, um Wissensdefizite auszugleichen. Zum anderen geht es über den Gewinn eines fehlenden Tatsachenwissens hinaus um die aktive und diskursive Mitgestaltung der Abwägungsprozesse und Praxis der Sicherheitsgewährleistung.

Eine verfahrensrechtlich dichtere Ausgestaltung besteht für den Austausch von hochsensiblen Informationen über konkrete Sicherheitsrisiken und -vorfäl-

le. Neben der Amtshilfe in Gestalt der Informationshilfe haben dabei spezielle Informationspflichten Bedeutung. Die nationalen NIS-Behörden informieren einen anderen Mitgliedstaat insbesondere dann, sofern ein gemeldeter Sicherheitsvorfall erhebliche Auswirkungen auf die Verfügbarkeit eines wesentlichen oder digitalen Dienstes in jenem Mitgliedstaat hat (Art. 14 Abs. 5, Art. 16 Abs. 6 NIS-RL). Im deutschen Recht besteht für den Informationsaustausch auf horizontaler Ebene diesbezüglich legislativer Klarstellungsbedarf, zumal § 8d VwVfG nur bei Ablauf der Umsetzungsfrist der NIS-Richtlinie Anwendung finden kann. In der operativen Informationskooperation ist im Kern ein europäischer Frühwarn- und Reaktionsmechanismus angelegt. Es ist indes primär Aufgabe des CSIRTs-Netzwerks, ein Verfahren zur unionsweiten Weitergabe dringlicher Informationen zu explorieren. Als Katalysator für den Aufbau einer europäischen CSIRT-Gemeinschaft wirkt die ENISA, deren Mandat unter anderem darin besteht, die Lücke zwischen der technischen Orientierung der CSIRTs und den politischen Zielen der Kommission zu schließen. Eine operative Rolle übernimmt die Agentur jedoch nicht.

Bei Sicherheitsvorfällen in wesentlichen Diensten, die zur Verletzung des Schutzes personenbezogener Daten führen, hat die nationale NIS-Behörde bei der Bearbeitung mit den Datenschutzbehörden zusammenzuarbeiten (Art. 15 Abs. 4 NIS-RL). Da sich das Kooperationsgebot nur auf Sicherheitsvorfälle bei wesentlichen Diensten bezieht, liegt es hier beim nationalen Gesetzgeber, das allgemeine Zusammenarbeitsgebot aus Art. 8 Abs. 6 der NIS-RL auch für Sicherheitsvorfälle bei digitalen Diensten zu spezifizieren, damit die Meldeinformationen über IT-Sicherheitsvorfälle mit Betroffenheit personenbezogener Daten zusammenlaufen.

Der übergreifende Ordnungsrahmen wird vor allem durch den unionsrechtlich kodifizierten Grundsatz der loyalen Zusammenarbeit geprägt. Aus diesem resultiert nicht nur eine allgemeine Rücksichtnahmepflicht, sondern auch eine allgemeine Kooperationspflicht mit wechselseitigen Informationspflichten. Aus dem Grundsatz bzw. aus der Verbindung einer Hauptpflicht mit diesem folgen auch Anforderungen an die inhaltliche Qualität von Informationen. Diese sollten im Grundsatz anschlussfähig (*actionable)* verlässlich (*reliable*) und handhabbar (*manageable*) sein.

Als kritische Rahmenbedingungen für einen gelungenen Wissenstransfer können gegenseitiges Vertrauen und sichere technische Rahmenbedingungen für den Informationsaustausch hervorgehoben werden. Wo der Austausch nicht durch Pflichten angeleitet wird, spielt die gegenseitige, subjektive Einschätzung der Kommunikationspartner eine gewichtige Rolle. Neben sozialen Faktoren wie Integrität, Kompetenz, Erreichbarkeit, Verlässlichkeit, Diskretion, Reputation, kulturellem Hintergrund und Sprachbarrieren hat Vertrauen in der NIS-

Kooperation eine technische Dimension. Die NIS-Richtlinie schafft mit dem Aufbau von Plattformen und eines Rechtsrahmens für den Informationsaustausch eine Basis der Erwartungsstabilisierung. Die Schaffung konkreterer Vertrauensquellen ist allerdings zu einem großen Teil Sache der Mitgliedstaaten. Die Gewährleistung der Sicherheit der Kommunikationsinfrastruktur sowohl der NIS-Kooperationsgruppe als auch der CSIRTs-Netzwerke ist den Mitgliedstaaten überlassen.

Der grenzüberschreitende Austausch personenbezogener Daten ist rechtfertigungsbedürftig. Soweit keine fachgesetzlichen Übermittlungsvorschriften greifen, kann auf das allgemeine europäische Datenschutzrecht rekurriert werden. Spätestens mit der Datenschutzgrundverordnung besteht ein einheitlicher Datenverwendungsraum, der zumindest bestehende datenschutzrechtliche Binnendifferenzierungen hinfällig macht. Soweit das allgemeine Datenschutzrecht Anwendung findet, sind auch Zweckänderungen für die Verwendung der generierten und ausgetauschten Daten denkbar. Für die beim BSI vorhandenen sicherheitsrelevanten Daten über kritische Infrastrukturen besteht eine spezialgesetzliche Zweckbindung. Von der Zweckbindung kann bei näherer Betrachtung auch die Weitergabe der Daten an andere zuständige Aufsichtsbehörden umfasst sein. Wird auf den Zweck der Verarbeitung bei der empfangenden Stelle abgestellt, dürfte die Übermittlung personenbezogener Daten an andere europäische Stellen erlaubt sein.

Der Schutz unternehmensbezogener Daten im Rahmen des auf der NIS-Richtlinie beruhenden Informationsaustausches zeichnet sich durch eine geringe Regelungsdichte aus. Nach der Regelungstechnik der Richtlinie richtet sich der Schutz zu einem maßgeblichen Teil nach dem Recht der nationalen übermittelnden Behörde. Sofern eine Befugnisnorm zur Übermittlung geschützter Daten gefordert wird, findet sich eine ausdrückliche Regelung dafür weder für das BSI noch für die Bundesnetzagentur. Bestehende Regelungen, insbesondere solche im Telekommunikationsrecht, beziehen sich nicht auf den Austausch im Rahmen der europäischen Kooperation im Bereich NIS. Die daraus resultierende Rechtsunsicherheit und die geringe Regelungsdichte stellen ein grundsätzliches Hindernis für einen Austausch sensibler Informationen dar.

Weniger Unwägbarkeiten ergeben sich aus dem den Informationsaustausch begrenzenden Organisationsrecht. Zu den besonderen organisationsrechtlichen Begrenzungen, die den Informationsaustausch betreffen können, gehört in Deutschland das Trennungsprinzip. Dem Austausch von Informationen im Nationalen Cyber-Abwehrzentrums steht das Trennungsprinzip allerdings solange nicht im Wege, wie personenbezogene Daten nicht zwischen Polizei und Nachrichtendienst ausgetauscht werden. Der Austausch allgemeiner Kenntnisse, technischer Informationen oder Informationen über Sicherheitslücken ist grund-

sätzlich zulässig. Für den Austausch personenbezogener Daten gilt indes ein informationelles Trennungsprinzip. Der Austausch zwischen Nachrichtendiensten und Polizei muss einem herausragenden öffentlichen Interesse dienen. Insofern sind für den Informationsaustausch des Bundesnachrichtendiensts mit NIS-Behörden geringere Anforderungen zu stellen, soweit diese von keinen Vollzugs- und Zwangsbefugnissen Gebrauch machen dürfen.

Die Mitgliedstaaten haben zu gewährleisten, dass die zuständigen NIS-Behörden ihre Aufgaben wirksam und effizient wahrnehmen können. Dabei stellt sich die Frage, ob die organisationsrechtliche Weisungsabhängigkeit der Behörden den Austausch von sicherheitskritischen Informationen begrenzen würde, weil die weisungsbefugte Stelle zur NIS-Behörde gegenläufigen Interessen verfolgen könnte, insbesondere dann, wenn sie gegenüber anderen Sicherheitsbehörden, die nicht den Schutzzielen der Gewährleistung der Netz- und Informationssicherheit verpflichtet sind, gleichfalls weisungsbefugt ist. Die Unabhängigkeit ließe sich sachlich mit einer höheren Objektivität und einem wirksameren Informationsaustausch rechtfertigen, wobei die Legitimation an den sachrichtigen Ergebnissen des Verwaltungshandelns gemessen werden könnte (Output-Legitimation). Eine unabhängige Behörde wäre etwa nicht daran gehindert, Informationen über kritische Sicherheitsschwachstellen anderen NIS-Behörden zu übermitteln, wenn sie nicht auch strategische Interessen derjenigen Sicherheitsbehörden zu berücksichtigen hätte, die für ihre Aufgabenerfüllung auf eben diese Sicherheitsschwachstellen angewiesen sind. Gegen die Weisungsunabhängigkeit einer Behörde lässt sich aber insbesondere mit Erkenntnissen aus der Regulierungsökonomie vorbringen, dass unabhängige Behörden durchaus auch eigene, dysfunktionale Interessen- und Abhängigkeitsstrukturen entwickeln können, die konträr zur eigenen Expertise stehen (*regulatory capture*). Eine abschließende Bewertung der Unabhängigkeit würde im Übrigen in Ermangelung eines verfassungsrechtlichen Maßstabs, anders als bei der Unabhängigkeit der Datenschutzaufsichtsbehörden, das Informationsverwaltungsrecht überfordern.

Als primärrechtliche Begrenzung des Informationsaustausches auf europäischer Ebene ist schließlich Art. 346 AEUV zu beachten. Die Berufung auf das Auskunftsverweigerungsrecht kommt vor allem bei sicherheitsrelevanten Informationen infrage, die kritische Infrastrukturen betreffen, deren Kritikalität in der Bedeutung für die öffentliche bzw. nationale Sicherheit begründet ist. Zwar steht den Mitgliedstaaten ein weiter Ermessenspielraum zu, in dem sie von ihrem Recht Gebrauch achen können. Die Ausübung des Rechts ist aber für jeden Einzelfall zu begründen und am Maßstab der Verhältnismäßigkeit zu messen. Der Aufbau eines automatisierten Informationsaustausches im Rahmen eines automatisierten Informationssystems steht dem aber nicht prinzipiell entgegen.

§ 5 Distribution von Informationen über die Netz- und Informationssicherheit

Die Untersuchung konzentrierte sich bislang darauf, wie öffentliche Stellen Daten und Informationen gewinnen können, um epistemischen Unsicherheiten zu begegnen, und wie die gewonnenen Informationen national und im Rahmen des europäischen NIS-Kooperationsnetzes weitergegeben werden, damit europaweit die Sicherheit im Cyberspace erhöht werden kann. Die dabei ausgearbeiteten Ergebnisse zeigen, dass die staatlichen wie europäischen Stellen im Rahmen des NIS-Kooperationsnetzes in einem beachtlichen Ausmaß Informationen und Daten aggregieren können. Das Informationsverwaltungsrecht als Informationsallokationsrecht betrachtet Informationen als Ressource, die als Steuerungsfaktor eingesetzt werden kann. Es stellt sich die Frage, wie das kognitive Potenzial dieses öffentlichen Informationspools bei den Privaten, d. h. den Anwendern, Nutzern und Unternehmen, genutzt werden kann, um die Internetsicherheit besser zu gewährleisten.

Im nachfolgenden Kapitel soll daher untersucht werden, wie der Staat und die Europäische Union als Informationsmittler auftreten können, um ihre Pflicht zur Gewährleistung der Internetsicherheit durch die Weitergabe von Informationen zu erfüllen. Dabei stehen nicht so sehr verfassungsrechtliche und demokratietheoretische Überlegungen im Vordergrund. Im Fokus steht vielmehr die Erkenntnis, dass das Wissen in der Informationsgesellschaft fragmentiert und zerstreut vorliegt und es gesamtgesellschaftlich sinnvoller sein kann, Informationen möglichst breit zu distribuieren, statt sie zentral zu akkumulieren und ggf. selbst zu verwerten.[1] Die Frage ist also, was die informationsverwaltungsrechtlichen Mittel und Pflichten zur Distribution von Wissen und Informationen zur Netz- und Informationssicherheit sind.

Da sicherheitskritische Informationen nicht einseitig und pauschal sicherheitsfördernd distribuiert werden können, sondern mit spezifischen Belangen, multipolaren Interessen, Konflikten und Konkurrenzen verbunden sind, ist zunächst zu bestimmen, welche Rolle die Information von Privaten in der Sicher-

[1] Vgl. *Schoch*, Diskussionsbeitrag, in: VVDStRL 63 (2004), S. 442 (443); *Augsberg*, Informationsverwaltungsrecht, 2014, S. 216.

heitsgewährleistung einnehmen kann (A.). Die eigentliche Distribution kann auf verschiedene Weisen vollzogen werden.[2] Rechtssystematisch kann eine Zweiteilung staatlicher Informationstätigkeit in aktives und reaktives Informationshandeln zugrunde gelegt werden. Aktives staatliches Informationshandeln ist dadurch gekennzeichnet, dass öffentliche Stellen von sich aus proaktiv die Öffentlichkeit oder einzelne Betroffene bzw. Interessierte informieren (B.). Informationsdistribution ist keineswegs ein paternalistischer Ansatz. Denn staatliche Stellen können auch zu reaktivem Informationshandeln verpflichtet sein, wenn Private von sich aus am staatlichen Wissen oder den vorhandenen Informationen partizipieren möchten (C.).

A. Funktion der Informationsdistribution für die Sicherheitsgewährleistung

Informationsdistribution betrifft das nach außen hin gerichtete Informationsverwaltungsrecht, d. h. die Kommunikativität des Rechtssystems und demnach die Informationsaustauschbeziehung mit Privaten.[3] Der Grundgedanke der Informationsdistribution, das „kognitive Kapital der Gesamtgesellschaft" durch neue informationelle Möglichkeiten und dadurch entstehende neue Informationen in der Summe steigen zu lassen,[4] lässt sich auf die Gewährleistung der Internetsicherheit anwenden. Staatliche Informationstätigkeit kann die Anwender, Nutzer, Betreiber oder Anbieter durch gezielte Informationen auf abstrakte oder konkrete Sicherheitsprobleme und Gefahren hinweisen (I.). Erhöhte Transparenz über Informationen mit Sicherheitsbezug kann ein Gegengewicht zu den mit der Zurück- und Geheimhaltung von Informationen verbundenen Gefahren für die Sicherheit schaffen und so zur Sicherheit von Informationstechnik und IT-Produkten beitragen (II.). Der Zugang zu Informationen erlaubt eine wirtschaftliche Weiterverwendung der Daten, sodass durch die damit ermöglichte Rekombination von Informationen neue (kommerzielle) Sicherheitslösungen entwickelt werden können (III.).

---

[2] Vgl. *Schoch*, AfP 2010, 313 (315); *ders.*, IFG, 2009, Einl. Rn. 109; *Caspar*, DÖV 2013, 371 (371 ff.).

[3] *Quabeck*, Dienende Funktion des Verwaltungsverfahrens und Prozeduralisierung, 2010, S. 225 f.; zum Begriff der Kommunikation § 2 C. II. 3.

[4] *Augsberg*, Informationsverwaltungsrecht, 2014, S. 198.

I. Sicherheit durch staatliche Informationstätigkeit

Informationelles Handeln des Staates ist eine Handlungsform, die nicht erst mit dem Informationszeitalter aktuell wurde, sondern seit jeher praktiziert wird.[5] Staatliche Informationstätigkeit erfüllte schon immer eine Funktion für den Staat. Neben der Aufklärung, Erziehung und politischen Steuerung diente sie der Selbstdarstellung absolutistischer Fürsten oder der Propaganda.

Das Bundesverfassungsgericht hat die Öffentlichkeitsarbeit von Bundesorganen in einer grundlegenden Entscheidung nicht nur für zulässig befunden, sondern deren Notwendigkeit unterstrichen. Aufgabe der staatlichen Öffentlichkeitsarbeit sei es, den Grundkonsens der Bürger mit der vom Grundgesetz geschaffenen Staatsordnung lebendig zu erhalten.[6] Das Volk im Sinne des Art. 20 Abs. 2 S. 1 GG, d. h. die Bürgerschaft, bedarf der hinlänglichen Information, um politische Entscheidungen nach Art. 20 Abs. 2 S. 2 GG in Wahlen und Abstimmungen treffen zu können. Eine verantwortliche Teilhabe der Bürger an der politischen Willensbildung des Volkes setze voraus, dass der Einzelne von den zu entscheidenden Sachfragen, Maßnahmen und Lösungsvorschlägen „genügend weiß, um sie beurteilen, billigen oder verwerfen zu können. Auch dazu vermag staatliche Öffentlichkeitsarbeit einen wesentlichen Beitrag zu leisten."[7] Das Gericht geht in einer späteren Entscheidung auch auf die gewandelte Form der Aufgabenerfüllung ein. Die Öffentlichkeitsarbeit gehe unter heutigen Bedingungen über die Darstellung von Maßnahmen und Vorhaben der Regierung hinaus. Es gehöre in einer Demokratie zur Aufgabe, über wichtige Vorgänge außerhalb und weit im Vorfeld der gestaltenden politischen Tätigkeit zu unterrichten. „In einer auf ein hohes Maß an Selbstverantwortung der Bürger bei der Lösung gesellschaftlicher Probleme ausgerichteten politischen Ordnung ist von der Regierungsaufgabe auch die Verbreitung von Informationen erfasst, welche die Bürger zur eigenverantwortlichen Mitwirkung an der Problembewältigung befähigen."[8] Der Gedanke, dass Informationshandeln die Bürger zu eigenverantwortlichem Handeln befähigen kann, ist infolge seiner allgemeinen Natur nicht nur auf das Informationshandeln der Bundesregierung, sondern auch auf das anderer Staatsorgane erstreckbar.[9]

---

[5] *Bumke*, Die Verwaltung 37 (2004), 3 ff.; *Feik*, Öffentliche Verwaltungskommunikation, 2007, S. 7; allgemein zur Kommunikation zwischen Verwaltung und Bürger *Kaiser*, Die Kommunikation der Verwaltung, 2009, S. 23 ff., 243 ff.

[6] BVerfGE 44, 125 (147).

[7] BVerfGE 44, 125 (147).

[8] BVerfGE 105, 252 (269).

[9] *Rossi*, Möglichkeiten und Grenzen des Informationshandelns des Bundesrechnungshofes, 2012, S. 186.

Während die Rechtsprechung des Bundesverfassungsgerichts ihren Ausgangspunkt im Demokratieprinzip hat, verweist Informationshandeln im administrativen Kontext auf eine Steuerungsressource. Der Staat als „Verwaltungsstaat" ist zwar eine rechtsstaatlich gesetzesbedingt funktionelle Bürokratie, muss sich aber an die gestiegene Bedeutung von Informationen in der Informationsgesellschaft anpassen.[10] Unter den „veränderten kognitiven Bedingungen moderner Gesellschaften" hat die Administrative Wissensmanagement zu betreiben.[11] In der steuerungswissenschaftlichen und kommunikationstheoretischen Forschung wurden schon recht früh auch informationelle Mittel im Kontinuum der staatlichen Steuerungsinstrumente erfasst. Seitdem zählen zu den Steuerungsinstrumenten neben denen des klassischen Ordnungsrechts, also durchsetzbare Geboten und Verbote und finanzielle Instrumente wie finanzielle Transfers, Anreizsysteme und die Schaffung künstlicher Märkte, auch informationelle Instrumente wie Informations- und Öffentlichkeitsarbeit sowie indikative und informative Erklärungen, Pläne und Programme sowie symbolische Belohnungen.[12]

Der Gedanke der Steuerung wird in der Rechtswissenschaft unterschiedlich bewertet.[13] Steuerung durch Information kann angesichts der hier zugrundeliegenden Problematik der Komplexität informationstechnischer Systeme jedoch gerade nicht im Sinne einer missbräuchlichen Einwirkung auf lineare Kausalverläufe verstanden werden. Die Modi des staatlichen Handelns sind im Sicherheitsverwaltungsrecht ohnehin verlagert bzw. erweitert. Staatliche Steuerung findet nicht nur durch hoheitlichen Befehl (Verwaltungsakte) statt, sondern in einem kooperativen Modus durch wissensgestützte persuasive Einwirkung (Informationsakte).[14] Informationen können durchaus als Mittel der Sicherheitsverwaltung begriffen werden, wenn sie für den Empfänger optimal bereitgestellt werden.[15]

Mit dem Zuwachs an Bedeutung, das dem öffentlichen Informationshandeln zukommt,[16] ändert sich das Verständnis des Staates. Dessen Auftreten wandelt sich vom dirigistischen, finalen Regierungshandeln zu einem auf Selbstregulie-

---

[10] *Pitschas*, Allgemeines Verwaltungsrecht als Teil der öffentlichen Informationsordnung, in: Hoffmann-Riem/Schmidt-Aßmann/Schuppert (Hrsg.), Reform des allgemeinen Verwaltungsrechts, 1993, S. 219 (269).

[11] *Augsberg*, Informationsverwaltungsrecht, 2014, S. 196.

[12] *Jann*, Kategorien der Policy-Forschung, 1981.

[13] Kritisch etwa *Lepsius*, Steuerungsdiskussion, Systemtheorie und Parlamentarismuskritik, 1999, S. 4 ff.

[14] Grundlegend zu informationsbezogenen Handlungstypen *di Fabio*, Risikoentscheidungen im Rechtsstaat, 1994.

[15] Vgl. *Eidenmüller*, JZ 2011, 814 (821).

[16] *Schoch*, NJW 2012, 2844 (2844 ff.).

rung setzenden öffentlichen Kommunizierens, das sich am Leitbild des mündigen Verbrauchers[17] und des lernenden Unternehmens orientiert. Begriffe wie der des „kooperativen" oder „kollaborativen" Staates und des „Gewährleistungsstaates" versuchen die veränderte Funktion des Staates begrifflich zu fassen.[18] Nicht zuletzt das Sozialstaatsprinzip kann herangezogen werden, um den Staat als *enabling state* zu konstruieren. Der freiheitliche Sozialstaat kann als organisierender, koordinierender und aktivierender Staat verstanden werden, der das Eigenleben der Gesellschaft voraussetzt und sich darauf beschränkt, diesem geeignete Rahmenbedingungen bereitzustellen, und dabei eine Aktivierungs-, Koordinations- und Organisationsfunktion übernimmt.[19]

Die mit Informationshandeln verfolgten Verwaltungsziele werden vielfältiger. Öffentliche Informationen werden etwa gezielt als Instrument des Verbraucherschutzes eingesetzt,[20] da eine behördliche Warnung, etwa vor einem bestimmten Produkt oder vor Hygienemängeln in Gaststätten, regelmäßig einen Lenkungseffekt bei den Verbrauchern entfaltet (*ruling through signals*)[21]. Die Information dient dabei nicht nur der Vorbereitung von Maßnahmen, sondern ist schon selbst Mittel der Durchsetzung des Rechts. Damit kann Informationshandeln Voraussetzung wirksamer, staatlicher Aufgabenerfüllung sein.[22]

Staatliche Informationstätigkeit kann letztlich mit der Aktivierung der staatlichen Schutzpflicht und der Gewährleistungsverantwortung begründet werden. Aus der staatlichen Informationsverantwortung kann das Gebot folgen, Informationen breitenwirksam zur Verfügung zu stellen.[23] Greifbar wird die Infor-

---

[17] *Becker/Blackstein*, NJW 2011, 490 ff.

[18] *Möllers*, Der vermisste Leviathan, 2008, S. 104; *Schliesky/Schulz* (Hrsg.), Transparenz, Partizipation, Kollaboration – Web 2.0 für die öffentliche Verwaltung, 2012; kritisch *Wewer*, Die Verwaltung 46 (2013), 563 (563 ff.).

[19] Bereits *Heller/Niemeyer*, Staatslehre, 6. Aufl. 1983, S. 230; *Kingreen*, Das Sozialstaatsprinzip im europäischen Verfassungsverbund, 2003, S. 130 f.; zur Koordinierungsnotwendigkeit staatlicher und privater Wissensbestände *Ladeur*, Der Staat gegen die Gesellschaft, 2006, S. 119 ff., 320 ff.

[20] Vgl. dazu *Wollenschläger*, VerwArch 102 (2011), 20 (24 ff.).

[21] *Schuppert*, Nudging: nicht wirklich neu und auch – ohne Kontextualisierung – nicht weiterführend, VerfBlog vom 16.04.2015, online abrufbar, mit Verweis auf *Offe*, Signals and Information as a Resource of Public Policy, 2010, S. 2. Siehe dazu auch *Sunstein*, U.Pa.L.Rev 147 (1999), 613 (613 ff.).

[22] Aktuell werden neue Methoden „wirksamen Regierens" unter dem vom amerikanischen Verfassungsrechtler Cass *Sunstein* und dem Ökonomen Richard *Thaler* geprägten Begriff des *nudging* diskutiert, wonach verhaltensökonomische Erkenntnisse bei der staatlichen Regelsetzung berücksichtigt werden. Siehe dazu kritisch *Eifert*, Nudging: Eine politische Aufgabe, in: Theorie und Praxis der sozialen Arbeit 66 (2015), S. 178 (178 ff.); *Smeddinck*, ZRP 2014, 245 (245 ff.); *Kirchhof*, ZRP 2015, 136 (136 ff.).

[23] *Spiecker gen. Döhmann*, Rechtswissenschaft 2010, 247 (263); *Groß*, Ressortforschung,

mationsverantwortung dann, wenn sie als Grundrechtsvoraussetzungsschutz durch staatliche Informationsvorsorge verstanden wird.[24] Die Legitimation für eine Wissensdistribution kann sich aus der „staatliche[n] Pflicht zur Schaffung der allgemeinen Voraussetzungen für den Gebrauch der Informations- und Kommunikationsgrundrechte“ speisen.[25]

Die hinter dem staatlichen Informationshandeln stehende Logik kann für die Gewährleistung der Internetsicherheit fruchtbar gemacht werden. Gerade auf diesem technischen Gebiet müssen auch durch Bürger, die Nutzer und Anwender sind, informierte Sachentscheidungen getroffen werden. Die Rolle des Staates als kooperativer Part in der Sicherheitsgewährleistung manifestiert sich exemplarisch in Art. 11 Abs. 2 EUV und § 3 Abs. 1 S. 2 Nr. 14 und 15 BSIG. Die Unionsverwaltung pflegt einen offenen, transparenten und regelmäßigen Dialog mit den repräsentativen Verbänden und der Zivilgesellschaft. Das BSI berät und warnt private Hersteller, Vertreiber und Anwender in Fragen der Sicherheit. Es arbeitet dabei „im Verbund mit der Privatwirtschaft “. Informationshandeln kann nicht zuletzt deshalb als legitimes Instrument wirksamer Aufgabenerfüllung angesehen werden, weil die gemeinsame Gewährleistung der Sicherheit ein aufgegebenes Verwaltungsziel ist.[26] Die Veröffentlichung sicherheitsbezogener Informationen ist grundsätzlich geeignet, den Mangel an Eigeninformationen bei Verbrauchern zu reduzieren und diese zu versierteren Risikoentscheidungen zu führen. Unternehmen können dadurch in einen Wettbewerb um sicherere Produkte und Dienstleistungen versetzt werden. Wirkung zeitigen solche Informationen vor allem dann, wenn sie von den Empfängern verarbeitet und internalisiert werden können.[27] Zur Erfüllung der staatlichen Gewährleistungsverantwortung führt das Informationshandeln vor allem dann, wenn die Sicherheit in kritischen Internetinfrastrukturen erhöht wird.

Agenturen und Beiräte – zur notwendigen Pluralität der staatlichen Wissensinfrastruktur, in: Röhl (Hrsg.), Wissen – Zur kognitiven Dimension des Rechts, Die Verwaltung, Beiheft 9, 2010, S. 135 (151 ff.).

[24] *Trute*, Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, VVDStRL 57 (1998), S. 216 (254 f.); vgl. *Hoffmann-Riem*, Enge und weite Gewährleistungsgehalte der Grundrechte?, in: in: Bäuerle/Hanebeck/Hausotter (Hrsg.), Haben wir wirklich Recht?, 2004, S. 53 (56).

[25] *Gröschner*, Transparente Verwaltung: Konturen eines Informationsverwaltungsrechts, in: VVDStRL 63 (2004), S. 344 (365); *Schliesky*/*Hoffmann*/*Luch*/*Schulz*/*Borchers*, Schutzpflichten und Drittwirkung im Internet, 2014, S. 167, 174.

[26] Siehe § 3 A.

[27] *Feiler*, Information Security Law in the EU and the U.S., 2011, S. 86 f.; *Fung*/*Graham*/*Weil*, Full Disclosure: The Perils and Promise of Transparency, 2007, S. 54 ff.

II. Sicherheit durch Transparenz

Die Informationsdistribution dient auch dem Ideal der Publizität, dessen zugrundeliegender Gedanke auch in der Sicherheitsgewährleistung Anwendung finden kann.

Das Ideal der Publizität lässt sich verfassungsrechtlich nachzeichnen. Der Gedanke der staatlichen Transparenz und die Forderung nach der Öffnung des Staates reichen bis in die Antike. Bereits dort war Publizität als Bedingung von Demokratie und Republik bekannt.[28] Die Aufklärung und der Liberalismus des 19. Jahrhunderts verwirklichten das Transparenzideal zum Teil in Judikative und Legislative.[29] Der Bereich der Exekutive, vor allem die Administrative, blieb ungeachtet der zeitgeistlichen Entwicklungen von den Öffnungstendenzen allerdings weitgehend unberührt.[30] Erst die gesetzgeberische Aktivität in den letzten Jahrzehnten, die durch europäische Richtlinien ausgelöst wurde, löste die Administrative immer weiter aus der Arkantradition und ließ sie zunehmend ein dem modernen Leitbild möglichst umfassender Transparenz entsprechenden Verwaltungshandeln realisieren.[31]

Der Transparenzgedanke ist auf europäischer Ebene in einer prägenden Verfassungsnorm verankert. Gemäß Art. 1 Abs. 2 EUV werden Entscheidungen in der Union möglichst offen und bürgernah getroffen. Der Gedanke der Transparenz ist hier als Entscheidungsmaxime zum Ausdruck gebracht.[32] Primärrechtliche Transparenzgebote gelten zudem gemäß Art. 15 Abs. 2 AEUV für den Normsetzungsprozess. Ausdruck des Transparenzprinzips ist für die Eigenverwaltung das Gebot einer „offenen" Verwaltung in Art. 298 Abs. 1 AEUV.

Unter Bezug auf das Grundgesetz kann der Transparenzgedanke anhand des Grundsatzes der Öffentlichkeit diskutiert werden. Dem Grundgesetz kann ein umfassender Grundsatz der Öffentlichkeit entnommen werden.[33] Für die Legislative und das Gesetzgebungsverfahren finden sich ausdrückliche bereichsspe-

---

[28] Vgl. *Gröschner*, Transparente Verwaltung: Konturen eines Informationsverwaltungsrechts, in: VVDStRL, 63 (2004), S. 344.

[29] Dazu *Rossi*, Informationszugangsfreiheit und Verfassungsrecht, 2004, S. 79 ff.

[30] *Weber*, RDV 2005, 243 (244).

[31] Vgl. *Pernice*, Verfassungs- und europarechtliche Aspekte der Transparenz staatlichen Handelns, in: Dix/Franßen/Kloepfer/Schaar/ Schoch (Hrsg.), Informationsfreiheit und Informationsrecht, 2014, S. 17 (18); *Masing*, Transparente Verwaltung, in: VVDStRL 63 (2004), S. 377 (422 ff.); *Wegener*, Der geheime Staat – Arkantradition und Informationsfreiheitsrecht, 2006, S. 124 ff., 390 ff.; kritisch zu einer Rechtsvergleichung, die den staatsorganisatorischen und kulturellen Zusammenhang außer Acht lässt *Möllers*, VerwArch 93 (2002), 22 (53).

[32] *Pechstein*, in: Streinz (Hrsg.), EUV/AEUV, 2. Aufl. 2012, EUV, Art. 1 Rn. 19.

[33] *Lederer*, Open Data, 2015, S. 217.

zifische Öffentlichkeitsvorgaben.[34] Jenseits explizierter Vorgaben können Gebote der Öffentlichkeit im Wege der Auslegung ermittelt werden. So kann die Öffentlichkeit als allgemeiner Verfassungsgrundsatz eingeordnet werden, auch wenn der Grad der normativen Dichte zu Konkretisierungsbedarf führt.[35] Aus der Rechtsqualität als Grundsatz folgt aber ein besonderes Regel-Ausnahme-Verhältnis. Die durch gegenläufige Interessen bedingte Nichtöffentlichkeit ist rechtfertigungsbedürftig und Ausnahmen sind restriktiv auszulegen.[36]

Die hier interessierende Facette verfassungsrechtlicher Offenheit lässt sich am Konzept von Open Government Data nachvollziehen. Der Inhalt von Open Government Data hat viele Bestimmungen erfahren.[37] Begrifflich wird auf die Offenheitskomponente (*open*) und auf den Gegenstand der Öffnung (*government data*) verwiesen.[38] In demokratietheoretischer Tradition kommt dieser Öffnung des Staates ein Eigenwert zu. Als regulative Idee und Ordnungsinstrument verstanden,[39] beinhaltet das Prinzip die Dimensionen Partizipation, Kollaboration und Transparenz.[40] Das Konzept von Open Government erfüllt aber nicht nur eine legitimitätsstiftende Funktion. Es geht auch um eine Involvierung der Bürger und Unternehmen über das staatskonstituierende Beteiligungsminimum hinaus. Die Offenheit von Verwaltungsdaten kann eine spezifisch sicherheitsbezogene Funktion einnehmen, die sich im Vergleich zur Begrenzung von Datenmacht im Datenschutz (1.), anhand der Debatten um die Herstellung von Sicherheit in Software (2.) sowie anhand staatlichen Sonderwissens bei Verschlüsselungen (3.) weiter entfalten lässt.

---

[34] Z. B. Art. 42 Abs. 1 S. 1, Art. 52 Abs. 3 S. 3 oder Art. 82 GG.

[35] BVerfGE 118, 277 (352); *Bröhmer*, Transparenz als Verfassungsprinzip – Grundgesetz und Europäische Union, 2004, S. 38 ff.; die Rechtsöffentlichkeit aus dem Rechtsstaatsprinzip ableitend BVerfGE 103, 44 (63).

[36] *Wegener*, Der geheime Staat – Arkantradition und Informationsfreiheitsrecht, 2006, S. 426; *Lederer*, Open Data, 2015, S. 219.

[37] *Lederer*, Open Data, 2015, S. 40.

[38] Eine Übersetzung als „Regierungsdaten" ist freilich zu eng. Übertragen auf den kontinentaleuropäischen Kontext sind damit Verwaltungsdaten gemeint. Siehe *von Lucke*/*Geiger*, Open Government Data, 2010, S. 2, 6, die auf Daten, Informationen, Wissen und Quellen Bezug nehmen. Vgl. auch *Internet & Gesellschaft Collaboratory* (Hrsg.), Offene Staatskunst, 2010, S. 52 f.

[39] *Schuler*, Online Deliberation and Civic Intelligence, in: Lathrop/Ruma (Hrsg.), Open Government, 2010, S. 91 f.; *BMI*, Open Government Data Deutschland, 2012, S. 25 f.

[40] *Janda*, Open Government, in: Schliesky/Schulz (Hrsg.), Transparenz, Partizipation, Kollaboration, 2012, S. 11 (15).

1. Begrenzung von Datenmacht am Beispiel des Datenschutzes

Im Datenschutz dient das Element der Informationsdistribution dazu, eine Informationsmachtbalance herzustellen und dadurch den Datenschutz zu stärken. Der Datenschutz wird zumeist vom Schutz des Individuums her begriffen. Darüber hinaus hat der Datenschutz einen „gesamthaften Aspekt".[41] Der gesamthafte Aspekt des Datenschutzes betrachtet das eigentliche Regelungsanliegen des Datenschutzes, also Datenmacht zu begrenzen und vor asymmetrischen Informationsbeziehungen zu schützen, unter der Prämisse, dass informationelle Verhältnisse immer auch Machtverhältnisse darstellen.[42] Die gesamtgesellschaftliche Bedeutung des Datenschutzes kommt im Volkszählungsurteil zum Ausdruck,[43] fand Niederschlag in der Datenschutzgesetzgebung[44] und folgt aus der Ableitung des Rechtsstaatsprinzips[45] sowie aus der Staatsaufgabe der Humanisierung von Technik[46].[47]

Informationelle Ungleichgewichte und Informationsasymmetrien werden durch informationelle Gegengewichte austariert und begrenzt.[48] Insbesondere Transparenz kann datenmachtbegrenzende Wirkung haben.[49] So sind zahlreiche Einzelvorgaben zur Transparenz im Datenschutzrecht Ausdruck dieses Gedankens und als Vorbedingung der informationellen Selbstbestimmung zu lesen. In die Datenverarbeitung muss grundsätzlich eingewilligt werden, wobei die Einwilligung nur wirksam ist, wenn sie auf einer freien Entscheidung beruht (Art. 6 Abs. 1 lit. a, 7, 9 Abs. 2 lit. a DS-GVO, sog. *informed consent*). Denjenigen, der Daten verarbeitet, treffen bestimmte Informationspflichten dazu, den Betroffenen über die Umstände der Datenverarbeitung zu unterrichten. Die Information hat in transparenter und verständlicher Form zu erfolgen (Art. 12 DS-GVO). Bestimmte Unternehmen müssen ein Verzeichnis aller Verarbeitungstätigkeiten führen, um die wichtigsten Vorgänge zu dokumentieren (Art. 30

---

[41] *Von Lewinski*, Die Matrix des Datenschutzes, 2014, S. 55.

[42] *Von Lewinski*, Zur Geschichte von Privatsphäre und Datenschutz, in: Schmidt/Weichert (Hrsg.), Datenschutz, 2012, S. 23 ff.

[43] BVerfGE 65, 1 (47, 50 f.); vgl. schon BVerfGE 27, 1 (9).

[44] Etwa in § 1 Abs. 1 Nr. 2 HDSG: „Aufgabe des Gesetzes ist es, die Verarbeitung personenbezogener Daten […] zu regeln, um […] das auf dem Grundsatz der Gewaltenteilung beruhende verfassungsmäßige Gefüge des Staates […] vor einer Gefährdung infolge der automatisierten Datenverarbeitung zu bewahren."

[45] *Steinmüller/Lutterbeck/Mallmann/Harbort/Kolb/Schneider*, Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, 1971, abgedruckt als Anlage 1 zur BT-Drs. VI/3826 vom 07.09.1972, S. 83.

[46] *Kloepfer*, Datenschutz als Grundrecht, 1980, S. 16.

[47] *Von Lewinski*, Die Matrix des Datenschutzes, 2014, S. 55.

[48] Vgl. *Grimm*, JZ 2013, 585 (587).

[49] *Von Lewinski*, Die Matrix des Datenschutzes, 2014, S. 77 f.

DS-GVO). Bei besonders risikobehafteten Datenverarbeitungen ist unter Umständen die Aufsichtsbehörde zu konsultieren (Art. 36 DS-GVO).

Die Transparenzvorschriften erhöhen den allgemeinen Grad des „Informiertseins". Im Bereich der Netz- und Informationssicherheit besteht mangels eines einheitlichen IT-Sicherheitsrechts kein entsprechendes Regelungsregime. Dennoch rechtfertig sich staatliche Informationsgenerierung nur unter dem Aspekt, nicht nur den Staat, sondern auch die Marktgegenseite, d. h. die Kunden eines Unternehmens oder die Betroffenen eines Sicherheitsvorfalls, aufzuklären. Dieses Prinzip kommt besonders bei den Pflichten zur Meldung von IT-Sicherheitsvorfällen zum Ausdruck. Diese Meldepflichten verfolgen neben dem Zweck, den Behörden die Erstellung eines Lagebildes zu ermöglichen und Reaktionsmaßnahmen einzuleiten, Transparenz (*transparency*) herzustellen und für die Sicherheit zu sensibilisieren (*awareness*).[50]

2. Argumente aus der Kryptokontroverse gegen exklusives staatliches Wissen

Noch deutlicher lässt sich die Gefahr exklusiven Wissens über Sicherheit, die durch die Konzentration sensibler sicherheitskritischer Informationen entsteht, am Beispiel der *Key-escrow*-Debatte (Kryptokontroverse) ausmachen. In der Kryptokontroverse geht es darum, ob die Netz- und Informationssicherheit besser durch proprietäres, d. h. exklusives Wissen (hier des Staates) oder durch distribuiertes, d. h. weit verbreitetes Wissen (hier der Anwender und Unternehmen) gewährleistet werden kann. Bei abstrahierter Betrachtung lassen sich Argumente für und gegen Informationsdistribution erkennen.

Die Vereinigten Staaten von Amerika hatten frühzeitig die Schlüsselhinterlegung (*key escrow*) bzw. die Implementierung der Möglichkeit, Nachschlüssel erzeugen zu können, vorangetrieben.[51] Der bei staatlichen Stellen hinterlegte bzw. generierbare Schlüssel sollte so den öffentlichen Zugriff auf kryptografische Verschlüsselungsverfahren und verschlüsselte Inhalte erlauben. Die „Clipper Chip"-Initiative, nach der den Behörden eine Art Generalschlüssel abzugeben gewesen wäre, konnte sich nicht durchsetzen. In einigen Staaten konnte sich (zeitweise) eine Schlüsselhinterlegungspflicht etablieren.[52] In Deutschland wurde 1999 die Kryptodebatte durch die von der Bundesregierung aufgestellten Eckpunkte für die Kryptopolitik vorerst beendet. Die Bundesregierung beab-

---

[50] *Heinickel/Feiler*, CR 2014, 708 (710); *Feiler*, Journal of Internet Law 2011, 1 (18 ff.); Art. 14 Abs. 6 NIS-RL.

[51] *Bizer*, Die Kryptokontroverse, in: Hammer (Hrsg.), Sicherheitsinfrastrukturen, 1995, S. 179 (209); vgl. *Kuner/Hladjk*, Rechtsprobleme der Kryptografie, in: Hoeren/Sieber/Holznagel (Hrsg.), Handbuch Multimedia-Recht, 42. Aufl. 2015, Teil 17, Rn. 86 ff.

[52] Vgl. *Gerhard*, (Grund-)Recht auf Verschlüsselung?, 2010, S. 118.

sichtigte es zu diesem Zeitpunkt nicht weiter, „die freie Verfügbarkeit von Verschlüsselungsprodukten in Deutschland einzuschränken".[53] Die Verwendung von Datenverschlüsselungsprodukten ist in Deutschland weiterhin weitgehend unreguliert.[54] Im Bereich der Telekommunikation unterliegen Nutzer grundsätzlich keinen Beschränkungen. Zwar regelt die Telekommunikations-Überwachungsverordnung (TKÜV) – neben den einfachgesetzlichen Abhör- und Überwachungsbefugnissen – die von den öffentlichen Telekommunikationsanlagenbetreibern einzuhaltenden technischen und organisatorischen Vorkehrungen. Internetprovider und Internetnetzknoten sind aber – außer in Fällen angeordneter Überwachungen – von den Verpflichtungen aus der TKÜV (vgl. § 3 Abs. 2 TKÜV) ausgenommen.[55]

Die Debatte um den staatlichen Zugang zu Schlüsseln ist jüngst wieder neu entfacht worden.[56] Gefordert wird, dass die „Internet systems" „redesigned" werden und dass es einen „government access" zu Informationen, auch verschlüsselten, in Datenspeicher- und Kommunikationssystemen gibt, um die Ermittlungskapazitäten der Sicherheitsbehörden den Bedrohungen im und über das Internet anzupassen. In dem Bericht der Gruppe der führenden Kryptografen und IT-Sicherheitsforscher, die bereits 1997 die massiven Sicherheitslücken der Clipper-Chip-Initiative aufzeigte, wird die Forderung nach einem „exceptional access" zu verschlüsselter Kommunikation mit dem Argument verworfen, sie sei „unworkable in practice", führe zu „enormous legal and ethical questions, and would undo progress on security at a time when Internet

---

[53] Pressemitteilung des Bundesministeriums für Wirtschaft und Technologie und des Bundesministeriums des Innern vom 02.06.1999: Eckpunkte der deutschen Kryptopolitik, abrufbar unter: http://www.fitug.de/news/newsticker/old/1999/newsticker020699224621.html. Gleichwohl heißt es dann aber einschränkend: „Durch die Verbreitung starker Verschlüsselungsverfahren dürfen die gesetzlichen Befugnisse der Strafverfolgungs- und Sicherheitsbehörden zur Telekommunikationsüberwachung nicht ausgehöhlt werden." Der Antwort des Bundesministeriums des Innern auf eine Kleine Anfrage zufolge hat der Kabinettsbeschluss nach wie vor Bestand, BT-Drs. 18/5144, S. 4. Soweit es diesen „berechtigten Stellen" möglich ist, dürften sie „rechtmäßig abgefangene, aber nutzerseitig verschlüsselte Kommunikation im Rahmen des technisch Möglichen […] entschlüsseln."

[54] Zu den wichtigen Ausnahmen wie Ausfuhrbeschränkungen und anderen Rechtsfragen siehe *Kuner/Hladjk*, Rechtsprobleme der Kryptographie, in: Hoeren et al. (Hrsg.), Handbuch Multimedia-Recht, 42. Aufl. 2015, Teil 17 Rn. 14 ff.

[55] *Kuner/Hladjk*, Rechtsprobleme der Kryptographie, in: Hoeren/Sieber/Holznagel (Hrsg.), Handbuch Multimedia-Recht, 42. Aufl. 2015, Teil 17 Rn. 56; vgl. aber § 3 Abs. 2 Nr. 3 TKÜV.

[56] *Comey*, Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?, Speech at the Brookings Institution, 2014, online abrufbar. Für Europa und Deutschland siehe die Antwort der Bundesregierung auf eine Kleine Anfrage BT-Drs. 18/5144, m. w. N.; *Hornung*, MMR 2015, 145 (145).

vulnerabilities are causing extreme economic harm".[57] In der Tat sind neben technischen Detailfragen drei wesentliche Punkte zu berücksichtigen, die das exklusive staatliche Wissen über die Entschlüsselung von Telekommunikation problematisch erscheinen lassen. Erstens schafft das exklusive Wissen über sicherheitskritische Mechanismen wie Verschlüsselung selbst ein Sicherheitsrisiko.[58] Cyberattacken auf Ziele, die Daten konzentrieren, könnten das Ausmaß einer Katastrophe annehmen. Das Informationssystem zur Verwaltung eines derart sensiblen Wissens würde zweitens eine enorme Zunahme an Komplexität bedeuten, vor allem in den betroffenen Produkten und weil eine nicht quantifizierbare Anzahl von Institutionen und Nutzern berücksichtigt werden müsste.[59] Jeder Aufbau eines neuen Systems ist mit Kosten verbunden und das Testen, Administrieren und Programmieren ist in hohem Maße kostenaufwendig. Zu bedenken ist, dass im Bereich der Informationstechnik für die Entwicklung sicherer Technik ein iterativer Review-Prozess notwendig ist.[60] Prinzipiell ist nicht zuletzt die Frage, wer die Systeme, die NIS-relevantes Wissen speichern, kontrolliert und überwacht.

Eine abschließende Aussage zu Gunsten oder zu Ungunsten exklusiven Wissens über die Sicherheit ist zwar nicht möglich. Stets ist aber für die Betrachtung der systemischen Internetsicherheit eine Gesamtrechnung aufzustellen, die

---

[57] *Abelson/Anderson/Bellovin/Benaloh/Blaze/Diffie/Gilmore/Green/Landau/Neumann/Rivest/Schiller/Schneider/Specter/Weitzner*, Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications, Computer Science and Artificial Intelligence Laboratory Technical Report, 2015, S. 1, online abrufbar.

[58] Zum Verhältnis von Vorratsdaten und den Anforderungen an die IT-Sicherheit *Biendl*, Die Vorratsdatenspeicherung in Europa, Deutschland und Bayern, 2011, S. 72 ff., online abrufbar; vgl. exemplarisch für die Gefahren in der Praxis *Hirschfeld Davis*, Hacking of Government Computers Exposed 21.5 Million People, New York Times vom 09.07.2015, online abrufbar; *Abelson/Anderson/Bellovin/Benaloh/Blaze/Diffie/Gilmore/Green/Landau/Neumann/Rivest/Schiller/Schneider/Specter/Weitzner*, Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications, Computer Science and Artificial Intelligence Laboratory Technical Report, 2015, S. 15: „This is a trade-off space in which law enforcement cannot be guaranteed access without creating serious risk that criminal intruders will gain the same access."

[59] Der frühere Leiter der Forschung bei der US-amerikanischen National Security Agency (NSA) beschrieb das Verhältnis von Sicherheit und Komplexität so: „When it comes to security, complexity is not your friend. […] The basic idea is simple: as software systems grow more complex, they will contain more flaws and these flaws will be exploited by cyber adversaries.", in: *Chang*, Is Your Data on the Healthcare.gov Website Secure?, Written Testimony before the Committee on Science, Space and Technology, U.S. House of Representatives, 2013, online abrufbar.

[60] Im kryptografischen Needham-Schroeder-Protokoll, das 1978 veröffentlicht wurde, fand man erst 1995, 17 Jahre später, Sicherheitslücken. Siehe *Gavin Lowe*, Information Processing Letters 1995, 131 ff., online abrufbar.

nicht nur die kurzfristigen geringfügigen und taktischen Vorteile berücksichtigt, sondern die strukturellen Gefahren des Informationsmanagements beachtet. Das staatliche Wissen über eine hochkritische Sicherheitslücke kann durch Angreifer missbraucht werden. Die Herstellung von Öffentlichkeit auch zu den Ergebnissen der Informationsgenerierung erlaubt hier ein Stück weit die Beobachtung der Beobachter und beugt dem Verletzungsrisiko vor. Das Prinzip der Dekonzentration von Datenmacht durch Offenheit kann grundsätzlich ein weiterer Beitrag zur Gewährleistung der Internetsicherheit sein.

3. Transparenzgedanke in der Debatte um Freie Software

Die Frage der Transparenz und Offenheit findet eine parallele Diskussion im Streit um die Frage, ob IT-Sicherheit besser durch Freie oder besser durch proprietäre Software gewährleistet werden kann.[61] Zwei Sicherheitsphilosophien treffen hier aufeinander, die sich beschreiben lassen als *security through transparency* auf der einen Seite und als *security through obscurity* auf der anderen Seite.[62]

Der Ansatz der Freien Software zeichnet sich neben anderen Merkmalen dadurch aus, dass der Quellcode des Programms offengelegt wird.[63] Das Gegenstück zu Freier Software ist proprietäre Software. Der Quellcode ist nicht frei, d. h. nicht offengelegt, und seine Verbreitung grundsätzlich lizenzrechtlich nicht gestattet. Die Unterscheidung folgt der Historie der Softwareentwicklung, -verbreitung und -verwendung. In den 1960er-Jahren entstand an den amerikanischen Universitäten eine akademische Hackerkultur, in der die Programmierer Software inkrementell verbesserten und so Code und Wissen austauschten. Es

---

[61] Am Beispiel von Browsern *Hunziker*/*Rihs*, DuD 2006, 6 (6 f.); aktuell Zehnter Zwischenbericht der Enquete-Kommission „Internet und digitale Gesellschaft" – Interoperabilität, Standards, Freie Software, 2013, BT-Drs. 17/12495, S. 22 ff., 34 ff.

[62] Vgl. *Feiler*, Journal of Internet Law 2011, 1 (18 ff.); *Shostack*/*Stewart*, The New School of Information Security, 2008, S. 68 ff.; *Fung/Graham/Weil*, Full Disclosure: The Perils and Promise of Transparency, 2007, S. 39 ff.

[63] Zu den vier Freiheiten Freier Software gehören die Freiheit, das Programm für jeden Zweck zu verwenden, die Freiheit, das Programm zu untersuchen und an individuelle Bedürfnisse anzupassen, die Freiheit, Kopien des Programms weiterzugeben, und die Freiheit, das Programm zu verändern und die veränderte Version zu veröffentlichen. Für die Freiheiten ist die Offenlegung des Quellcodes unabdingbar, vgl. *Free Software Foundation*, Inc., GNU Operation System, The Free Software Definition, abrufbar unter: http://www.gnu.org/philosophy/free-sw.en.html. Regelmäßig wird auch der weniger ideologisch konnotierte Begriff Open-Source-Software synonym gebraucht. Um der Verwirkung der Begriffe vorzubeugen, werden zudem auch Begriffe wie Organic Software oder Ethical Software verwendet, vgl. *Schießle*, Free Software, Open Source, FOSS, FLOSS – same same but different, Blogbeitrag vom 11.05.2012, online abrufbar. Freie Software ist nicht mit Freeware zu verwechseln, mit der kostenlose Software gemeint ist.

entwickelte sich „eine Kultur der gegenseitigen Hilfe und des freien Austausches“.[64] Später, in den 1970er-Jahren, wurde Software zu einem bedeutenden (verknappten) Wirtschaftsgut und die Unternehmen machten einen urheberrechtlichen Schutz für ihre Entwicklungen geltend und führten Lizenzverträge mit den Anwendern ein, mit denen der Gebrauch der Programme, insbesondere die Weitergabe und Veränderbarkeit, beschränkt wurde. Als Folge arbeiteten die Softwareentwickler isoliert und unabhängig voneinander an oftmals gleichgelagerten Problemen. Der damals am Massachusetts Institute of Technology (MIT) tätige Programmierer Richard Stallman nahm dies zum Anlass das unter dem Namen GNU[65] bekannte Betriebssystem zu entwickeln, welches später mit Linus Torvalds zum GNU/Linux-System weiterentwickelt wurde. Die Software zeichnet sich durch die GNU General Public License (GPL) und andere freie Dokumentationslizenzen aus, die urheberrechtlich jede Änderung, Erweiterung oder Ableitung dauerhaft erlauben und die Software frei verfügbar halten.[66]

Aufgrund der beschriebenen Eigenschaften und Lizenzmodelle wird der Freien Software häufig eine höhere Sicherheit zugesprochen.[67] Auf die Sicherheit wirkt sich der Zugang zum Quellcode dadurch aus, dass dieser durch Experten auf Sicherheitslücken hin überprüft werden kann. Detektierte Schwachstellen können korrigiert werden. Die Sicherheit eines Produkts kann dadurch insgesamt so gehärtet werden, dass auch dessen Einsatz in sicherheitskritischen Umgebungen möglich ist. Etwaige Hintertüren, d. h. in die Software eingebaute Programmbestandteile, die es ermöglichen, unter Umgehung der regulären Zugriffssicherung Zugriff zu Programm und Daten zu erlangen (sog. *backdoors*), können durch die Untersuchungsmöglichkeit aufgedeckt werden. Dagegen ist bei proprietärer Software eine Codeanalyse zur Detektion von Schwachstellen von außen grundsätzlich nicht möglich, sodass der Nutzer die Sicherheitsrisiken einer Software kaum bewerten kann. Der Nutzer ist dadurch abhängig von den Fehlerbehebungsintervallen und Produktzyklen des Herstellers.[68] Infolge von

---

[64] *Die Beauftragte der Bundesregierung für Informationstechnik* (Hrsg.): Migrationsleitfaden. Leitfaden für die Migration von Software, Version 4.0, 2012, S. 19, online abrufbar.

[65] GNU steht für das rekursive Akronym „GNU’s not UNIX“.

[66] Die Vertreterin der Lizenz ist die ebenfalls von Richard *Stallmann* 1985 gegründete Free Software Foundation (FSF). Die aktuelle Version ist die GNU General Public License, Version 3, 29. Juni 2007, abrufbar unter: http://www.gnu.org/licenses/gpl-3.0.

[67] Enquete-Kommission „Internet und digitale Gesellschaft“, Zehnter Zwischenbericht – Interoperabilität, Standards, Freie Software, 2013, BT-Drs. 17/12495, S. 27; *BSI*, Freie Software (FLOSS: Freie, Libre und Open Source Software), Strategische Positionen des BSI zu Freier Software, abrufbar unter: https://www.bsi.bund.de/DE/Themen/weitereThemen/Freie Software/freiesoftware_node.html.

[68] *Die Beauftragte der Bundesregierung für Informationstechnik* (Hrsg.): Migrationsleitfaden. Leitfaden für die Migration von Software, Version 4.0, 2012, S. 20.

Nichtveröffentlichungsvereinbarungen kann es sogar vorkommen, dass Sicherheitsforscher die ihnen bekannten Sicherheitslücken einer Software nicht veröffentlichen dürfen.

Die Argumentation für Freie Software spricht überwiegend für ein allgemeines Prinzip zugunsten der staatlichen Offenheit und Transparenz auch im Bereich Netz- und Informationssicherheit.[69] Es gibt jedoch strukturelle und systemische Dysfunktionen, die keinesfalls außer Acht gelassen werden dürfen.[70] Denn die Kenntnis von Sicherheitslücken kann unter bestimmten Bedingungen auch nicht zu ihrer Behebung eingesetzt werden, sondern zu Zwecken, die den Schutzzielen der IT-Sicherheit gegenläufig sind, wie etwa kriminellen Zwecken. Eine bekanntgewordene Sicherheitslücke kann außerdem dann weiterhin ausgenutzt werden, wenn die Freie Software nicht ständig weiterentwickelt wird. Eine pauschale Bevorzugung der einen oder der anderen Variante ist nach allem kaum möglich. Gleichwohl macht die Debatte um Freie Software deutlich, dass sich Offenheit und Sicherheit nicht prinzipiell von vorneherein ausschließen. Offenheit kann sogar die Sicherheit stärken.

III. Sicherheit durch Informationszugang und -weiterverwendung

Eine besondere Ausprägung der staatlichen Transparenz ist der Zugang zu Informationen. Denn neben dem aktiven Informationshandeln entscheidet der Zugang zu staatlichen Informationen „über den Grad der Informiertheit im Rahmen der Cybersicherheit".[71]

Durch Art. 41 Abs. 2 lit. b, 42 GRCh und Art. 15 Abs. 3 AEUV ist das Teilhaberecht an Verwaltungsinformationen zur grundrechtlichen Anerkennung gelangt.[72] Das Grundgesetz sieht kein ausdrückliches Grundrecht auf Informationszugang vor. Die dem Paradigmenwechsel der Öffnung des Staates Rechnung tragende Verfassungsinterpretation, nach der aus Art. 5 Abs. 1 S. 1 2. Hs. GG ein Grundrecht auf Informationsfreiheit abzuleiten sei, ist allerdings im Vordringen befindlich.[73] Das Informationsfreiheitsgesetz des Bundes und die der

---

[69] Die Argumentation bezieht sich lediglich auf die Sicherheit und betrifft nicht die strategische, technische und wirtschaftliche Beurteilung der Anpassbarkeit, Verwendungsmöglichkeit, Weitergabe, Hersteller- und Dienstleisterbeziehungen, Qualität, Kosten, Interoperabilität, die möglichen Geschäftsmodelle, Haftung und Gewährleistung, Nutzeranforderungen etc. der Softwaretypen.

[70] Zur Gegenposition etwa *Microsoft*, Linux im Handel – Was jeder Händler wissen sollte, Whitepaper 2001, Punkt 7.

[71] *Bötticher*, Open Source Intelligence, in: Lange/dies. (Hrsg.), Cyber-Sicherheit, 2015, S. 181 (191 f.).

[72] *Claasen*, Gute Verwaltung im Recht der Europäischen Union, 2008.

[73] Siehe § 5 C. I. 2.

Länder auf einfachgesetzlicher Ebene stehen außerdem für eine Bestätigung der Entwicklung des zunehmenden Informationszugangs.

Durch die Informationszugangsfreiheit kommt dem Staat die Stellung als Informationsmittler zu. Die Rolle des Staates als Informationsintermediär ergibt sich insbesondere daraus, dass der Begriff der „amtlichen Information" nach § 1 IFG nicht voraussetzt, dass der Bund Urheber der Information ist. Vielmehr ist die Herkunft der Information unbeachtlich. Lediglich der Zweck der Information ist erheblich, d. h., sie muss in Erfüllung einer öffentlichen Tätigkeit angefallen sein. Erfasst sind somit auch die behördlich gespeicherten Daten, die zuvor von Privaten generiert wurden.[74] Die Informationsfreiheit zielt mit der kognitiven Öffnung des Staates auf die Neudistribution sowohl staatlichen als auch privaten Wissens und hebt damit die hoheitliche Monopolisierung von Informationen auf.[75]

Einen ganz praktischen, wenn auch eher indirekten Nutzen könnte der Zugang zu Informationen, die bei der nationalen NIS-Behörde vorliegen, haben, wenn der durch einen IT-Angriff oder Fehler in einem IT-Produkt Geschädigte in einem zivilrechtlichen Haftungsprozess für die ihm obliegende Darlegungs- und Beweislast auf beim BSI gesammelte Informationen zurückgreifen könnte. Die Verteilung dieser Last stellt eines der größten Hindernisse für den Geschädigten dar, da er kaum Einblicke in die Vorgänge beim Schädiger hat und auch sonst häufig über zu wenig relevante IT-forensische Informationen verfügt. Die Rechtsprechung kennt bei der deliktischen Haftung zwar wie im Produkthaftungsrecht Beweiserleichterungen für den Nachweis der Verletzung einer objektiven Verkehrspflicht, die zum Teil bis zur Umkehr der Beweislast für die Fehlerfreiheit bei In-Verkehr-Bringen eines Produkts reichen.[76] Der Geschädigte hat dennoch grundsätzlich den Schaden und die Ursächlichkeit nachzuweisen. Dem Geschädigten obliegt demnach der Beweis der kausalen Rechtsgutverletzung, des Produktfehlers sowie der Nachweis, dass der Produktfehler aus dem Organisationsbereich des Schädigers herrührt.[77] Im Bereich der IT-Sicherheit ist die Beweisführung hier häufig nicht möglich.[78] Der Zugriff auf Informationen beim BSI über Auskunftsverlangen nach dem IFG könnte für dieses Problem Abhilfe schaffen.

---

[74] *Steffen Augsberg*, Der Staat als Informationsmittler – Robin Hood oder Parasit der Wissensgesellschaft, DVBl. 2007, 733 (739).

[75] *Pitschas*, Allgemeines Verwaltungsrecht als Teil der öffentlichen Informationsordnung, in: Hoffmann-Riem/Schmidt-Aßmann/Schuppert (Hrsg.), Reform des Allgemeinen Verwaltungsrechts, 1993, S. 219 (256); *Augsberg*, DVBl. 2007, 733 (739).

[76] *Sprau*, in: Palandt, BGB, § 823 Rn. 183.

[77] *Foerste*, in: ders./v. Westphalen, Produkthaftungshandbuch, 3. Auflage 2012, § 30 Rn. 29 ff.; *Spindler*, in: BeckOK/BGB, 37. Edition 2013, § 823 Rn. 553.

[78] *Spindler*, CR 2016, 297 (312).

Neben der Informationsdistribution in Form des Zugangs zu amtlichen Informationen ist die private Weiterverwertung von Informationen des öffentlichen Sektors Teil der Öffnung der Verwaltung und der multipolaren Wissensvermittlung des Staates.[79] Die Idee der freien Verwendung von zugänglichen Informationen richtet sich vor allem darauf zu ermöglichen, dass neue marktfähige Mehrwertprodukte und -leistungen erstellt werden können. Ein neuer Wert kann Informationen durch die Herauslösung aus ihrem bisherigen Kontext, durch Rekombination sowie durch Herstellung neuer Bezüge zu ihnen zukommen.[80] Dieses Wertschöpfungspotenzial für die innovative Nutzung von Informationen wird vor allem für Dienstleistungen und Produkte in der Informations- und Kommunikationstechnologie gesehen.[81]

B. Aktives Informationshandeln

Aktive staatliche Informationstätigkeit ist die von Amts wegen unternommene Distribution von Informationen. Informationen werden Rezipienten in der Annahme mitgeteilt oder „aufgedrängt“[82], sie würden passiv wahrgenommen oder aus ihnen würde Nutzen gezogen. Es kann zwischen öffentlichkeits- (I.) und individualbezogenem (II.) Informationshandeln unterschieden werden.[83]

I. Öffentlichkeitsbezogene Informationstätigkeit

Öffentlichkeitsbezogenes Informationshandelns richtet sich an einen unbestimmten Adressatenkreis.[84] Bei solchen Publikumsinformationen sind aufgrund der möglichen Eingriffsintensität je nach Handlungsform Anforderungen

[79] *Ino Augsberg*, Informationsverwaltungsrecht, 2014, S. 214 f.

[80] *Masing*, Transparente Verwaltung, in: VVDStRL 63 (2004), S. 377 (393).

[81] *Wiebe*, Zugang zu und Verwertung von Informationen der öffentlichen Hand, in: Metzger/Wimmers (Hrsg.), DGRI Jahrbuch 2014, 2015, Rn. 364; vgl. schon *Europäische Kommission*, Grünbuch über die Informationen des öffentlichen Sektors in der Informationsgesellschaft, KOM(1998) 585; zu möglichen Geschäftsmodellen der Informationsweiterverwendung *Podszun*, Die Marktordnung für Public Sector Information: Plädoyer für eine wettbewerbsorientierte Auslegung der Richtlinie, in: Dreier/Fischer/van Raay/Spiecker gen. Döhmann (Hrsg.), Informationen der öffentlichen Hand – Zugang und Nutzung, 2016, S. 335 (336 ff.).

[82] Diese Kategorie stammt aus dem Datenschutzrecht. Dort beschreibt der Begriff den Fall, dass eine verantwortliche Stelle Informationen erhält, ohne diese nachgefragt zu haben, *Spiecker gen. Döhmann*, Rechtswissenschaft 2010, 247 (272); vgl. *Tinnefeld/Buchner/Petri*, Einführung in das Datenschutzrecht, 8. Aufl. 2012, S. 499 ff.

[83] *Kloepfer*, Informationsrecht, 2002, § 10, Rn. 79 ff.; vgl. *Schoch*, Entformalisierung staatlichen Handelns, in: Isensee/Kirchhof (Hrsg.), HbStR III, 3. Aufl. 2005, § 37, Rn. 74.

[84] *Schoch*, VBlBW 2014, 361 (362).

an die Zulässigkeit und die Qualität des Informationshandelns zu stellen (1.). Die Kategorisierung der Handlungs- und Erscheinungsformen hat Bedeutung für die Eingriffsintensität einer Maßnahme, aber auch für die jeweilige kognitive Dimension und die mögliche Steuerungswirkung einer Information. Ein Kanon ist weder abschließend gesetzlich festgelegt, noch lässt sich die jeweilige Form stets dem Gesetzestext entnehmen. Aus Beispielen in der Rechtsprechung lassen sich Fallgruppen bilden. So hatte sich die Rechtsprechung mit amtlicher Berichterstattung[85], Unterrichtung[86], behördlicher Aufklärung[87], Empfehlung[88] und der amtlichen Warnung[89] auseinanderzusetzen.[90] Dabei bleibt jedoch jede Einordnung stets der kontextbezogenen Beurteilung im Einzelfall vorbehalten. Die Informationstätigkeit ist weniger nach der äußeren Erscheinungsform als vielmehr nach der inhaltlichen Zielrichtung zu bestimmen. Das Spektrum reicht von einer aufklärenden Transparenzmaßnahme ohne Lenkungswillen bis hin zu bewusst Einfluss nehmenden Empfehlungen oder Warnungen. Für den Bereich der Netz- und Informationssicherheit reicht das Instrumentarium von allgemeiner Aufklärung über Sicherheitsprobleme einschließlich der Information über Sicherheits- und Datenschutzverletzungen (2.) über die Veröffentlichung von Sicherheitsanforderungen und Ergebnissen aus Produktuntersuchungen (3.) sowie Warnungen vor Sicherheitslücken und anderen Gefahren (4.) bis hin zur Empfehlung von Sicherheitsprodukten (5.).

1. Allgemeine Anforderungen an Publikumsinformationen

Soweit Publikumsinformation nicht grundrechtsneutral ist, bedarf es für eine Informationstätigkeit grundsätzlich einer Rechtsgrundlage (a). Zur Rechtmäßigkeit der Information gehören auch Anforderungen an die Qualität der Information (b).

a) Erfordernis der Rechtsgrundlage

Die Publikumsinformation ist die amtliche Versorgung der Öffentlichkeit mit Informationen.[91] Die Beschreibung staatlichen Informationshandelns als „Pub-

[85] BVerfGE 113, 63, siehe auch NJW 2005, 2912.

[86] RhPfVerfGH, NVwZ 2008, 897.

[87] BVerfG, NJW 2011, 511, siehe auch ZUM 2010, 957 m. Anm. *Ladeur*, der den Charakter der Äußerung der Bundeszentrale für politische Bildung im gegebenen Fall privatrechtlich bewertet.

[88] VGH Kassel, NJW 1995, 2371.

[89] BVerfGE 105, 279, siehe auch NJW 2002, 2626, bestätigt durch EGMR, NVwZ 2010, 177.

[90] Vgl. zur Fallgruppenbildung auch *Schoch*, VBlBW 2014, 361, 364 ff.

[91] *Schoch*, AfP 2010, 313 (315); *Guckelberger*, Rechtliche Anforderungen an die aktive

likumsinformation“ oder „Öffentlichkeitsarbeit“ darf nicht als harmloser Umgang mit Informationen missverstanden werden.[92] Sowohl intendierte als auch nicht intendierte Steuerungseffekte (Spill-over-Effekte) der Kommunikation können grundrechtsverletzende Wirkungen zeitigen. Aus diesem Grund beschäftigte sich die rechtsdogmatische Debatte mit der Eingriffsqualität von staatlichen Informationsakten und der Erforderlichkeit und Bestimmtheit der Eingriffsgrundlage.[93] Die Gesetzgeber sind dementsprechend zunehmend dazu übergegangen, die Voraussetzungen für die Information der Öffentlichkeit ausdrücklich zu regeln. Es haben sich zudem verschiedene Grundsätze hinsichtlich der Zulässigkeit von Informationshandeln herausgebildet.

Die grundrechtsneutrale oder ausgestaltende Informationstätigkeit erfordert grundsätzlich keine besondere gesetzliche Ermächtigung, soweit sie im Rahmen der allgemeinen Behördenbefugnis und Zuständigkeit erfolgt und von der Aufgabenzuweisungsnorm gedeckt ist.[94] Bei einem informationellen Grundrechtseingriff bedarf das staatliche Informationshandeln nach dem Grundsatz des Gesetzesvorbehalts einer Ermächtigungsgrundlage.[95] Insbesondere der Schutzbereich von Art. 12 GG, der den Schutz auf verzerrungsfreien Wettbewerbs umfasst, kann durch Informationseingriffe verletzt werden.[96] Für das behördliche Informationshandeln ist dies anerkannt.[97] Für die regierungsamtliche Informationstätigkeit soll dagegen auch bei mittelbaren Eingriffen die Rechtsgrundlage in der ungeschriebenen Aufgabe der Staatsleitung liegen können.[98]

b) Qualität der Information

Die Rechtmäßigkeitsanforderungen des Informationshandelns beziehen sich neben der Frage der Befugnis zum Informationshandeln als solcher auf die die Qualität der Information. Vor allem sind stets die Gebote der Sachlichkeit und Richtigkeit der Informationen und Warnungen sowie das Verhältnismäßig-

---

Informationsvorsorge des Staates im Internet, in: Hill/Schliesky (Hrsg.), Die Vermessung des virtuellen Raums, 2012, S. 73 ff.

[92] *Feik*, Öffentliche Verwaltungskommunikation, 2007, S. 9.

[93] *Gusy*, NVwZ 2015, 700 (701).

[94] BVerfGE 105, 279 (304), hält ein Gesetz schon aus tatsächlichen Gründen nicht für sinnvoll; *Gusy*, NVwZ 2015, 700 (701).

[95] BVerfGE 113, 63 (74 ff.); BVerwG, NJW 2006, 1303 (1304).

[96] BVerfGE 105, 252 (265); *Spiecker gen. Döhmann*, Rechtswissenschaft 2010, 247 (266).

[97] Anders OVM Münster NWVBl. 2010, 355 (356); OVG Bremen, NJW 2010, 3738 (3738); *Schoch*, EuZW 2011, 388 (393).

[98] BVerfGE 105, 252 (268 f.); BVerfGE 105, 279 (301); EGMR, NVwZ 2010, 177; BVerfG, ZUM 2010, 957 (m. Anm. *Ladeur)*: Die Bundeszentrale für politische Bildung dürfe als nicht rechtsfähige Anstalt im Geschäftsbereich des Bundesministeriums des Innern die „Aufgabe der Staatsleitung“ für einen informationellen Eingriff heranziehen.

keitsprinzip zu beachten. Das auf den Inhalt der Information bezogene Sachlichkeitsgebot betrifft sowohl die Darstellung der Fakten als auch die grundsätzlich zulässigen Wertungen.[99] Das Richtigkeitsgebot fordert, dass die Tatsachen einwandfrei erhoben und zusammengestellt wurden, mithin zutreffend sind. Eine Verzerrung, Verfälschung oder unangemessene Dramatisierung, auch durch die Art und Weise der Darstellung, verbietet sich.[100] Das Übermaß- und Willkürverbot gilt wie für jedes andere Handeln staatlicher Einrichtungen.[101]

Für den technischen geprägten Bereich der Sicherheit von Netz- und Informationssystemen ist es grundsätzlich unproblematisch, die „Wahrheit" als Kriterium der Eingriffsqualität heranzuziehen. Der die Rechtsordnung durchziehende Wahrheitsgrundsatz ist an sich nicht problematisch, weil die Rechtsordnung auf die Ermöglichung eines hohen Maßes an markterheblichen Informationen und damit auf Markttransparenz zielt. Dementsprechend schützt Art. 12 GG „nicht vor der Verbreitung zutreffender und sachlich gehaltener Informationen am Markt, die für das wettbewerbliche Verhalten der Marktteilnehmer von Bedeutung sein können, selbst wenn die Inhalte sich auf einzelne Wettbewerbspositionen nachteilig auswirken".[102] Das Wahrheitskriterium bringt im Verbraucherschutz aber dann Schwierigkeiten in sich, wenn der staatliche Kommunikationsakt einen über den Inhalt einer Mitteilung hinausreichenden Informationswert aufweist.[103]

2. Aufklärung zur Sensibilisierung für Sicherheitsprobleme

Die allgemeine Wissensvermittlung wird über die Aufklärung vorgenommen, die Teil der schlicht hoheitlichen Öffentlichkeitsarbeit ist und keinen bestimmten Adressatenkreis voraussetzt. Die Aufklärung ist im Grundsatz auf die Be-

---

[99] BVerfGE 105, 279 (295): keine „diffamierenden oder verfälschenden Darstellungen"; BVerfGE 105, 252 (271): keine „unsachlichen oder herabsetzenden Formulierungen".

[100] BVerfGE 113, 63 (65); zum allgemeinen Verbot staatlicher Desinformation und denkbarer Ausnahmen *Ingold*, Desinformationsrecht: Verfassungsrechtliche Vorgaben für staatliche Desinformationstätigkeit, 2011, S. 76 ff., 90 ff.

[101] BVerfGE 113, 63 (66 ff.). Dass das BSI Empfehlungen ausspricht, an die es sich selbst nicht hält, und zudem sachlich falsche Empfehlungen ausspricht, belegt exemplarisch: http://www.golem.de/news/mindeststandards-bsi-haelt-sich-nicht-an-eigene-empfehlung-1310-102042.html.

[102] BVerfGE 105, 252 (265).

[103] Dies ist etwa bei verbraucherrechtlichen „Ekellisten" der Fall, in denen Aufsichtsbehörden Fotografien im Gaststättenbereich veröffentlichen. Die Suggestivkraft von Bildern und die situativen Bedingungen können den „Wahrheitsgehalt" relativieren. *Augsberg*, Informationsverwaltungsrecht, 2014, S. 205 weist auf diese spezifisch mediale Logik der „Aufmerksamkeitsökonomie" hin.

wusstseinsbildung gerichtet.[104] Sie soll zu einer kritischen Auseinandersetzung mit Problemlagen anregen und dazu befähigen, relevante Gesichtspunkte bei Entscheidungen zu berücksichtigen. Es geht darum, etwaige „Unwissenheit oder ungenügende Kenntnis über etwas" zu „beseitigen".[105] Allgemeines Aufklärungsziel ist die Sensibilisierung hinsichtlich bestimmter Sicherheitsprobleme. Damit verbunden ist die Absicht, der Adressat einer Information möge sein Verhalten durch freiwillige Vernunft und Einsicht ändern.[106] Gegenstand der Aufklärung ist die Vermittlung von Sachinformationen. Die grundrechtsdogmatische Diskussion bezieht sich zumeist auf die Frage, inwiefern Aufklärungshandeln Wertungen aussprechen darf und inwieweit die Form von anderen grundrechtseingreifenden Handlungsformen abzugrenzen ist.[107]

Als Teil der Aufklärungsarbeit können die Berichte der NIS-Behörden (a), die Stellungnahmen der Datenschutzaufsichtsbehörden (b) und die Information über Sicherheitsvorfälle durch die NIS-Behörden verstanden werden (c).

a) Berichte der NIS-Behörden

Die NIS-Richtlinie sieht keine der Aufklärung der Öffentlichkeit dienenden Berichtspflichten vor. Allerdings bestehen einfachgesetzlich Berichtspflichten für das BSI (aa) und die Bundesnetzagentur (bb). Unionsrechtlich vorgesehen sind die Tätigkeitsberichte der Datenschutzaufsichtsbehörden (cc).

aa) Bericht des Bundesamts für Sicherheit in der Informationstechnik

Das BSI berichtet gemäß § 13 BSIG dem aufsichtsführenden Bundesministerium des Innern (BMI) über seine Tätigkeit. Der Bericht dient aber nicht nur dem Tätigkeitsnachwies des Bundesamtes. Die relevanten Informationen sollen in die Sitzungen des Nationalen Cyber-Sicherheitsrates einfließen. Ausweislich des Wortlauts dient die Berichtspflicht darüber hinaus der Aufklärung der Öffentlichkeit. Der Gesetzgeber erkennt damit die zentrale Rolle der Sensibilisierung für das Thema IT-Sicherheit an.[108] Hinsichtlich der Internetsicherheit eignet sich Aufklärung zur Sensibilisierung sowohl der Betreiber und Anbieter als

[104] *Gröschner*, DVBl. 1990, 619 (620), differenziert. Öffentlichkeitsarbeit sei auf die Willensbildung gerichtet, Aufklärung, Empfehlung, Warnung auf die Bewusstseinsbildung des Einzelnen; vgl. *Kloepfer*, Informationsrecht, 2002, § 10 Rn. 81, der in der staatlichen Öffentlichkeitsarbeit einen Beitrag zur Meinungsbildung sieht.

[105] *Feik*, Öffentliche Verwaltungskommunikation, 2007, S. 23.

[106] *Feik*, Öffentliche Verwaltungskommunikation, 2007, S. 24.

[107] Etwa *Brandt*, Umweltaufklärung und Verfassungsrecht, 1994, S. 91 f.

[108] IT-Sicherheitsgesetz, Gesetzesbegründung, BT-Drs. 18/4096, S. 55; eine weitere jährliche Berichtspflicht des BSI ist in § 5 Abs. 10 BSIG statuiert. Diese soll den Innenausschuss des Deutschen Bundestages hinsichtlich der Informationstechnik in der Bundesverwaltung

auch der Nutzer. Das Instrument der Aufklärung bietet sich vor allem deshalb an, weil ein Großteil der Angriffe auf die Sicherheit bereits durch Standardsicherungsmaßnahmen abgewehrt werden kann. Die Sensibilisierung durch allgemeine Informationen über Gefährdungslagen kann schon darüber Wirkung erzielen, dass einfache Maßnahmen ergriffen und leicht umsetzbare Hinweise angenommen werden.

Ein höheres Sicherheitsbewusstsein kann eine allgemein höhere Sicherheitserwartung der Anwender von IT-Produkten zur Folge haben. Eine höhere Erwartung kann in haftungsrechtlicher Sicht zur Begründung einer Verkehrssicherungspflicht, nach der nur Sicherungsmaßnahmen zu treffen sind, die der Verkehr erwarten kann, führen. Die damit verbundene Hersteller- und Anbieterhaftung kann zusätzlich Anreize für die Herstellung sicherer IT-Produkte mit sich bringen.

Fraglich ist aber, ob die Berichtspflicht des BSI ein geeignetes und damit verhältnismäßiges Mittel zur Erreichung des Ziels bezeichnet. Berichtspflichten sind primär ein Mittel zur Aufsicht von Behörden, sie sind, wie auch in § 13 BSIG vorgesehen, in kalendarischen Zyklen zu erstatten. Der Bereich der Netz- und Informationssicherheit ist hingegen anlassgetrieben. Typischerweise werden im Feld der IT-Sicherheit Informationen durch IT-Sicherheitsunternehmen oder die Verbände zeitnah und anlassbezogen publiziert. Es bedarf darüber hinaus proaktiver Einzelfallinformation über Sicherheitslagen, die sich über einen begrenzten Zeitraum entwickelt haben und denen nur über Austausch von Analyse und Wissen begegnet werden kann.[109] Soll die Aufklärung wirksam sein und zu Schutzmaßnahmen befähigen, kann sie sich nicht der Schnelllebigkeit der Materie entziehen. Anders als bei anderen zyklisch anfallenden Informationspflichten kann der Rhythmus auch nicht damit begründet werden, dem Bericht komme, wie bei den jährlichen „Bemerkungen" des Bundesrechnungshofes nach § 97 BHO, eine Entlastungsfunktion zu. Die Aufklärung der Öffentlichkeit dient aber gleichsam der allgemeinen Sensibilisierung, die über anlassbezogene, punktuelle Informationen hinausgeht. Sie dient als Anregung dazu, sich mit grundlegenden Phänomenen der Thematik zu beschäftigen. Insofern ist an die Wirksamkeit der Berichtspflicht nicht der Maßstab anzulegen, wie er an Informationshandeln zu legen ist, das darauf abzielt, konkrete Sicherheitsprobleme zu lösen. Die Berichtspflicht ist demnach grundsätzlich geeignet, die Öffentlichkeit aufzuklären.

---

zum einen über die Anwendung und Umsetzung der Vorschrift informieren, zum anderen über die Bedrohungslage und technische Entwicklung, vgl. BT-Drs. 16/13259, S. 7.

[109] Zur Kritik siehe Stellungnahme des FIfF zum IT-Sicherheitsgesetz der Bundesregierung vom 17.12.2014, S. 13, online abrufbar; vgl. auch Entschließungsantrag zur dritten Beratung des Gesetzentwurfs der Bundesregierung, BT-Drs. 18/5127, S. 3.

Die Aufklärung der Öffentlichkeit kann dadurch geschwächt werden, dass die der Aufklärung dienenden Berichte nicht durch das BSI veröffentlicht werden. Nicht auf den ersten Blick ist dem Wortlaut von § 13 BSIG zu entnehmen, dass nicht das BSI über den Inhalt der Berichte entscheidet, sondern vorrangig dem BMI die Aufklärungsaufgabe zukommt. Erst durch dessen jährlich vorzulegenden zusammenfassenden Bericht wird die Öffentlichkeit über Gefahren für die Sicherheit aufgeklärt. Informationen können so im BMI gefiltert werden, insbesondere dann, wenn ihrer Veröffentlichung kollidierende Interessen von Sicherheitsbehörden entgegenstehen, die ebenfalls der Aufsicht des BMI unterstehen.[110] Der Rechtsfolgenverweis in § 13 Abs. 2 S. 2 BSIG führt zur Anwendung des gestuften Verfahrens bei Warnungen und damit zur Begrenzung der Öffentlichkeitsaufklärung. Der Kreis der zu informierenden Personen kann eingeschränkt werden, wenn die Veröffentlichung zum Missbrauch der Informationen führen kann.[111]

bb) Bericht der Bundesnetzagentur

Die Bundesnetzagentur hat nach § 121 TKG dagegen den gesetzgebenden Körperschaften des Bundes einen Tätigkeitsbericht über die Lage und Entwicklung auf dem Gebiet der Telekommunikation vorzulegen. Die Berichtspflicht muss nicht auf den Tätigkeitsnachweis verkürzt werden. In der Praxis geht der Bericht zwar nicht über das Referieren der bereichsspezifischen Aufgaben aus dem 7. Teil des TKG und einiger statistischer Angaben über überprüfte Sicherheitskonzepte und eingegangene Meldungen hinaus.[112] Die Tätigkeitsberichte dienen aber neben der Information über die eigene Tätigkeit der regelmäßigen parlamentarischen Kontrolle und der Zusammenarbeit zwischen Gesetzgeber und Verwaltung.[113] Erleichtert werden soll auch die Beurteilung, ob die Regulierungsziele gemäß § 2 TKG erreicht wurden. Die Bundesnetzagentur kann daher ohne Mitredaktion des übergeordneten Ministeriums auf die Defizite hinsichtlich des Regelungsziels der öffentlichen Sicherheit (§ 2 Abs. 2 Nr. 9 TKG) hinweisen und darüber Aufklärung betreiben.[114]

---

[110] Siehe zum spezifischen Problem der Weisungsgebundenheit des BSI unter § 4 C. III. 2. und dem Responsible-Disclosure-Verfahren unten § 5 B. I. 4. b).

[111] Dazu im Einzelnen § 5 B. I.

[112] *Bundesnetzagentur*, Tätigkeitsbericht nach § 121 Abs. 1 TKG vom 07.12.2015, Telekommunikation 2014/2015, S. 218 bis 226, online abrufbar.

[113] *Altmeppen*/*Geppert*, in: Geppert/Schütz (Hrsg.), BeckTKG, 4. Aufl. 2013, § 121 Rn. 1; BR-Drs. 80/96, S. 52.

[114] Vgl. *Böcker*, in: Säcker (Hrsg.), TKG, 3. Aufl. 2013, § 121 Rn. 13 ff.

cc) Bericht der Datenschutzaufsichtsbehörde

Der Aufklärung zur Sensibilisierung können ferner die Berichte der Datenschutzbehörden dienen. Nach §§ 26 Abs. 1 S. 1, 38 Abs. 1 S. 1 BDSG haben der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und die sonstigen Datenschutzaufsichtsbehörden dem Deutschen Bundestag alle zwei Jahre einen Tätigkeitsbericht zu erstatten. Da die Datenschutzaufsicht institutionell unabhängig ist und keiner Aufsicht unterliegt,[115] kann dem Bericht keine Kontrollfunktion zukommen. Daher können die Berichte auch dafür genutzt werden, die Öffentlichkeit zu sensibilisieren,[116] über allgemeine Datenschutzprobleme und -erfordernisse zu informieren oder zu exemplarischen Einzelfällen Stellung zu nehmen.[117] Sowohl Bürger als auch Fachkreise können über abstrakte wie konkrete Gefährdungen informiert werden.[118] Die Öffentlichkeit ist sogar angesichts der knappen personellen Ausstattung und des damit einhergehenden Durchsetzungsdefizits für Datenschutzbehörden das entscheidende Medium dafür, auf datenschutzverantwortliche Stellen einzuwirken.[119]

Mit der durch die DS-GVO gestärkten Stellung und Ausstattung der Aufsichtsbehörden[120] gehen erweiterte Aufklärungsmöglichkeiten einher. Anders als in der Datenschutz-Richtlinie ist der Bildungs- und Aufklärungsauftrag der Datenschutzaufsicht nun zentral im Aufgabenprofil verankert.[121] Gemäß Art. 57 Abs. 1 lit. b DS-GVO gehört zu den gesetzlich vorgegebenen Aufgaben der Datenschutzaufsicht, die Öffentlichkeit für Risiken und Vorschriften im Zusammenhang mit der Datenverarbeitung zu sensibilisieren und sie über diese aufzuklären.[122] Die Aufklärung ist dabei eine Handlungspflicht („muss“).

Zur durch die DS-GVO formalisierten Öffentlichkeitsarbeit gehört der vorzulegende Tätigkeitsbericht (Art. 59 DS-GVO). Die Berichtszyklen sind kürzer, der Tätigkeitsbericht ist als Jahresbericht vorzulegen. Der Bericht ist zwar nicht direkt an die Öffentlichkeit zu richten, er ist ihr aber zugänglich zu machen. Die Verordnung legt es in das Ermessen der Behörde, dem Bericht eine Liste der „Arten“ der gemeldeten Verstöße und der getroffenen Abhilfemaßnahmen bei-

---

[115] Siehe § 4 C. III. 2.

[116] Vgl. *von Lewinski*, RDV 2004, 163 (163 ff.).

[117] *Von Lewinski*, in: Auernhammer, 4. Aufl. 2014, BDSG, § 26 Rn. 5.

[118] Vgl. VG Schleswig, ZD 2014, 102, nachfolgend OVG Schleswig-Holstein, ZD 2014, 536.

[119] Siehe zur Öffentlichkeit als „Verbündete“ des Datenschutzbeauftragten BGH, NJW 2003, 979 (980).

[120] Dazu *von Lewinski*, DuD 2012, 564 (565).

[121] *Roßnagel*, Zusätzlicher Arbeitsaufwand für die Aufsichtsbehörden der Länder durch die Datenschutz-Grundverordnung, 2017, S. 84.

[122] Vgl. Erwägungsgrund 122, 132 DS-GVO.

zufügen.[123] Ob eine schlichte Auflistung von Verstößen und Anordnungen ohne nähere Kontexteinbettung aussagekräftig und damit zweckmäßig ist, kann bezweifelt werden. Im Zweifel dürften die Berichte mit technischen, gesellschaftlichen oder wirtschaftlichen Kontextinformationen anzureichern sein.

b) Stellungnahmen der Datenschutzaufsichtsbehörden

Als Medium der Aufklärungsarbeit der Datenschutzaufsichtsbehörden kommt neben dem Tätigkeitsbericht die Stellungnahme in Betracht. Als beratende Befugnis ausgestaltet ist das Recht jeder Aufsichtsbehörde, von sich aus oder auf Anfrage zu „allen Fragen" im Zusammenhang mit dem Datenschutz Stellungnahmen an die Öffentlichkeit zu richten (Art. 58 Abs. 3 lit. b DS-GVO). Die Datenschutz-Richtlinie sah eine derartige Befugnis nicht vor. Wegen der Offenheit der Befugnis kann die Aufsichtsbehörde auch zu Fragen der Datensicherheit Stellung nehmen. Dafür kommen alle Formen amtlicher Äußerungen infrage, solange sie den allgemeinen Rechtmäßigkeitsanforderungen entsprechen und im Zuständigkeitsbereich der jeweiligen Behörde liegen.[124]

Ob jedoch Art. 58 Abs. 3 lit. b DS-GVO so ausgelegt werden kann, dass die Öffentlichkeit stets Adressat von Stellungnahmen sein kann, ist eine Frage der grammatikalischen Auslegung. Vor dem Passus „sowie an die Öffentlichkeit zu richten" hat der Verordnungsgeber die Öffnungsmöglichkeit „im Einklang mit dem Recht des Mitgliedstaats" eingefügt. Diese könnte so verstanden werden, dass sie sich nur auf den unmittelbar nachfolgenden Passus bezieht („oder im Einklang mit dem Recht des Mitgliedstaats an sonstige Einrichtungen und Stellen") oder aber auch auf die Öffentlichkeit („sowie"). In der englischsprachigen Fassung sind die Einrichtung und Stellen und die Öffentlichkeit ohne das sog. *serial comma* aufgezählt („or, in accordance with national law, to other institutions and bodies as well as to the public"), sodass die Vorschrift auch so ausgelegt werden könnte, dass den Mitgliedstaaten ein Gestaltungsspielraum zusteht. Dem Sinn der Öffnungsklausel, den Mitgliedstaaten dort einen Konkretisierungsspielraum einzurichten, wo es den Unionsgesetzgeber überfordern würde, entspricht es dagegen eher, dass sich dieser Spielraum nur auf die sonstigen Stellen und Einrichtungen bezieht.[125] Es ist bei der Unterschiedlichkeit der Vergleichsgruppen auch kein Grund ersichtlich, warum der Verordnungsgeber den

---

[123] *Körffer*, in: Paal/Pauly, DSGVO, 2016, Art. 59 Rn. 3.

[124] Vgl. im Zusammenhang mit der Öffentlichkeitsarbeit des Unabhängigen Datenschutzzentrums Schleswig-Holstein über die Datenschutzkonformität des Dienstes Facebook *Härting*, CR 2011, 585 (587 f.).

[125] Kühling/Martini/Heberlein/Kühl/Nink/Weinzierl/Wenzel, Die Datenschutz-Grundverordnung und das nationale Recht, 2016, S. 194.

Mitgliedstaaten die Disposition über die Öffentlichkeit als Adressat überlassen wollte. Die Öffentlichkeit ist demnach stets zulässiger Adressat von Stellungnahmen.

c) Information über Sicherheitsvorfälle

Der Gesetzgeber hat auf die geringe Bereitschaft der Unternehmen, Sicherheitsvorfälle publik zu machen, mit der Einführung von Meldepflichten reagiert. Die Kehrseite der Meldepflichten sind die Befugnisse zur Veröffentlichung von Sicherheitsverletzungen (aa). Für Verletzungen des Datenschutzes besteht mit dem Inkrafttreten der DS-GVO dagegen keine datenschutzbehördliche Befugnis mehr, die Öffentlichkeit zu informieren (bb).

aa) Unterrichtung über Sicherheitsverletzungen

Veröffentlicht werden können Sicherheitsverletzungen bei Telekommunikationsunternehmen (1). Das BSI verfügt über keine Informationsbefugnis, obwohl sie unionsrechtlich eingefordert wird (2).

(1) Sicherheitsverletzungen bei Telekommunikationsunternehmen

Die nationale Regulierungsbehörde im Telekommunikationssektor kann nach Art. 13a Abs. 3 UAbs. 2 S. 2 Rahmen-RL die Öffentlichkeit unterrichten oder die Unternehmer zur Information der Öffentlichkeit verpflichten. Diese unionsrechtliche Vorgabe ist mit § 109 Abs. 5 S. 7 TKG umgesetzt. Danach ist die Bundesnetzagentur befugt, die Öffentlichkeit über eine gemeldete Sicherheitsverletzung zu informieren. Alternativ kann sie die Telekommunikationsbetreiber und Diensteanbieter zu dieser Unterrichtung auffordern, wenn sie zu dem Schluss gelangt, die Bekanntgabe der Sicherheitsverletzung liege im öffentlichen Interesse, § 109 Abs. 5 S. 7 HS. 2 TKG. Die strenge Begründung zum Entwurf dieser Regelung hebt hervor, dass eine Unterrichtung nur erfolgen darf, wenn es das öffentliche Interesse erfordert.[126] In der mehrpoligen Grundrechtssituation stehen sich das Interesse des Unternehmens, nicht durch hoheitliche Äußerungen beeinträchtigt zu werden, und das Interesse der Öffentlichkeit an der Aufklärung über potenzielle Gefahren gegenüber.

In dieser Abwägung liegt eines der drängendsten Probleme der Internetsicherheit: die Divergenz von Wahrheit und Version. Bei einer bestimmteren Kenntnis über kritische Sicherheitsprobleme kann es begründet sein, dass es vertraulich behandelt wird. Gelangt dieses Wissen an die Öffentlichkeit, könnte es nämlich für unredliche Zwecke genutzt werden. Geheimhaltung kann jedoch auch darauf

[126] BT-Drs. 17/5707, S. 83.

zielen, bestimmte Sicherheitsprobleme zu verdecken: „Denn Sicherheitsprobleme sind in der Regel auch Ausdruck eines Versagens.“[127] Das Interesse an der Nichtöffentlichkeit von Sicherheitslücken kann monetäre Gründe haben, denn Sicherheit wird regelmäßig als Kostenfaktor und nicht als Investition betrachtet.[128] Werden Sicherheitsvorfälle bei einem Unternehmen in der Öffentlichkeit bekannt, kann der Eindruck eines unzureichenden Sicherheitsstands entstehen. Es ist den Betroffenen ohnehin kaum einsichtig einen Imageschaden durch die Publikation eines Sicherheitsschadens und damit einen Vertrauensverlust zu riskieren, der ohnehin bereits entstanden ist. Daher gelangen Informationen über Sicherheitsangriffe und -vorfälle kaum an die Öffentlichkeit.[129]

Das öffentliche Interesse erfordert demnach die Veröffentlichung grundsätzlich nicht, wenn dieser berechtigte, überwiegende Interessen der betroffenen Unternehmen entgegenstehen. Dies ist insbesondere dann der Fall, wenn durch die Veröffentlichung schwerwiegende Folgen drohen. Das öffentliche Interesse an der Unterrichtung der Öffentlichkeit über eine Sicherheitsverletzung besteht dagegen dann, wenn der Verdacht begründet ist, durch das Unterlassen der Veröffentlichung entstehe in der Öffentlichkeit eine subjektive Wahrnehmung von Sicherheit, die von der Wirklichkeit divergiert. Die Öffentlichkeit sollte erkennen können, ob persönlicher oder politischer Handlungsbedarf besteht. Berücksichtigung bei der Ausübung des pflichtgemäßen Ermessens sollte außerdem der Umstand finden, dass die proaktive Information der Öffentlichkeit durch die NIS-Behörde Dritten überhaupt Anlass gibt, gegenüber der Behörde konkrete Auskunftsansprüche über entsprechende Vorfälle geltend zu machen.[130]

Aus Gründen der Verhältnismäßigkeit kann es geboten sein, als milderes Mittel das Unternehmen aufzufordern, selbst die Öffentlichkeit zu unterrichten. Der Grundrechtseingriff fällt insoweit milder aus, als sich das Unternehmen als „Herrin der Publikumsinformation“ gerieren und insoweit das „Gesicht wahren“ kann. Die Wahl des Inhalts und der Form der Benachrichtigung sind dem Unternehmen anheimgestellt. Ob die Unternehmen zu einer unverzüglichen Publikumsinformation verpflichtet werden können, kann aufgrund des nicht eindeutigen Wortlauts des § 109 Abs. 5 S. 7 TKG in Zweifel gezogen werden („auf-

---

[127] *Gaycken*, Offizielle Versionen versus mögliche Wahrheiten – Cybersecurity und das Problem der Geheimhaltung, in: Haupter (Hrsg.), Der digitale Dämon, 2013, 49 (49).

[128] Zu den fehlenden ökonomischen Anreizen in der Cybersicherheit siehe § 1 A.

[129] *Lovet*, Fighting cybercrime: Technical, juridical and ethical challenges, Virus Bulletin Conference Proceedings, 2009, 63 (63 f.); vgl. *Vogel*, Towards a global convention against cybercrime, Proceedings World Conference on Penal Law, 2007, 1 (4); *Gaycken*, Offizielle Versionen versus mögliche Wahrheiten – Cybersecurity und das Problem der Geheimhaltung, in: Haupter (Hrsg.), Der digitale Dämon, 2013, 49 (49 ff.).

[130] Siehe zum reaktiven Informationshandeln § 5 C.

fordern“).[131] Eine Anordnungsbefugnis dürfte jedoch wohl dann anzunehmen sein, wenn schwerwiegende Sicherheitsverletzungen gegeben sind.[132]

(2) Fehlende Rechtsgrundlage für das BSI

Eine der telekommunikationsrechtlichen Grundlage entsprechende Veröffentlichungsbefugnis besteht für das BSI nicht. Gleichwohl ist das grundsätzliche Interesse der Öffentlichkeit daran, über Bedrohungen und sicherheitsrelevante Vorfälle informiert zu werden, in der NIS-Richtlinie anerkannt.[133]

Über einzelne, gemeldete Sicherheitsvorfälle bei Betreibern wesentlicher Dienste und Anbietern digitaler Dienste soll die NIS-Behörde oder das CSIRTs unterrichten dürfen. Über Sicherheitsvorfälle bei Betreibern wesentlicher Dienste soll die Öffentlichkeit gemäß Art. l4 Abs. 6 NIS-RL nach Anhörung der Betreiber unterrichtet werden können, sofern die Sensibilisierung der Öffentlichkeit zur Verhütung von Sicherheitsvorfällen oder zur Bewältigung aktueller Sicherheitsvorfälle erforderlich ist. Die Unterrichtung der Öffentlichkeit über Sicherheitsvorfälle bei Anbietern digitaler Dienste oder deren Offenlegung kann gemäß Art. l6 Abs. 7 NIS-RL zusätzlich dann erfolgen, wenn sie auf sonstige Weise im öffentlichen Interesse liegt.

Die Reichweite dieser unionsrechtlich intendierten Informationstätigkeit hängt vom Bedeutungsgehalt der Unterrichtung ab. Als typisierte Erscheinungsform ist sie noch wenig systematisiert.[134] Aus dem Wortlaut ergibt sich aber, dass eine Befugnis gegeben sein muss, die es erlaubt, über einzelne Sicherheitsvorfälle zu unterrichten. Im Umkehrschluss ist den Mitgliedstaaten nicht lediglich aufgegeben, eine nur abstrakt-generelle Informationsmöglichkeit einzuführen, sondern eine Rechtsgrundlage zu schaffen, welche die NIS-Behörde zu verhältnismäßigen Informationseingriffen ermächtigt.

Die bestehenden Rechtsgrundlagen setzen die in der NIS-Richtlinie vorgesehenen Befugnisse nicht um.

Die zentrale Vorschrift, die dem BSI Unterrichtungspflichten auferlegt, ist § 8b Abs. 2 Nr. 4 BSIG. Die Öffentlichkeit als Adressat der Unterrichtung ist jedoch in keiner Variante genannt.[135] Die Information einer Vielzahl von Infra-

---

[131] *Eckhardt*, in: Geppert/Schütz (Hrsg.), BeckTKG, 4. Aufl. 2013, § 109 Rn. 84, der aber nur wegen einer fehlenden Zeitangabe darauf schließt, dass eine Pflicht zur unverzüglichen Verpflichtung nicht besteht.

[132] Anders wohl *Eckhardt*, in: Geppert/Schütz (Hrsg.), BeckTKG, 4. Aufl. 2013, § 109 Rn. 84.

[133] Erwägungsgrund 40 und 59 NIS-RL.

[134] Keine eigene Erscheinungsform ist die Unterrichtung bei *Feik*, Öffentliche Verwaltungskommunikation, 2007, S. 7 ff.; als Kategorie der behördlichen Publikumsinformation hingegen bei *Schoch*, VBlBW 2014, 361 (364).

[135] Irritierenderweise führt die Begründung, BT-Drs. 17/5707, S. 46, aus, dass die Öffent-

strukturbetreibern kann zwar einer Publikumsinformation gleichkommen, eine Information der allgemeinen Öffentlichkeit kann sich auf diese Vorschrift jedoch nicht stützten.

Der telekommunikationsrechtliche § 109 Abs. 5 S. 4 TKG verfolgt zwar das der NIS-Richtlinie zugrundeliegende Regelungsanliegen der Öffentlichkeitsinformation, der Anwendungsbereich bezieht sich jedoch nicht auf digitale und wesentliche Dienste im Sinne der NIS-Richtlinie.

In Betracht kommt außerdem § 7 BSIG, der dem BSI erlaubt, Warnungen und Empfehlungen an die Öffentlichkeit zu richten.[136] Ungeachtet der Frage, ob die Unterrichtung als Minus zur Warnung auf diese Grundlage gestützt werden kann, sieht § 7 BSIG schon tatbestandlich nicht vor, dass über Sicherheitsvorfälle informiert werden kann. Außerdem sieht das Mandat in § 7 BSIG lediglich die Information der betroffenen Hersteller vor der öffentlichen Warnung vor („informieren"). Das von Art. 14 Abs. 6 und Art. 16 Abs. 7 NIS-RL vorgesehene Anhörungsverfahren wird von § 7 BSIG nicht abgebildet.[137]

Als Legitimitätsgrundlage für Publikumsinformationen ließe sich schließlich die mit dem IT-Sicherheitsgesetz erweiterte Aufgabennorm in § 3 Abs. 1 S. 2 Nr. 2 BSIG heranziehen. Das BSI nimmt demnach die Aufgabe wahr, Erkenntnisse „Dritten" zur Verfügung stellen, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist. Dritte sind sonstige Einrichtungen, Unternehmen aus anderen Sektoren außerhalb der kritischen Infrastrukturen sowie die Zivilgesellschaft. Die Qualität als Aufgabennorm lässt es jedoch nur bedingt zu, eine Publikumsinformation auf sie zu stützen, die über allgemeine Angaben eines Sicherheitsvorfalls hinausgeht. Informationen mit Prangerwirkung (*name and shame*), welche negative Rückschlüsse auf Unternehmen oder die Branche zulassen, oder weiterführende Angaben über Produkt, Täter, Betroffene, Folgen usw. wären auf dieser Grundlage grundsätzlich unzulässig. Gezielte Steuerungseffekte können auf Grundlage von § 3 BSIG also nicht erreicht werden.

Im Rahmen der Umsetzung des Regelungsanliegens, über Bedrohungen und Sicherheitsvorfälle die Öffentlichkeit zu informieren, erscheint es sinnvoll, die Informationen auf europäischer Ebene zu aggregieren sowie kontinuierlich in mehreren Landessprachen zugänglich zu machen. Die im Unionsrecht angeleg-

---

lichkeit informiert wird, wenn das öffentliche Interesse dies erfordert. Nur als Redaktionsversehen kann es angesehen werden, dass diese Ausführung im Zusammenhang mit § 8b Abs. 2 Nr. 4 BSIG steht, der ausdrücklich die Öffentlichkeit nicht als Adressat zulässt. Ausweislich des Fehlens der Öffentlichkeit als potenzieller Adressat kann diese, als Redaktionsversehen zu betrachtende, Aussage nicht darüber hinweghelfen, dass die Vorschrift abschließend ist.

[136] Siehe § 5 B. I. 4. und 5.

[137] Vgl. *Schallbruch*, CR 2016, 663 (668 f.).

te Parallelstruktur der Veröffentlichungsbefugnisse bei der Bundesnetzagentur und der NIS-Behörde führt dazu, dass die interessierte Öffentlichkeit, die sich nicht auf einen Mitgliedstaat beschränkt, auf mehrere Anlaufstellen verwiesen ist. Richtig ist insofern der Ansatz, dem Sekretariat des CSIRTs-Netzwerk die Aufgabe zu übertragen, eine Internetseite zu unterhalten, auf der die übermittelten Daten mit Fokus auf die Interessen und Bedürfnisse der Unternehmen veröffentlicht werden. Die unionsrechtlichen Vorgaben bleiben hier aber schwach.[138] Wirksam wäre eine solche Transparenzmaßnahme, wenn die unionsweite Veröffentlichung auch Hinweise zur möglichen Risikobegrenzung und Bewältigung von Sicherheitsvorfällen beinhalten würde.[139]

bb) Veröffentlichung einer Verletzung des Schutzes personenbezogener Daten durch Verantwortliche

Verletzungen des Schutzes personenbezogener Daten sind unter bestimmten Voraussetzungen publik zu machen. Anders als bei Verletzungen der Netz- und Informationssicherheit steht die Befugnis, die Öffentlichkeit über eine Verletzung zu informieren, nicht der Datenschutzbehörde selbst zu. Die Öffentlichkeit ist vielmehr durch die verantwortlichen Stellen selbst zu informieren.

Bei Internetdiensteanbietern ist hinsichtlich dieser Veröffentlichungspflicht zu unterscheiden.

Für Anbieter von Telemedien gilt durch den Rechtsfolgenverweis in § 15a TMG auf § 42a BDSG das allgemeine Datenschutzrecht.[140] Die Regelung des § 42a BDSG sieht in Satz 5 vor, das an Stelle der Benachrichtigung des von der Verletzung Betroffenen die Information der Öffentlichkeit tritt, und zwar durch Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeigneten Maßnahme. Die Betroffenen sollen in verständlicher Form über drohende Beeinträchtigungen informiert werden, damit erforderliche Maßnahmen zur Abwehr, zur Begrenzung oder zum Ersatz eines Schadens getroffen werden können.[141]

---

[138] Erwägungsgrund 16 NIS-RL.

[139] So noch angedacht im Bericht des Europäischen Parlaments über den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union vom 12.02.2014 (A7-0103/2014). Die Informationen sollten zudem geräteunabhängig zugänglich sein und sogar die Veröffentlichung von personenbezogenen Daten erlauben, falls dies notwendig wäre.

[140] Siehe bereits § 3 D. I. 3.

[141] *Gola*/*Klug*/*Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl. 2015, § 42a Rn. 6.

Die Information der Öffentlichkeit erfolgt nur bei einem unverhältnismäßigen Aufwand einer Benachrichtigung der einzelnen Betroffenen. Dies ist insbesondere bei einer Vielzahl der Betroffenen der Fall oder dann, wenn deren Kontaktdaten nicht bekannt sind.[142]

Eine § 42a BDSG entsprechende Verpflichtung enthält Art. 34 Abs. 3 lit. c DS-GVO. Eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme hat bei einem unverhältnismäßigen Aufwand der einzelnen Benachrichtigung zu erfolgen. Die betroffenen Personen sollen „wirksam informiert" werden. Demzufolge bezweckt die Veröffentlichung nicht primär die Information der Öffentlichkeit als solche, sondern sie ist nur Medium, um letztlich die von der Verletzung Betroffenen zu erreichen.

Für Anbieter öffentlicher Kommunikationsdienste besteht keine Vorschrift, die die gleichen Tatbestandsvoraussetzungen und Rechtsfolgen wie in § 42a BDSG in Verbindung mit § 15a TMG regelt. § 109a Abs. 1 S. 5 TKG verweist nur auf § 42a S. 6 BDSG. Eine an die Öffentlichkeit gerichtete Informationspflicht besteht für Telekommunikationsdiensteanbieter daher nicht. Die DS-GVO dürfte jedoch für Telekommunikationsdienste, ebenso wie für Telemediendienstanbieter, eine Harmonisierung im Bereich der Veröffentlichungspflicht bei Verletzungen des Datenschutzes bewirken. Art. 95 DS-GVO, der das Verhältnis der DS-GVO zur RL 2002/58/EG regelt, nimmt Betreiber von Telekommunikationsdiensten nur insoweit von den Verpflichtungen der DS-GVO aus, als keine zusätzlichen Pflichten in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung der Kommunikationsdienste durch sie auferlegt werden und soweit die Betreiber besonderen in der RL 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen. Da die Vorgaben zur Verarbeitung nicht die Benachrichtigungspflicht betreffen, dürfte von der DS-GVO eine harmonisierende Wirkung ausgehen.

3. Veröffentlichung von Sicherheitsanforderungen und Untersuchungsergebnissen

Über die Aufklärung zur Sensibilisierung für Sicherheitsprobleme hinaus geht die Veröffentlichung der Sicherheitskataloge für Telekommunikationsunternehmen (a) und der Erkenntnisse aus Produkt- und Systemuntersuchungen (b).

---

[142] *Herbst*, in: Auernhammer, BDSG, 4. Aufl. 2014, § 42a Rn. 22; vgl. BT-Drs. 16/12011, S. 34.

a) Veröffentlichung des Sicherheitskatalogs

Den Sicherheitskatalog, den die Bundesnetzagentur im Einvernehmen mit dem BSI und dem BfDI erstellt,[143] hat die Bundesnetzagentur nach § 109 Abs. 6 S. 3 TKG zu veröffentlichen.[144] Der Katalog enthält eine kurze, allgemein gehaltene Auflistung von Sicherheitsempfehlungen, die die Grundlage für den sicheren Betrieb internetbasierter Telekommunikationssysteme bilden.[145] Der Sicherheitskatalog hat die Funktion, den zur Sicherheit verpflichteten Telekommunikationsunternehmen grundsätzliche inhaltliche Hinweise und Empfehlungen zu geben. Umfassende Maßnahmeempfehlungen enthält der Katalog nicht.[146] Gleichwohl erhalten auch Anbieter von Sicherheitsprodukten und -systemen Informationen darüber, welche Anforderungen an die IT-Sicherheit im Hinblick auf das Betreiben von Telekommunikations- und Datenverarbeitungssystemen staatlicherseits gestellt werden. Insofern wird für die Anbieter auf dem Markt eine gewisse Transparenz darüber geschaffen, welche Nachfrage grundsätzlich besteht.

b) Veröffentlichung der Erkenntnisse aus Produkt- und Systemuntersuchungen

Die Befugnis des BSI, IT-Produkte mittels Reverse Engineering zu untersuchen, dient neben dem Auffinden von Schwachstellen der Erhöhung der Sicherheit durch Veröffentlichung der gewonnenen Erkenntnisse. Auf Grundlage von § 7a Abs. 2 S. 2 BSIG darf das Amt die gewonnenen Erkenntnisse weitergeben und veröffentlichen. Eine unionsrechtliche Vorgabe liegt § 7a BSIG nicht zugrunde.

Aufgrund der Bindung der Veröffentlichungsbefugnis an drei Aufgaben des BSI (§ 3 Abs. 1 S. 2 Nr. 1, 14 und 17 BSIG) wird betont, dass die Vorschrift „streng […] beschränkt“[147] ist. Die nähere Betrachtung der Aufgabennormen ergibt gleichwohl, dass Erkenntnisse zu weit definierten Zwecken weitergegeben und veröffentlicht werden dürfen. So schließt § 3 Abs. 1 S. 2 Nr. 17 BSIG die Beratung und Warnung der Stellen des Bundes und der Länder sowie der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informa-

---

[143] Dazu bereits § 3 D. I. 2. (1).

[144] Der Katalog von Sicherheitsanforderungen Version 1.1 ist mit der Veröffentlichung im Amtsblatt Nr. 3 der Bundesnetzagentur am 17.02.2016 in Kraft getreten. Funktional äquivalent ist § 11 Abs. 1c S. 2 EnWG.

[145] *Bundesnetzagentur*, Katalog von Sicherheitsanforderungen, Version 1.1, Stand 07.01. 2016, S. 50 f., online abrufbar.

[146] *Bundesnetzagentur*, Katalog von Sicherheitsanforderungen, Version 1.1, Stand 07.01. 2016, S. 5, online abrufbar.

[147] *Terhaag*, IT-Sicherheitsgesetz, 2015, S. 39.

tionstechnik unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen ein. Die Veröffentlichung ist demnach nicht auf die Sicherheit in kritischen Infrastrukturen begrenzt. Augrund des Merkmals „Beratung" muss die Veröffentlichung keinen Appellcharakter aufweisen. Sie kann allgemein dazu dienen, auf die sicherheitstechnischen Implikationen einer gewonnenen Erkenntnis hinzuweisen. In Abgrenzung zur Weitergabe ermöglicht es die Veröffentlichung, über die unmittelbar Betroffenen hinaus Interessierte zu erreichen. Die Veröffentlichung ist angezeigt, wenn die Erkenntnis einen Bezug zum europäischen Binnenmarkt aufweist.

Der Schutz der Hersteller vor dem behördlichen Informationshandeln ist stärker ausgestaltet. Anders als bei der Warnung vor Sicherheitslücken in informationstechnischen Produkten und Diensten werden die Hersteller vor der Veröffentlichung nicht nur lediglich informiert. Sie dürfen vielmehr vor der Publikation Stellung nehmen. Gelingt dem Hersteller des untersuchten Produkts bei einem Fehler also die Abhilfe, ist die Veröffentlichung des Fehlers aus Gründen der Verhältnismäßigkeit grundsätzlich unzulässig, da sie nicht mehr erforderlich wäre.[148]

Aufgrund der mit dem IT-Sicherheitsgesetz eingeführten Veröffentlichungsbefugnis erweitert sich das Informationsrecht des BSI. Mit der Warnbefugnis in § 7 BSIG war immerhin ein gewisser Nukleus eines digitalen IT-Informationsrechts zu erkennen. Das Gefahrenabwehrrecht verfügt aber ohne die Regelung des § 7a BSIG nicht über ausreichende Instrumente, um über die von Produkten ausgehenden Risiken für Daten, insbesondere für mit dem Persönlichkeitsrecht verbundene Nutzerdaten, zu informieren. Das klassische Produktsicherheitsrecht hält zwar mit Art. 16 Abs. 2 VO (EG) Nr. 756/2008 bzw. § 31 Abs. 2 S. 1 ProdSG eine Rechtsgrundlage zur Publikumsinformation bereit. Die Marktüberwachungsbehörden sind sogar grundsätzlich verpflichtet, Informationen über gefährliche Produkte zu veröffentlichen. Der Anwendungsbereich des ProdSG ist bei Soft- und Hardware-Produkten jedoch nicht abschließend geklärt.[149] Die produktsicherheitsrechtliche Veröffentlichungspflicht knüpft im Übrigen an eine Verbindung der Erkenntnis zu Produkten an Risiken für die Sicherheit und Gesundheit von Personen. Demgegenüber geht § 7a Abs. 2 BSIG durch die Aufgabenverweisung deutlich weiter, wenn die Folgen fehlender oder unzureichender Sicherheitsvorkehrungen lediglich zu berücksichtigen sind. Die Folgen müssen nicht nur am Maßstab hochrangiger Rechtsgüter, sondern können anhand der Schutzziele der Netz- und Informationssicherheit beurteilt werden.

---

[148] Vgl. BT-Drs. 18/4096, S. 25.

[149] Siehe § 3 D. II. 1.

4. Warnungen vor Sicherheitslücken und sonstigen Gefahren

Eine wichtige Regelung für staatliches Informationshandeln im Bereich der IT-Sicherheit ist die mit „Warnungen" überschriebene und mit dem IT-Sicherheitsgesetz neu gefasste Befugnis des § 7 BSIG. Die Warnbefugnis ermöglicht es dem BSI, seine gewonnenen Erkenntnisse als Warnung an die Öffentlichkeit oder an betroffene Kreise zu richten. Das BSI kann zur Wahrnehmung dieser Aufgabe Dritte einbeziehen. Ausdrücklich sind Warnungen vor Sicherheitslücken in IT-Produkten und -Diensten, vor Schadprogrammen sowie im Falle des Abs. 1 vor einem Datenverlust oder einem unerlaubten Datenzugriff gestattet.[150]

Die Anwendung der als Ermessensvorschrift ausgestalteten Befugnis (a) muss die besondere, mitunter adversarische Interessenkonstellation berücksichtigen (b).

a) Voraussetzungen und Reichweite des Tatbestands

§ 7 BSIG unterscheidet die Warn- und Empfehlungsbefugnis. Die Möglichkeit, vor Sicherheitslücken, Schadprogrammen und Datenschutzvorfällen unter Nennung oder Verzicht auf eine namentliche Hersteller- oder Produktbezeichnung zu warnen sowie Empfehlungen auszusprechen, ist weitreichend. In Betracht kommen sämtliche geeignete Kommunikationsmittel. Eine gesetzliche Begrenzung auf ein bestimmtes Medium wie in § 42a Abs. 1 BDSG ist nicht vorgesehen. Vor allem dürften elektronische Verteiler für eine öffentliche Information infrage kommen.

Greift die namentliche Erwähnung der Unternehmen und der Produkte in rechtlich geschützte Interessen Dritter ein, bedarf es entsprechend § 7 Abs. 2 S. 1 BSIG hinreichender Anhaltspunkte dafür, dass Gefahren für die IT-Sicherheit von den Produkten oder Diensten, etwa durch Sicherheitslücken, ausgehen. Die Hersteller sind zudem gemäß § 7 Abs. 1 S. 3 vor der Veröffentlichung zu informieren, solange dies ohne Zweckgefährdung möglich ist. Eine Befugnis, zur Lückenschließung anzuweisen, besteht indes nicht. Aus den allgemeinen Kriterien der Sachlichkeit, Richtigkeit und Verhältnismäßigkeit folgt, dass, wenn möglich, auf eine namentliche Nennung zu verzichten ist und so die Inter-

---

[150] *Buchberger*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, BSIG, § 7 Rn. 1. Der Gesetzeswortlaut des § 7 Abs. 1 S. 1 BSIG a. F. vor Erlass des IT-Sicherheitsgesetzes sprach noch von einem „weitergeben" von Warnungen; nunmehr ist klargestellt, dass das BSI nicht nur zur bloßen Weitergabe von Informationen berechtigt ist. Die Warnbefugnis bei Datenverlust und einem unerlaubten Zugriff in § 7 Abs. 1 S. 1 Nr. 1 c) BSIG wurde durch das IT-Sicherheitsgesetz neu in das BSIG aufgenommen.

essen des betroffenen Unternehmens vor allem mit Blick auf potenzielle Rufschädigungen und wirtschaftliche Nachteile zu berücksichtigen sind.[151]

Eine Pflicht zur Warnung vor Gefahren statuiert die Norm entgegen Forderungen im Gesetzgebungsverfahren nicht,[152] sie ist als Ermessensvorschrift („kann") ausgestaltet. Eine Pflicht zur Veröffentlichung von Sicherheitslücken ließe sich allenfalls bei einer Ermessensreduzierung auf null annehmen. Die Ermessensausübung wird geleitet durch die Abwägung mit den Gefahren und Schäden, die bei einer Veröffentlichung durch die Möglichkeit noch nicht behobener Sicherheitslücken drohen. Eine Zurückhaltung bei der Warnung über bestehende Sicherheitsgefahren kann sich ebenso aus den Interessen der betroffenen Hersteller ergeben. Dem Prinzip der verantwortungsvollen Veröffentlichung ist regelmäßig Vorzug zu geben.[153] Bei der Empfehlung bestimmter Produkte ist das BSI durch die Beachtung des Gleichheitsgrundsatzes aus Art. 3 GG begrenzt. Schließlich ist auch eine dysfunktionale Einflussnahme auf den Markt zu vermeiden.[154]

b) Responsible Disclosure als ermessensleitende Strategie für die Warnung vor Sicherheitslücken

Der Versuch, das staatliche Informationshandeln durch abstrakte und formelle Kriterien in einer eigenständigen Dogmatik einzuhegen, ist als gescheitert angesehen worden.[155] Schon im Ansatz ist vielfach keine Lösung in der Abwägung ersichtlich, die hinsichtlich Eignung und Erforderlichkeit für jedes der kollidierenden Rechtsgüter zu einem positiven Ergebnis kommt, soweit die Abwägung nur zugunsten der einen oder der anderen Position fallen kann. Zur Herstellung praktischer Konkordanz muss daher „auf Stufe der Angemessenheit eine Abwägung erfolgen, die die jeweiligen Vor- und Nachteile bei der Verwirklichung der verschiedenen betroffenen Rechtsgüter in ihrer Gesamtheit einbezieht".[156]

Die Frage, ob und wann vor Sicherheitslücken zu warnen ist bzw. diese zu veröffentlichen sind, ist besonders kontrovers und sensibel. Im Lichte der genannten Abwägungsmaxime lässt sich für die an die Öffentlichkeit gerichtete

---

[151] Die Namensnennung ist aus Gründen der Verhältnismäßigkeit prinzipiell zurückhaltend vorzunehmen, vgl. für das Lebensmittelrecht *Teufer*, K&R 2013, 629 (632 f.).

[152] So etwa die persönliche Stellungnahme von *Pfitzmann* an den Innenausschuss des Bundestages vom 07.05.2009, S. 3, online abrufbar.

[153] Dazu sogleich.

[154] *Buchberger*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, BSIG, § 7 Rn. 3.

[155] So und mit möglichen Inhalten einer allgemeinen Dogmatik *Feik*, Öffentliche Verwaltungskommunikation, 2007, S. 187 ff. (191).

[156] BVerwG, BeckRS 2009, 41565 (Rn. 11).

Warnung vor Sicherheitslücken auf Grundlage von § 7 BSIG gleichwohl eine Strategie formulieren, die das Ermessen des BSI leiten sollte.

Im Ausgangspunkt können zwei Grundtypen der Veröffentlichung von Sicherheitslücken unterschieden werden. Jede Veröffentlichungsform kann jeweils spezifische Risiken, Kosten und kognitive Erfolge mit sich bringen.[157] Die beiden Extremmodelle sind auf der einen Seite die sog. Full Disclosure,[158] die frühzeitigste und zwingende Veröffentlichung von Sicherheitslücken, und auf der anderen Seite die Non-Disclosure,[159] die Nichtveröffentlichung von Schwachstellen. In der dem IT-Sicherheitsgesetz vorangegangenen Debatte wurde die Forderung laut, das BSI im Sinne einer Full Disclosure zur Veröffentlichung von IT-Sicherheitslücken zu verpflichten. Der Präsidiumsarbeitskreis „Datenschutz und IT-Sicherheit" der Gesellschaft für Informatik e.V. kritisierte den Entwurf des IT-Sicherheitsgesetzes unter anderem deshalb, weil der Entwurf nicht vorsah, Zero-Day-Vulnerabilities[160] zwingend zu veröffentlichen.[161] In diesem Zusammenhang steht auch die Kritik des Chaos Computer Club (CCC) an der Ankündigung des Bundesnachrichtendienstes, auf dem Schwarzmarkt sogenannte Zero-Day-Exploits aufzukaufen.[162] Die Entstehung eines Schwarzmarktes solle vielmehr dadurch verhindert werden, dass Sicherheitslücken konsequent veröffentlicht werden, damit diese geschlossen werden. Das hinter der Full Discolure stehende Sicherheitsprinzip kann als *security through transparency*, das des gegenläufigen Modells der Non-Disclosure als *security through obscurity* beschrieben werden. Nach diesem Ansatz soll die Sicherheit dadurch gewährleistet werden, dass der Kreis derjenigen, die Sicherheitslücken kennen,

---

[157] *Cencini/Yu/Chan*, Software Vulnerabilities, 2005, S. 9.

[158] *Schneier*, Full Disclosure of Security Vulnerabilities is a ‚Damned Good Idea', 2007, online abrufbar.

[159] Bundesamt für Sicherheit in der Informationstechnik, Handhabung von Schwachstellen, 2015, S. 1.

[160] Zero-Day-Vulnerabilities sind unveröffentlichte und nicht behobene Sicherheitslücken in der Software, die zu Exploits führen können.

[161] *Gesellschaft für Informatik*, IT-Sicherheitsgesetz schafft Unsicherheit, Meldung vom 18.11.2014, abrufbar unter: http://www.gi.de/aktuelles/meldungen/detailansicht/article/it-sicherheitsgesetz-schafft-unsicherheit.html.

[162] *Chaos Computer Club*, CCC verurteilt den Ankauf von „0days" durch den BND, Pressemitteilung vom 11.10.2014, abrufbar unter: http://www.ccc.de/de/updates/2014/0days-an-den-bnd. Angeregt wurde die Debatte auch durch die Ankündigung des BND, im Rahmen der Strategischen Initiative Technik (SIT) unter dem Codenamen „Nitidezza" Softwareschwachstellen mit einem Budget von 300 Millionen Euro einzukaufen. Dazu Spiegel Online vom 9.11.2014, BND will Informationen über Software-Sicherheitslücken einkaufen, abrufbar unter http://www.spiegel.de/spiegel/vorab/bnd-will-informationen-ueber-software-sicherheitsluecken-einkaufen-a-1001771.html.

möglichst klein gehalten wird. Die Sicherheitslücken sollen durch interne Qualitätssicherungsprogramme geschlossen werden.

Angesichts der Interessenkonstellation und der abweichenden Sicherheitsphilosophien spricht in Anwendung des Zweifelssatzes jedoch viel für einen Lösungsansatz, der nicht pauschal die zwingende Veröffentlichung von Sicherheitslücken favorisiert, sondern im Wege der beschränkten, verantwortungsbewussten Veröffentlichung (sog. Responsible Disclosure) die Interessen von *security* und *secrecy* in Einklang bringt.

Die Grundidee der Responsible Disclosure ist die koordinierte Veröffentlichung von Sicherheitslücken unter Zustimmung der Betroffenen, insbesondere also der Hersteller einer Soft- oder Hardware. Der Entdecker einer Sicherheitslücke kooperiert mit dem Hersteller bei Analyse und Behebung der Schwachstelle. Informationen zur Schwachstelle werden Dritten erst dann zugänglich gemacht, wenn die Risiken für die Betroffenen hinreichend minimiert werden konnten.

Zunächst sind die Motive für die Veröffentlichung von Sicherheitslücken zu erfassen.[163] Zum einen wird das primär technische Ziel sichergestellt, eine IT-Sicherheitslücke überhaupt zu identifizieren und zu schließen. Das Risiko für Anwender wie Nutzer wird durch die Behebung von Schwachstellen gesenkt. Die Kenntnis von Sicherheitslücken führt ferner dazu, durch die erkannten Fehler zu lernen und dadurch die Entwicklung von Erkennungswerkzeugen und -methoden voranzutreiben. In der Gesamtrechnung können so auch Zeit und Ressourcen gespart werden, die Einzelne für die Entdeckung von Lücken einsetzen. Grundgedanke der Veröffentlichung von Sicherheitslücken ist damit, den Herstellern und Anwendern Anreize zu schaffen, Maßnahmen gegen Sicherheitslücken zu ergreifen. Zudem wird auf den Markt für Sicherheitsprodukte eingewirkt und das Informationsniveau insgesamt gehoben. Der „mündige Anwender" soll durch das geschärfte Sicherheitsbewusstsein eine informierte Entscheidung über die Wahl der genutzten Software und Hardware treffen können.

Bei näherer Betrachtung der multipolaren Interessen- und Grundrechtskonstellation, die dem staatlichen Umgang mit Sicherheitslücken zugrunde liegt, erweist sich dann auch die Forderung einer pauschalen Veröffentlichung als zweifelhaft. Die Lösung des Problems der Veröffentlichung von Sicherheitslücken und der Warnung vor ihnen kann nur die Balancierung der konfligierenden sicherheitspolitischen Erwägungen sein. Gegen die pauschale Aufdeckung spricht, dass die Geheimhaltung von Informationen über Sicherheitslücken den Sicherheitsbehörden und Nachrichtendiensten ermöglicht, ihren Ermittlungs-

---

[163] Siehe exemplarisch den sog. Internet Draft der Internet Engineering Task Force, Responsible Vulnerability Disclosure Process, 2002, 1.4, abrufbar unter: http://tools.ietf.org/html/draft-christey-wysopal-vuln-disclosure-00#section-1.4.

maßnahmen und Aufklärungsoperationen nachzugehen. Die Sicherheitsbehörden haben ein genuines Interesse daran, die staatlich bekannten Sicherheitslücken für ihre Aufgaben zu nutzen.[164] Das Geheimhalten von Sicherheitslücken hat wiederum klare Dysfunktionen. Alle Klassen von Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Netzen und Daten, aber auch viele Formen der Internetkriminalität, zum Beispiel in der Wirtschaftsspionage, werden durch nicht gepatchte Sicherheitslücken ermöglicht. Die offenen Stellen bezeichnen immer auch Angriffspunkte für unbefugte und nicht berechtigte Dritte. Dem Einzelnen wird es zudem nicht ermöglicht, sich selbst aktiv zu schützen und entsprechende Vorkehrungen zu treffen. Ferner fördert die Nichtveröffentlichung die Aufrechterhaltung eines Schwarzmarktes für Informationen über Zero-Days, an dem staatliche Akteure unter Einsatz hoher Beträge an Steuergeldern, aber auch die organisierte Kriminalität beteiligt sind. Außerdem steigen die Preise durch eine zunehmende Nachfrage auf diesen Märkten.

Jeweils gewichtige Gründe sprechen sowohl für als auch gegen die (zwingende) Veröffentlichung von Sicherheitslücken. Sicherheit ist damit eine Frage der für vorzugswürdig befundenen Sicherheitsstrategie. Die sicherheitsrechtspolitischen Erwägungen kann das einfache Recht nur insofern abbilden, als grundrechtlich geschützte Interessen stets sorgfältig zu gewichten, zu bewerten und abzuwägen sind. Diesem Gebot wird der Veröffentlichungsmodus der Responsible Disclosure grundsätzlich gerecht. § 7 Abs. 1 S. 3 BSIG erlaubt durch das abgestufte Notifizierungsverfahren und die Einbindung von Herstellen die verantwortungsbewusste Veröffentlichung von Sicherheitslücken.[165] Die Verbreitung von IT-Sicherheitsinformationen kann nach § 7 Abs. 1 S. 4 BSIG dadurch beschränkt werden, dass nicht die Öffentlichkeit allgemein, sondern nur ausgewählte Personen und Institutionen informiert werden. Zugunsten höherer Anreize für Hersteller, Sicherheitslücken zügig zu schließen, ließe sich zwar *de lege ferenda* darüber nachdenken, die Entscheidung über eine Warnung nicht in das allgemeine („kann"), sondern in das gebundene Ermessen („soll") der Verwaltung zu legen. Die Entscheidung für eine Warnung würde so die Regel darstellen; nur bei entgegenstehenden Interessen in besonderen Fällen würde die Abwägungspflicht aktiviert. Allerdings wird eine gebundene Entscheidung der Anforderung einer Feinjustierung, wie sie in sicherheitskritischen Bereichen erforderlich ist, nicht gerecht. Zeitpunkt, Art und Umfang einer Warnung sind in jedem Einzelfall darauf abzustimmen, ob durch die Information über eine Sicherheitslücke das Ausnutzen für Angriffe gefördert wird. Die Vorschrift kann

[164] Vgl. *Pohl*, DuD 2007, 684 (685).

[165] Vgl. für CERT-Bund, BSI, RFC-2350, 4.2.: CERT-Bund strongly supports responsible disclosure principles and therefore cooperates with vendors in order to handle relevant security issues within their products.

daher hinsichtlich der Umsetzung des Gedankens der Responsible Disclosure als Vorbild für die Ausgestaltung entsprechender Befugnisse in anderen Mitgliedstaaten herangezogen werden.

5. Empfehlungen von Sicherheitsmaßnahmen und Sicherheitsprodukten

Das BSI kann zur Gefahrenabwehr konkrete Sicherheitsmaßnahmen sowie den Einsatz bestimmter Sicherheitsprodukte empfehlen (a). Bei empfehlendem Informationshandeln stellt sich das Problem besonderer Verstärkungsdynamiken (b). Im Zusammenhang mit der Darstellung von Risikoinformationen bietet es sich für die Darstellung von Informationen an, auf Erkenntnisse der Verhaltensökonomie zurückzugreifen (c).

a) Empfehlung bei Gefahrenverdacht

Das BSI kann nach § 7 Abs. 2 BSIG Sicherheitsmaßnahmen und den Einsatz bestimmter Sicherheitsprodukte empfehlen. Eine unionsrechtliche Vorgabe besteht für diese Kompetenz nicht.

Ob die Empfehlung an die Öffentlichkeit gerichtet sein darf, ergibt sich nicht eindeutig aus dem Wortlaut des § 7 Abs. 2 BSIG. Der Passus „kann das Bundesamt die Öffentlichkeit“ in § 7 Abs. 2 S. 1 BSIG bezieht sich grammatikalisch nur auf die Warnbefugnis. Bei binnensystematischer Betrachtung kann auch nicht im Umkehrschluss aus § 7 Abs. 1 S. 1 Nr. 2 BSIG, der eine Befugnis für nicht an die Öffentlichkeit gerichtete Empfehlungen statuiert, auf die Öffentlichkeit als zulässigen Adressaten geschlossen werden, da der Unterschied der beiden Kompetenzen darin begründet liegen kann, dass § 7 Abs. 2 S. 1 BSIG die Befugnis um die mögliche Nennung der Bezeichnung und des Herstellers des betroffenen Produkts erweitert. Andererseits ergibt sich aus dem Gesetz auch kein ausdrücklicher Ausschluss der Öffentlichkeit. Jedenfalls kommt wegen der Bindung an die Aufgabe des BSI zur Beratung und Warnung ein breiter Adressatenkreis für die Empfehlung in Betracht (vgl. § 3 Abs. 1 S. 2 Nr. 14 BSIG).

Empfehlungen können als Aussagen verstanden werden, die dem angesprochenen Adressatenkreis bestimmte Verhaltensweisen nahelegen.[166] Die Empfehlung durch staatliche Stellen ist kein Hinweis auf das rechtliche Dürfen oder Müssen und zielt auch nicht auf die Beschränkung des ohnehin nicht rechtlich determinierbaren freien Willens. Sie ist die staatlicherseits erwünschte Freiheitsausübung. Die Empfehlung impliziert dadurch die Möglichkeit eines im Vergleich zu anderen zulässigen Verhaltensweisen vernünftigeren Verhaltens.[167]

---

[166] *Feik*, Öffentliche Verwaltungskommunikation, 2007, S. 26.

[167] *Gramm*, Der Staat 30 (1991), 51 (67).

Durch eine Verhaltenempfehlung wird der angesprochenen Person jedoch nicht der Handlungsspielraum genommen.

Die Empfehlung von konkreten Schutzmaßnahmen und Sicherheitsprodukten zielt primär auf den Rechtsgüterschutz. Daneben kann der Empfehlung eine kognitive Dimension beigemessen werden. In kognitiver Hinsicht verfolgt die Empfehlungstätigkeit das Ziel, die Sicherheitsvorfälle dadurch zu vermeiden oder zu bewältigen, dass die Adressaten durch entsprechende Informationen befähigt werden, zu handeln oder Kenntnis über geeignete Abhilfemaßnahmen zu erlangen. Die informationsverwaltungsrechtliche Bedeutung der Empfehlung besteht vor allem darin, dass den Behörden weitere Eingriffsmittel neben den Warnhinweisen und der Veröffentlichung von Sicherheitslücken nicht zur Verfügung stehen, um proaktiv zur Informationssicherheit beizutragen. Daher ist insbesondere die Bereitstellung von Empfehlungen als unverzichtbare Grundlage für die Sicherheitsgewährleistung anzusehen.[168] Praktisch sehr bedeutsam sind daher außerhalb des Gefahrenverdachts die allgemeinen Hinweise und Empfehlungen, wie der IT-Grundschutz nach BSI oder die ISi-Reihe.[169]

Trotz Verbleiben des Handlungsspielraums sind an die Empfehlung Anforderungen zu stellen, die sich aus ihrem Charakter als einer Kombination von Tatsachenfeststellung und Werturteil ergeben.[170] Daher kann eine konkrete Verhaltensempfehlung, die auf eine Gefahrensituation gestützt ist, die Wirkung einer Warnung erreichen.[171] Je näher die Empfehlung einer Warnung kommt, d. h., je

---

[168] Vgl. Stellungnahme des BSI von *Andreas Könen* zum Expertengespräch der Projektgruppe Zugang, Struktur und Sicherheit im Netz am 28.11.2011, abrufbar unter http://www.bundestag.de/internetenquete/dokumentation/Zugang_Struktur_und_Sicherheit_im_Netz/PGZustrSi_2011-11-28_oeffentliches_Expertengespraech/PGZuStSi_2011-1128_Expertengespraech_Stellungnahme_Koenen.pdf; des Weiteren *Deutscher Bundestag*, Enquete-Kommission Internet und Digitale Gesellschaft, Teilbericht der Projektgruppe Zugang, Struktur und Sicherheit im Netz, A-Drs. 17(24)064, S. 81 f.

[169] BSI-Standards zur Internet-Sicherheit (ISi-Reihe), deren Ziel es ist, „Behörden und Unternehmen umfassende Informationen zur Verfügung zu stellen, damit diese ihre Internet-Aktivitäten möglichst eigenständig sicher neu aufbauen, erweitern oder anpassen können." Die ISi-Reihe besteht nach Fachthemen geordneten Modulen, die Varianten für individuelle Bedürfnisse berücksichtigen und dem Schutzbedarf angepasst sind. Die Module sind nach Adressat gegliedert, wozu IT-Fachleute, IT-Führungskräfte gehören. Enthalten sind generische oder produktbezogene Checklisten als Hilfestellung für Administratoren, Programmierer und Web-Entwickler.

[170] *Heintzen*, NuR 1991, 301 (304).

[171] *Kloepfer*, Staatliche Informationen als Lenkungsmittel, 1998, S. 17; *Schürmann*, Öffentlichkeitsarbeit, 1992, S. 105. Die Warnung ist negativ auf das Unterlassen eines bestimmten Verhaltens gerichtet, während die Empfehlung positiv auf ein bestimmtes Verhalten zielt. Die Empfehlung, ein bestimmtes Programm zu verwenden, kann der Warnung entsprechen, nicht ohne dieses Programm zu verfahren.

wahrscheinlicher ein Eingriff in die Grundrechte Dritter bewirkt wird, desto eher sind an die Empfehlung diejenigen Anforderungen zu stellen, die auch für Warnungen gelten.[172] Außerhalb des eingriffsrelevanten Verhaltens ergeben sich grundrechtliche Gleichheitsprobleme.[173] Ein Unternehmen darf nicht unsachlich bevorteilt oder benachteiligt werden. Die richtige Tatsachenfeststellung ist folglich Rechtmäßigkeitsvoraussetzung.[174] Die in der Empfehlung liegende immanente Wertung muss auf einem sachlichen Grund fußen. Die Wertung darf nicht durch sachfremde Erwägungen geleitet sein oder willkürlich erfolgen.[175] Die Anhaltspunkte und Kriterien, auf die sich die Behörde stützt, sind gerichtlich vollumfänglich nachprüfbar.[176] Das Gesetz stellt dem Anwender für den Ausspruch einer Empfehlung im Übrigen weder konkretisierende Kriterien zur Seite noch gibt es ein einzuhaltendes Verfahren vor. Das dem Telos des Responsible Disclosure entsprechende Verfahren ist ausdrücklich nicht vorgesehen, da § 7 Abs. 2 auf die Vorabinformation der Hersteller, wie sie § 7 Abs. 1 S. 3 BSIG vorsieht, nicht Bezug nimmt.

Um in der Empfehlung bestimmte Produkte und Hersteller zu benennen, müssen hinreichende Anhaltspunkte für das Vorliegen einer Gefahr gegeben sein. Zwar sprechen beide Tatbestandsvarianten, § 7 Abs. 1 S. 1 Nr. 2 bzw. § 7 Abs. 2 S. 1 BSIG, von Empfehlungen zu Sicherheitsmaßnahmen und zum Einsatz bestimmter Sicherheitsprodukte. Die Formulierung „hinreichende Anhaltspunkte" in § 7 Abs. 2 S. 1 BSIG legt aber nahe, dass eine konkrete Empfehlung bestimmter Sicherheitsmaßnahmen bzw. konkret bezeichneter Sicherheitsprodukte einen Gefahrenverdacht voraussetzt.[177] Ein Gefahrenverdacht liegt vor, wenn zwar Anhaltspunkte für eine Gefahr ersichtlich sind, der Behörde aber bewusst ist, dass die erkennbare Sachlage mit Unsicherheiten behaftet ist und eine sichere Prognose des Schadenseintritts nicht zulässt.[178] Die vorliegenden Anhaltspunkte und Tatsachen müssen noch keine Gefahr begründen, aber zu dem starken Verdacht führen, dass sich die Sachlage zu einer Gefahr verdichten könnte.[179]

---

[172] *Feik*, Öffentliche Verwaltungskommunikation, 2007, S. 26.

[173] Vgl. *Gusy*, NJW 2000, 977 (986).

[174] Hält man die an die Öffentlichkeit gerichtete Empfehlung für zulässig, findet § 7 Abs. 2 S. 2 BSIG Anwendung. Fehlinformationen sind danach zu korrigieren, wenn die Voraussetzungen *ex post* nicht vorliegen.

[175] *Feik*, Öffentliche Verwaltungskommunikation, 2007, S. 26.

[176] *Buchberger*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, BSIG, § 7 Rn. 6.

[177] Vgl. *Buchberger*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, BSIG, § 7 Rn. 6.

[178] *Kugelmann*, Polizei- und Ordnungsrecht, 2. Aufl. 2012, Rn. 125; *Schoch*, Polizei- und Ordnungsrecht, in: ders. (Hrsg.), Besonderes Verwaltungsrecht, 15. Aufl. 2013, Kap. 2, Rn. 95 f.

[179] *Kugelmann*, Polizei- und Ordnungsrecht, 2. Aufl. 2012, Rn. 125.

Der Modus der Empfehlung ist nicht vorgegeben. Diese kann verbal oder durch schriftliche Publikation erfolgen. Möglich erscheinen jedoch auch optische Zeichen wie Gütesiegel oder Symbole. Auch darin kann der staatliche Wunsch eines bestimmten Konsumverhaltens deutlich erkennbar sein.

b) Problem eigendynamischer Verstärkungseffekte

Ein besonderes Problem bei Produktempfehlungen und Warnungen sind die möglicherweise damit verbundenen eigendynamischen Verstärkungseffekte. Stellt staatliches Informationshandeln einmal die Regel dar, kann möglicherweise dem Unterlassen ein Informationswert unterstellt werden („es wird schon alles in Ordnung sein“[180]). Das Informationshandeln muss berücksichtigen, dass staatliche Tätigkeit eine Erwartungshaltung aufbauen kann, die ein Gefühl der Sicherheit nach sich zieht und die enttäuscht werden kann. Zugleich besteht die Gefahr, dass das Informationsverhalten eine Dynamik annimmt, in der die zunächst zurückhaltende (negative) Informationspolitik sich zu einer Politik mit Positivanreizen verstärkt.[181] Aus Warnungen in Ausnahmefällen vor IT-Schwachstellen werden zunehmend Empfehlungen konkreter Produkte. Mit anderen Worten, es besteht die Gefahr, dass an die Stelle aufklärenden Informationshandelns ein edukatorisches Staatshandeln tritt.[182] Insgesamt zeigt sich an der Befugnis des § 7 BSIG, wie nah das Aufklärungshandeln an der Wirtschaftspolitik ist und daneben Funktionen des Verbraucherinformationsrechts übernimmt, denn Letzteres soll die „Auswahl- und Entscheidungskompetenz von Verbrauchern in der Marktwirtschaft“ verbessern.[183] Doch die ihrerseits mit Unwägbarkeiten verbundene Verhaltensbeeinflussung, die durch eine mit staatlicher Autorität ausgesprochene Warnung und Empfehlung bewirkt wird, kann mit unvermeidbaren nachteiligen Spill-over-Effekten verbunden sein.[184] Aus

---

[180] *Gusy*, Die Informationsbeziehungen zwischen Staat und Bürger, in: Hoffmann-Riem et al. (Hrsg.), Grundlagen des Verwaltungsrechts, Band II, 2. Aufl. 2012, § 23, Rn. 16 mit Verweis auf BVerfGE 105, 252 (269), 279 (302).

[181] *Augsberg*, Informationsverwaltungsrecht, 2014, S. 206.

[182] Dazu *Lüdemann*, Edukatorisches Staatshandeln, 2004.

[183] *Schoch*, NJW 2010, 2241 (2242).

[184] *Augsberg*, Informationsverwaltungsrecht, 2014, S. 207, der auch auf die Kritik zu der im Kern im EU-Verbraucherrecht verankerten Zielvorstellung einer Markttransparenz verweist, die vorgebracht wird bei *Rehberg*, Der staatliche Umgang mit Information – Das europäische Informationsmodell im Lichte von Behavioral Economics, in: Eger/Schäfer (Hrsg.), Ökonomische Analyse der europäischen Zivilrechtsentwicklung, 2007, S. 284 ff. Ferner als Beispiel VG Köln, Beschluss v. 11.03.1999 – 20 L 3737/98, CR 1999, 557 (558): Der Firmenname der Ast. war in einer Äußerung des Bundesdatenschutzbeauftragten nicht benannt. Die grundrechtsbeeinträchtigende Wirkung sah das Gericht aber durch die anschließende na-

der Möglichkeit solcher unerwarteter grundrechtsrelevanter Nebeneffekte folgt das Gebot einer behutsamen Anwendung der Empfehlungskompetenz.

c) Besondere Anforderungen an die Informationsdarstellung

Bei Publikumsinformationen in Form von Empfehlungen ist es außerdem naheliegend, verhaltenswissenschaftliche Erkenntnisse in die rechtliche Betrachtung mit einzubeziehen.[185] Die Steuerungswirkungen des Rechts auf menschliches Verhalten zu betrachten, ist Ansatz der verhaltensökonomisch geprägten Disziplin Behavioral Law and Economics. Für das Informationshandeln ist dabei vor allem vor dem Hintergrund, dass dieses eine bestimmte Risikoperzeption der Öffentlichkeit bewirkt, bedeutsam, dass in Erweiterung des neuklassischen Rationalitätsmodells auch kognitive Verzerrungen in die Betrachtung mit einbezogen werden.[186] Zentral ist dabei die Erkenntnis, dass entgegen den Annahmen von Theorien rationaler Entscheidung (*rational choice*), nach denen Menschen unter Berücksichtigung der optimalen Menge an Informationen sowie anderer Inputs ihren Nutzen maximieren und in diesem Sinne rational handeln, den handelnden Akteuren eine fehlerfreie Informationsverarbeitung gerade nicht gelingt.[187]

Empfehlungen können bei den Adressaten vor allem dann zu risikobehafteten Entscheidungen führen, wenn ihnen die möglichen Nebenwirkungen und Folgen einer Entscheidung, die sich auf eine bestimmte Information aus der Empfehlung stützt, nicht von vorneherein bekannt sind. Gerade dem einzelnen (privaten) Verbraucher kann es widerfahren, dass er sich zur Befriedigung seiner Präferenzen und zum Schutz persönlicher Güter (etwa der Sicherheit der eigenen, sozial relevanten und sensiblen Daten) auf den Vorsorgegedanken einlässt und überflüssige, Risiken missachtende Entscheidungen trifft (etwa ein vermeintlich sichereres IT-Produkt implementiert). Die durch negative Folgen entstehende Verunsicherung kann sich langfristig nachteilig für die Vertrauen in Anspruch nehmende staatliche Informationstätigkeit auswirken.[188] Es stellt sich daher die Frage, wel-

---

mentliche Nennung in den Medien gegeben, die nicht bloß allgemein und als Reflex gegeben wäre.

[185] Zur Verwendbarkeit verhaltenswissenschaftlicher Erkenntnisse im Recht *Engel*, Behavioral Law and Economics – eine kritische Einführung, in: ders./Englerth/Lüdemann/Spiecker gen. Döhmann (Hrsg.), Recht und Verhalten – Beiträge zu Behavioral Law and Economics, 2007, S. 363 (383); allgemein *Sunstein* (Hrsg.), Behavioral Law and Economics, 2000, passim.

[186] *Jolls*/*Sunstein*/*Thaler*, Stanford Law Review 50 (1998), 1471 (1476 ff.).

[187] *Englerth*, Behavioral Law and Economics – eine kritische Einführung, in: Engel/ders./Lüdemann/Spiecker gen. Döhmann (Hrsg.), Recht und Verhalten – Beiträge zu Behavioral Law and Economics, 2007, S. 60 (102).

[188] Zu den Internet-Milieus zu Vertrauen und Sicherheit im Netzt siehe Deutsches Institut

che Beschaffenheit Informationen aufweisen müssen, damit einem Vertrauensverlust der Öffentlichkeit prophylaktisch begegnet werden kann.

Die Problemstellung lässt näher am fiktiven Beispiel einer digitalen Pandemie darstellen. Im Falle einer europäischen digitalen Pandemie mit Computervieren, -würmern oder anderer Schadsoftware könnte eine NIS-Behörde eine Warnung verbunden mit der Empfehlung einer Abhilfemaßnahme aussprechen.

Um Nutzen und Risiken einer mehr oder weniger komplexen Abhilfemaßnahme abwägen zu können, benötigen die Adressaten Zusatzinformationen über die Implikationen der Maßnahme (z. B. über die mit dem Einsatz einer bestimmten Sicherheitsmaßnahme verbundenen Risiken). Vor dem Hintergrund verhaltenswissenschaftlicher Erkenntnisse kann angezweifelt werden, dass das bloße Bereitstellen solcher Informationen ausreicht. Vielmehr muss eine bestimmte Darstellung der Information erfolgen, um fehlerhafte Wahrnehmungs- und Verarbeitungsvorgänge zu vermeiden („Comprehension is as essential as disclosure").[189]

Als Schutzmechanismus gegen normativ unerwünschte Folgen von Risikoinformationen kommt ein rechtliches Informationsdarstellungsgebot in Betracht.[190] Gesetzliche Minimalanforderungen bestimmter Darstellungsformen sind dem Recht nicht unbekannt. Im Zivilrecht bestehen bereits vielfach Darstellungsregelungen. Das Lauterkeitsrecht beispielsweise sorgt dafür, dass der Unternehmer im Rahmen des Möglichen und Zumutbaren alle Informationen preisgibt, „die der durchschnittliche Verbraucher je nach den Umständen benötigt, um eine informierte geschäftliche Entscheidung zu treffen" (Art. 7 Abs. 1 UGP-RL[191]).[192] Darin kann die Berücksichtigung der Erkenntnis gesehen werden, dass bestimmte Darstellungen von Preisen zur Folge haben können, dass Verbraucher den Preis eines Produktes als unter dessen tatsächlichem Wert liegend einschätzen und so zu einer irregeleiteten Kaufentscheidung gelangen.[193] Im Datenschutzrecht wird das Gebot, eine für die Öffentlichkeit bestimmte In-

---

für Vertrauen und Sicherheit im Internet (DIVSI), DIVSI Milieu-Studie zu Verstreuen und Sicherheit im Internet, 2012, S. 15 ff.

189 *Pflug*, Pandemievorsorge, 2013, S. 223.

190 Im Zusammenhang von Impfempfehlungen *Spiecker gen. Döhmann*/*Kurzenhäuser*, Das rechtliche Darstellungsgebot – Zum Umgang mit Risikoinformationen am Beispiel der Datenerhebung im Bundesinfektionssschutzgesetz (IfSG), in: Engel/Englerth/Lüdemann/Spiecker gen. Döhmann (Hrsg.), Recht und Verhalten – Beiträge zu Behavioral Law and Economics, 2007, S. 133 (133 ff., 143).

191 Richtlinie 2005/29/EG über unlautere Geschäftspraktiken.

192 *Köhler*, in: ders./Bornkamm, UWG, 34. Aufl. 2016, § 1 Rn. 18.

193 *Spiecker gen. Döhmann*/*Kurzenhäuser*, Das rechtliche Darstellungsgebot – Zum Umgang mit Risikoinformationen am Beispiel der Datenerhebung im Bundesinfektionssschutzgesetz (IfSG), in: Engel/Englerth/Lüdemann/Spiecker gen. Döhmann (Hrsg.), Recht und Verhalten – Beiträge zu Behavioral Law and Economics, 2007, S. 133 (157).

formation „präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache“ abzufassen, aus dem Grundsatz der Transparenz abgeleitet.[194]

Wie im Zivilrecht spielen auch im staatlichen Informationshandeln die Autonomie und die Freiwilligkeit der anschließenden Entscheidung eine tragende Rolle. Die Gefahr von irrationalen Entscheidungen ist im Kontext der Informationstätigkeit zum Thema Internetsicherheit nicht weniger ausgeprägt.

Eine normative Vorgabe zur Darstellung von Publikumsinformationen enthält § 7 BSIG indes nicht. Die konkrete Ausgestaltung einer spezifischen Darstellung stellt den Gesetzgeber ob der Vielzahl zu berücksichtigender Erkenntnisse über die Rezeption von Informationen und wegen des Wandels in der verhaltenswissenschaftlichen Forschung vor rechtstechnische Schwierigkeiten.[195] Aus dem Grundsatz der Rechtmäßigkeit des Verwaltungshandelns ergibt sich gleichwohl das Richtigkeitsziel der Risikoangemessenheit eines Informationshandelns. Zumindest in der Rechtsanwendung sollte daher eine Offenheit für die Einbeziehung von als gesichert geltenden verhaltenswissenschaftlichen Erkenntnissen bestehen.[196]

Dazu gehören bei Risikoinformationen die Verfügbarkeitsheuristik, die Wahrscheinlichkeitsvernachlässigung, die Verlust-Aversion und die Kaskadeneffekte.

Heuristiken prägen das Entscheidungsverhalten des Einzelnen und stellen kognitive Simplifizierungsstrategien dar. Auf sie greifen Menschen insbesondere dann zurück, wenn sie über Risiken nachdenken.[197] In der individuellen Informationsverarbeitung kann es dazu kommen, dass auf geringe Risiken unverhältnismäßig reagiert wird, weil Risiken kognitiv verfügbar sind. Dies ist vor allem dann der Fall, wenn Informationen zeitlich kurz zurückliegen oder noch besonders präsent sind (etwa durch Medienberichte). Entscheidungen auf Grundlage rezipierter Informationen werden nach einer gewissen Verfügbarkeitsheuristik getroffen.[198] Aktuell verfügbaren Informationen wird demnach gegenüber der sog. statistischen Base Rate überproportionales Gewicht eingeräumt. Zur Vermeidung von Fehlreaktionen bei den Adressaten einer Empfehlung oder Warnung sollte daher, wenn möglich, die Risikowahrscheinlichkeit indiziert werden.

---

[194] Erwägungsgrund 58 DS-GVO.

[195] Vgl. für die Informationsdarstellung im Kontext des IfSG *Spiecker gen. Döhmann*/*Kurzenhäuser*, Das rechtliche Darstellungsgebot – Zum Umgang mit Risikoinformationen am Beispiel der Datenerhebung im Bundesinfektionsschutzgesetz (IfSG), in: Engel/Englerth/Lüdemann/Spiecker gen. Döhmann (Hrsg.), Recht und Verhalten – Beiträge zu Behavioral Law and Economics, 2007, S. 133 (145, 147).

[196] Vgl. für die Gesetzgebung *Sunstein*, Gesetze der Angst, 2007, S. 141.

[197] *Tversky*/*Kahnemann*, Science 185 (1974), 1124 (1124).

[198] Vgl. *Tversky*/*Kahnemann*, Psychological Review 90 (1983), 293 (295 ff.).

Eine weitere zu berücksichtigende Verhaltensweise ist die Wahrscheinlichkeitsvernachlässigung. Menschen neigen dazu, stark emotional aufgeladene Risiken für wahrscheinlicher zu halten als solche, denen sie ohne oder mit nur geringem emotionalem Engagement gegenüberstehen, und zwar auch dann, wenn die Wahrscheinlichkeit ihrer Realisierung objektiv größer ist als subjektiv angenommen.[199] Daraus folgt zunächst, dass staatliches Informationshandeln das spezifische Verhältnis von Kognition und Emotion in Konstellationen von Risikobewertungen durch Einzelne reflektieren und sich der Risiken des Informationshandelns bewusst machen sollte.

Mit der Rational-Choice-Annahme im Konflikt stehen darüber hinaus Risikoentscheidungsverhaltensweisen, nach denen Menschen Gütern und Rechten einen höheren Wert beimessen, je länger sie diese besitzen. Diese Erscheinung wird als Besitz-Effekt (*endowment effect*) charakterisiert.[200] Der Gedanke der Verlustaversion (*loss aversion*) versucht in diesem Zusammenhang zu erklären, dass Menschen einen Verlust schwerer gewichten als Gewinne in derselben Höhe.[201] Individuelle Entscheidungen konzentrieren sich demnach primär auf den Erhalt des Status quo statt auf eine potenzielle Verbesserung. Empfehlungen und Warnungen können wirksamer sein, wenn in der Kommunikation einer Information dieser Effekt Berücksichtigung findet.

Durch Informationshandeln können nicht zuletzt nur schwer absehbare Kaskadeneffekte entstehen. Gemeint sind soziale Kaskaden, deren typisches Merkmal es ist, dass beteiligte Personen genau dasjenige Signal verstärken, durch das sie selbst beeinflusst worden sind. Risikoentscheidungen erfordern ökonomisch betrachtet kostenintensive Recherchen. Menschen neigen daher dazu, auf einfach verfügbare Informationen (etwa in Form scheinbar repräsentativer Anekdoten) zurückzugreifen. In sozialen Kontexten entstehen so Informationskaskaden, durch die persönlich präferierte Informationen weitererzählt werden, die objektiv falsch sein können. Je nach Vertrauensverhältnis können Zuhörer der Erzählung schnell von der Plausibilität, ein ernsthaftes Risiko liege vor, überzeugt sein. Im äußersten Fall einer solchen sozialen Konstruktion können so Ängste hinsichtlich von Gefahren geschürt werden, die realiter so nicht existieren.[202]

---

[199] Vgl. *Slovic*/*Fischhoff*/*Lichtenstein*, Facts and Fears: Understanding Perceived Risk, in: Schwing/Albers Jr. (Hrsg.), Societal risk assessment: How safe is safe enough?, 1980, S. 181 ff.; *Loewenstein*/*Weber*/*Hsee*/*Welch*, Psychological Bulletin 127 (2001), 267 (269).

[200] *Englerth*, Behavioral Law and Economics – eine kritische Einführung, in: Engel/ders./Lüdemann/Spiecker gen. Döhmann (Hrsg.), Recht und Verhalten – Beiträge zu Behavioral Law and Economics, 2007, S. 60 (84).

[201] *Kahneman*/*Tversky*, Econometrica 47 (1979), 263 (263 ff.).

[202] *Kuran*/*Sunstein*, Stanford Law Review 51 (1999), 683 (717).

Zusammenfassend muss das Informationsverwaltungsrecht als informiertes Recht an der Schaffung von Vertrauen interessiert sein und berücksichtigen, dass staatliche Interventionen unter Umständen sogar „Möglichkeiten und Anreize für Individuen beseitigen, ihr eigenes Wissen über die Bewältigung von Vertrauensrisiken zu erweitern."[203] Konkret folgt daraus neben dem Gebot maßvoller Informationstätigkeit, dass in Empfehlungen die Wahrscheinlichkeiten von Risiken verfügbarer gemacht und ggf. geringe Risikowahrscheinlichkeiten besonders in der Darstellung der Information betont werden. Die Darstellung der Risiken für persönliche Güter kann tendenziell dysfunktionalen Informationskaskaden entgegenwirken. Dies setzt bereits Maßnahmen gegen die verwaltungsinterne Risikoverzerrung voraus. Eine Erweiterung des Darstellungsgebots auf die Risikowahrscheinlichkeit wirkt insofern präventiv auf die Amtsträger ein und beugt der Weitergabe überzogener Risikowahrnehmung vor. In europäischer Perspektive drängt sich der Gedanke der Harmonisierung eines IT-sicherheitsbezogenen Informationshandelns auf. Gerade im Fall einer länderübergreifenden „digitalen Pandemie" erscheint eine Zentralisierung in tatsächlicher Hinsicht sinnvoll, da föderale oder mitgliedstaatliche Divergenzen in der Bewertung bestimmter Risiken Ungewissheit verstärken und zu einer weiteren Verunsicherung führen. Die Herstellung eines institutionalisierten Einklangs der Informationstätigkeit unter der Nutzung der ENISA und der europäischen Kooperationsstrukturen erscheint vor diesem Hintergrund angezeigt.

II. Individualbezogene Informationstätigkeit

Das individualbezogene Informationshandeln richtet sich an einen bestimmten oder bestimmbaren Adressatenkreis. Eine Warnung vor Gefahren auf dem Gebiet der Internetsicherheit kann etwa den von einem Sicherheitsvorfall betroffenen Personenkreis adressieren. Formalisierte individualbezogene Informationsverfahren bestehen für Betreiber kritischer Infrastrukturen (1.) und für datenschutzrechtlich Verantwortliche sowie für Betroffene von Datenschutzverletzungen (2.). Für die gezielte Informationstätigkeit von Bedeutung sind nicht zuletzt informelle Zusammenschlüsse (3.).

1. Betreiber kritischer Infrastrukturen

Die Betreiber kritischer Infrastrukturen werden vom BSI mit bestimmten sicherheitsrelevanten Informationen versorgt. Gemäß § 8b Abs. 2 Nr. 4 in Verbindung mit Nr. 1 bis 3 BSIG unterrichtet das BSI die Betreiber über sie betref-

[203] *Engel*, Vertrauen: ein Versuch, in: Preprint 1999/12, S. 44.

fende Informationen. Dies sind nach § 8b Abs. 2 Nr. 4 BSIG die wesentlichen Informationen für die Abwehr von Gefahren für die Sicherheit der Informationstechnik, insbesondere Informationen zu Sicherheitslücken, Schadprogrammen, Angriffe und dabei beobachtete Vorgehensweisen, Analyseergebnisse über potenzielle Auswirkungen auf die Verfügbarkeit der Infrastruktur und das Lagebild bezüglich der Sicherheit. Übermittelt werden die Informationen gemäß § 8b Abs. 3 S. 3 BSIG nicht direkt an die Betreiber kritischer Infrastrukturen, sondern an die von ihnen nach S. 1 für die Kommunikation zu benennende Kontaktstelle. Klarstellend verweist § 8b Abs. 5 BSIG auf die Möglichkeit, für Betreiber des gleichen Sektors ergänzend zu den Kontaktstellen eine gemeinsame Ansprechstelle zu benennen. Damit können bestehende und genutzte Kommunikationsstrukturen genutzt und erweitert werden. Entscheidend ist, dass der Übermittlungsprozess nachvollziehbar und auditierbar ist.[204]

Die Unterrichtungsverpflichtung bezieht sich demnach nicht auf sämtliche gesammelte und analysierte Informationen. Die Informationen müssen einen konkreten Bezug zur Informationstechnik eines Infrastrukturbetreibers aufweisen. Das BSI hat damit nur solche Informationen zu geben, welche für die Betreiber so relevant sind, dass sie für die Abwehr von Gefahren für die Informationssicherheit erforderlich sind. Bei der Unterrichtung sind die schutzwürdigen Interessen anderer (betroffener) Betreiber sowie die potenziellen Folgen einer Weitergabe zu berücksichtigen. Greift die Weitergabe von Informationen in die geschützten Interessen anderer meldender Betreiber ein, ist nur dann zu unterrichten, wenn dies verhältnismäßig ist. Gleichwohl sind die Informationen zeitnah („unverzüglich“) weiterzugeben.

In dieser Pflicht zur Information der Infrastrukturbetreiber ist die eigentliche Legitimation für IT-Meldepflichten zu sehen. Die durch die Meldepflichten ermöglichte staatliche Informationsgenerierung ist damit nicht Selbstzweck der NIS-Verwaltung. Die Informationspflicht der NIS-Behörde ist das Spiegelbild zur Meldepflicht der Betreiber. Auf der Grundlage der Informationspflicht werden die gemeldeten Informationen über die Kontaktstelle im Sinne des § 8b Abs. 3 BSIG zurückgespeist. Dabei sind die Informationen an die Betreiber bereits ausgewertet und nehmen Bezug auf das Lagebild in der Informationssicherheit. Im Gegenzug zur Meldepflicht erhalten die Betreiber im Zweifel ein Mehrfaches an Information und Expertise zurück.

Die verpflichtende Unterrichtung der Betreiber ist unionsrechtlich nicht vorgesehen. Die Logik eines Informationstausches im Sinne eines „Gebens und Nehmens“ zwischen der NIS-Verwaltung und den Unternehmen ist indes in Art. 14 Abs. 5 UAbs. 2 NIS-RL angelegt. Die NIS-Behörde oder das CSIRT

[204] BT-Drs. 18/4096, S. 28.

stellt demnach, wenn es unter den Umständen möglich ist, einem Betreiber, der einen Sicherheitsvorfall meldet, relevante Informationen für die wirksame Bewältigung des Sicherheitsvorfalls zur Verfügung.

Das BSIG schafft über die unionsrechtliche Vorgabe hinaus ein allgemeines Beratungs- und Informationsrecht gegenüber dem BSI. Die Betreiber können das BSI nach § 3 Abs. 3 BSIG ersuchen, damit dieses bei der Sicherung der Informationstechnik berät und unterstützt. Ob das BSI dem Ersuchen entspricht, steht im Ermessen der Behörde. Es darf dabei jedoch auf qualifizierte Sicherheitsdienstleister verweisen. Eine besondere Unterstützung kann in diesem Zusammenhang darstellen, dass das BSI gemäß § 8b Abs. 6 BSIG im Falle von Störungen der informationstechnischen Systeme kritischer Infrastrukturen die Mitwirkung des Herstellers der Systeme bei der Störungsbeseitigung verlangen kann. Über den Verweis in § 8b Abs. 6 S. 2 BSIG auf § 8c Abs. 3 BSIG gilt diese Anordnungsbefugnis auch für Störungen bei Telekommunikationsnetzbetreibern und -diensteanabietern.

Gleichwohl sind die Telekommunikationsunternehmen nicht in den unmittelbaren Informationsaustausch mit einbezogen. Durch § 8c Abs. 3 BSIG gelten die Verpflichtungen zur Einrichtung einer Kontaktstelle und zur Unterrichtung durch das BSI gerade nicht für Betreiber kritischer Infrastrukturen, soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen. Eine rechtliche Notwendigkeit für die Ausnahme dieser Infrastrukturen aus dem System der individualbezogenen Informationsmaßnahmen ist mit Blick auf den Mehrwert nicht ersichtlich. Möglich erscheint aber die indirekte Information über die Bundesnetzagentur, da diese nach § 8b Abs. 2 Nr. 4 b) BSIG vom BSI unverzüglich über die zur Erfüllung ihrer Aufgaben erforderlichen Informationen unterrichtet. Die unmittelbare Information der Betreiber und Anbieter ist zwar nicht wie für das BSI gesetzlich vorgesehen. Das steht der informellen individualbezogenen Weitergabe rechtlich nicht geschützter Informationen aber nicht entgegen.

2. Information in informellen Zusammenschlüssen

Die NIS-Behörde kann sich zur Bereitstellung von Erkenntnissen abseits der gesetzlich formalisierten Informationswege informeller Kooperationsstrukturen bedienen. Der Informationsaustausch im Rahmen öffentlich-privater Partnerschaften ist sowohl auf europäischer als auch auf nationaler Ebene insbesondere mit Blick auf die Sicherheit in kritischen Infrastrukturen von Bedeutung.[205]

---

[205] Die Bedeutung wird in Erwägungsgrund 35 der NIS-RL betont. Siehe auch *Wiater*, Sicherheitspolitik zwischen Staat und Markt, 2013, S. 90 ff.; *Könen*, DuD 2016, 12 (12 ff.); *Pohlmann*, DuD 2016, 38 (38 ff.).

Art. 7 Abs. 1 lit. b NIS-RL schreibt vor, dass die nationalen Strategien für die Sicherheit von Netz- und Informationssystemen den Aspekt der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor behandeln sollen. Die Cyber-Sicherheitsstrategie für Deutschland von 2016 erfüllt diese Vorgabe und führt hierzu aus, dass der verfolgte kooperative Ansatz auch den gegenseitigen Informationsaustausch umfasse. Die Bundesregierung „wird hierfür eine Kooperationsplattform für Staat und Wirtschaft institutionalisieren, die innerhalb der vorgegebenen rechtlichen Grenzen vor allem einen Austausch relevanter Lageinformationen zur Abwehr von Cyber-Angriffen ermöglicht."[206]

Solche mehr oder weniger informellen Zusammenschlüsse sind zwar rechtlich unverbindlich, müssen aber keineswegs wirkungslos sein. Als wichtige Plattform kann die sog. Allianz für Cybersicherheit angeführt werden. Dabei handelt es sich um eine Initiative des BSI in Zusammenarbeit mit Bundesverbänden aus der Informations- und Telekommunikationswirtschaft. Der Zusammenschluss des BSI mit Unternehmen soll eine eigene Wissensbasis aufbauen und den gegenseitigen Informations- und Erfahrungsaustausch unterstützen.[207] Die Mitglieder der Allianz sind in die Gruppen Teilnehmer, Institutionen im besonderen staatlichen Interesse (INSI), Partner und Multiplikatoren eingeteilt.[208] Der Zugriff auf die Informationen ist nur Vertretern mit Teilnehmerstatus gestattet. Die INSI erhalten darüber hinaus Zugriff zu einem geschützten Bereich. Das BSI stellt hier ihr wachsendes Repertoire an Informationen zur Sicherheitslage im Cyberraum zur Verfügung. Bereitgestellt werden nicht nur Lageberichte mit Statistiken, sondern auch Warnmeldungen und Schwachstelleninformationen. In diesem informellen Zusammenschluss kann das BSI seinen Beratungsauftrag wahrnehmen oder Empfehlungen auf Grundlage von § 7 Abs. 1 S. 1 Nr. 2 und Abs. 2 BSIG aussprechen.

Im Übrigen kann als „Generalklausel" der individualisierten Informationstätigkeit § 3 Abs. 1 S. 2 Nr. 2 BSIG angesehen werden. Das BSI stellt gesammelte und ausgewertete Informationen Dritten, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist, zur Verfügung. Dritte sind Adressaten außerhalb der Verwaltung, neben den Betreibern kritischer Infrastrukturen auch Unternehmen und sonstige Einrichtungen, die anerkanntermaßen zum Bereich der

---

[206] Bundesministerium des Innern, Cyber-Sicherheitstrategie für Deutschland 2016, S. 25.

[207] *Deutscher Bundestag,* Enquete-Kommission Internet und digitale Gesellschaft, Bericht der Projektgruppe Zugang, Struktur und Sicherheit im Netz, BT-Drs. 17/12541, S. 45; zur zukünftigen Stärkung des kooperativen Ansatzes durch Institutionalisierung von Informationsaustauschplattformen Unterrichtung durch die *Bundesregierung*, Cyber-Sicherheitsstrategie für Deutschland 2016, BT-Drs. 18/10395, S. 9.

[208] *Allianz für Cybersicherheit*, Über uns, Einführung, abrufbar unter: https://www.allianz-fuer-cybersicherheit.de.

kritischen Infrastrukturen im weiteren Sinne gehören oder sonst ein berechtigtes Sicherheitsinteresse an den entsprechenden Informationen geltend machen können.[209]

3. Datenschutzrechtlich Verantwortliche und Betroffene einer Verletzung

a) Betroffene einer Datenschutzverletzung

Stellt ein Angriff auf die Sicherheit eines Netz- und Informationssystems zugleich eine Verletzung der datenschutzrechtlichen Pflichten zur Datensicherheit dar, kommt die Information derjenigen in Betracht, deren personenbezogene Daten betroffen sind. Nach § 38 Abs. 1 S. 6 BDSG kann die Datenschutzaufsichtsbehörde im Falle eines festgestellten Verstoßes gegen das Datenschutzrecht die Betroffenen informieren. Entgegen dem Wortlaut, der die Unterrichtung in das Ermessen der Behörde stellt, wird mit Blick auf die entsprechende unionsrechtliche Vorgabe eine allgemeine Benachrichtigungspflicht angenommen.[210] Nach Art. 28 Abs. 4 UAbs. 1 S. 2 RL 95/46/EG „[ist] die betroffene Person […] darüber zu informieren, wie mit der Eingabe verfahren wurde." Diese Formulierung legt nahe, dass die Aufsichtsbehörde regelmäßig nur auf eine Initiative des Betroffenen hin, die gemäß Art. 28 Abs. 4 UAbs. 1 S. 1 RL 95/46/EG möglich ist, verpflichtet ist. Vor diesem Hintergrund erscheint eine differenzierte Betrachtung sinnvoll. Gegen eine allgemeine Informationspflicht der Aufsichtsbehörde spricht die fehlende Praktikabilität. Ein einziger Datenschutzverstoß kann eine Vielzahl von Personen betreffen. Eine Unterrichtung jedes einzelnen Betroffenen kann zu einem unverhältnismäßigen Aufwand führen und zeitliche wie finanzielle Ressourcen binden. Die Intention des Unionsgesetzgebers kann vielmehr so verstanden werden, dass eine Unterrichtungspflicht nur bei einem gesteigerten Interesse des Betroffenen besteht. Dies dürfte neben dem Fall, dass der Betroffene die Aufklärung des Vorfalls selbst durch einen Hinweis oder eine Anzeige angeregt hat, insbesondere bei erheblichen Nachteilen, die durch die Unkenntnis des Datenschutzverstoßes drohen, gegeben sein.[211] Ein bestehender Kontakt der Behörde zum Betroffenen darf in solchen Fällen für die Begründung der Informationspflicht nicht erforderlich sein.[212]

Die Unterrichtung betrifft inhaltlich den festgestellten Verstoß gegen datenschutzrechtliche Bestimmungen. Der Rechtsprechung zufolge müssen Einzel-

---

[209] Die Begründung zum IT-Sicherheitsgesetz nennt als Beispiel wissenschaftliche Einrichtungen, BT-Drs. 18/4096, S. 38.

[210] *Grittmann*, in: Taeger/Gabel (Hrsg.), BDSG, 2. Aufl. 2013, § 38 Rn. 19.

[211] *Plath*, in: Plath, BDSG/DSGVO, 2. Aufl. 2016, § 38 BDSG, Rn. 27; *von Lewinski*, in: Auernhammer, BDSG, 4. Aufl. 2014, § 38 Rn. 29.

[212] *Brink*, in: BeckOK DatenSR, BDSG, 18. Ed. 2016, § 38 Rn. 44.

heiten über das geprüfte Verfahren nicht mitgeteilt werden.[213] Der Wortlaut legt zumindest nahe, dass der Betroffene vorrangig über die Tatsache eines Verstoßes informiert werden soll („so ist sie befugt, […] hierüber zu unterrichten"). So kann dieser von seinem Strafantragsrecht nach § 44 Abs. 2 BDSG Gebrauch machen. Die Vorschrift schließt dagegen auch nicht aus, dass die Behörde detailliert über einen Verstoß informiert, damit etwaige Schutzmaßnahmen getroffen werden können.

Die Vorschrift im BDSG geht weiter als der korrespondierende Art. 58 Abs. 2 lit. e DS-GVO. Unionsrechtlich ist die Unterrichtung der Betroffenen durch die Aufsichtsbehörde nicht vorgesehen. Die Behörden dürfen den Verantwortlichen lediglich anweisen, die betroffenen Personen zu benachrichtigen. Die behördliche Information wäre allenfalls im Wege der Ersatzvornahme denkbar. Den Mitgliedstaaten ist allerdings nach Art. 58 Abs. 6 DS-GVO das Recht gewährt, ihren Aufsichtsbehörden weitere als die aufgeführten Befugnisse zu übertragen, sodass § 38 Abs. 1 S. 6 BDSG inhaltlich weiterhin Bestand haben kann.

b) Individuelle Beratung in Fragen der Datensicherheit

Zu den Aufgaben der Datenschutzaufsichtsbehörden gehört die Beratung von Verantwortlichen, Auftragsdatenverarbeitern und Datenschutzbeauftragten. Zwar fällt die datenschutzrechtliche Beratung nach Art. 39 Abs. 1 lit. a DS-GVO grundsätzlich den jeweiligen Datenschutzbeauftragten zu. Darüber hinaus ist es insbesondere nach Art. 57 Abs. 1 lit. d DS-GVO die Pflicht („muss") der Aufsichtsbehörde, die Verantwortlichen und Auftragsverarbeiter „für die ihnen aus dieser Verordnung entstehenden Pflichten [zu] sensibilisieren". Die Sensibilisierung setzt hier keinen Antrag voraus, sondern bezeichnet eine offensive allgemeine Aufklärung und Beratung.[214] Mit Bezug auf die Datensicherheit muss die Beratung insbesondere darauf zielen, dass Datenschutz nicht nur eine grundrechtssensitive Datenverarbeitung erfordert, sondern auch das Ergreifen der entsprechenden technisch-organisatorischen Maßnahmen.

Vor allem wegen der Unentgeltlichkeit der behördlichen Aufgabenerfüllung (Art. 57 Abs. 3 DS-GVO) ist es fernliegend, dass die Datenschutzbehörden zu einer umfassenden Compliance-Beratung personell oder sachlich in der Lage sind. Ein wirksamer Grundrechtsschutz setzt zwar eine effektive Aufgabenwahrnehmung voraus. Die Behörde muss aber in ihrem Ermessen über eine zweckmäßige Verteilung der zur Verfügung stehenden Ressourcen entscheiden

---

[213] Ohne nähere Begründung VG Bremen, RDV 2010, 129 (131).

[214] *Roßnagel*, Zusätzlicher Arbeitsaufwand für die Aufsichtsbehörden der Länder durch die Datenschutz-Grundverordnung, 2017, S. 87 mit weitergehenden Ausführungen zu Beratungspflichten, die im Schwerpunkt Fragen außerhalb der Datensicherheit betreffen.

können. Bei einer praxisnahen Betrachtung kommt insofern nur punktuell in herausgehobenen Fällen eine Sensibilisierung oder Beratung in Betracht.

C. Reaktives Informationshandeln

Über die reaktiven Informationspflichten können Private von sich aus am staatlichen Wissen partizipieren. Die dafür erforderliche Öffnung der Verwaltung ist verfassungsrechtlich angelegt (I.). Die Gatekeeper-Funktion der Verwaltung wird bei den meisten NIS-Behörden durch einen Informationszugangsanspruch reduziert (II.). Der Anspruch ist aber nicht schrankenlos und steht im Spannungsverhältnis zum Geheimhaltungsbedürfnis. Für das Informationszugangsrecht bestehen neben den allgemeinen Ausnahmen besondere Begrenzungen für den Zugang zu Informationen mit Bezug zu kritischen Infrastrukturen (III.). Hinsichtlich der zugänglich gemachten Informationen besteht keine besondere Aufbereitungs- oder Beschaffungspflicht, die Informationen sind aber grundsätzlich maschinenlesbar für die weitere, freie Weiterverwendung bereitzustellen (IV.).

I. Grundrecht auf Informationszugang

Bei der Informationszugangsfreiheit geht es um den Zugang des Bürgers zu den Informationen bei den Verwaltungen der Länder oder des Bundes.[215] Die zugrunde liegenden Streitigkeiten und Argumentationen kreisen hier um rechtsstaatliche und demokratietheoretische Überlegungen.[216] Mit einem erweiterten Verständnis von Informationsverwaltungsrecht kann die Informationsdistribution durch den Staat im Sinne der hier verfolgten These erklärt werden als „die verwaltungsrechtliche Reaktion auf die gestiegene soziale Relevanz des Wissens einerseits und die Dezentralisierung der gesellschaftlichen Wissensbestände, die neue Koordinations- und Kooperationsanstrengungen erforderlich macht".[217] Dieses Verständnis berücksichtigt das gewandelte Rollenverständnis des Staates, zu dessen Aufgaben es gehört, „unter den veränderten kognitiven Bedingungen" eine „adäquate Ausgestaltung der informationellen Beziehungen zwischen Staat und Bürgern" herzustellen.[218]

---

[215] Vgl. *Schoch*, IFG, 2009, Einleitung, Rn. 1 ff.
[216] *Masing*, Transparente Verwaltung, in: VVDStRL 63 (2004), S. 377 ff.
[217] *Augsberg*, Informationsverwaltungsrecht, 2014, S. 196.
[218] *Augsberg*, Informationsverwaltungsrecht, 2014, S. 196 f.

Der Gedanke der Informationsfreiheit findet sich im Unionsrecht als Grundrecht wieder (1.). Ein verfassungsunmittelbares subjektives Recht auf Informationszugangsfreiheit lässt sich aus dem Grundrecht nicht ableiten (2.).

1. Grundsatz der Offenheit und Recht auf Zugang zu Dokumenten im Unionsrecht

Der Grundsatz der Offenheit gehört zu den allgemeinen Bestimmungen im AEUV. Das Transparenzprinzip wird in Art. 15 Abs. 3 AEUV konkretisiert,[219] der die „weitgehende Beachtung" dieses Grundsatzes von den Organen, Einrichtungen und sonstigen Stellen der Union fordert. Ziel ist es, eine verantwortungsvolle Verwaltung zu fördern und die Beteiligung der Zivilgesellschaft sicherzustellen. Einen individuellen Anspruch auf den Zugang zu Dokumenten begründet Art. 15 Abs. 3 AEUV. Dem Wortlaut nach ist der Anspruch frei und voraussetzungslos.[220] Die Norm hat allerdings keine Wirkung, die *self executing* wäre. Einschränkungen für die Ausübung des Rechts ergeben sich aus einer Verordnung, die gemäß Art. 15 Abs. 3 UAbs. 2 AEUV nach dem ordentlichen Gesetzgebungsverfahren festgelegt werden. Nach dieser Bestimmung ist die konkrete Ausgestaltung dem Gesetzgeber, dem Europäischen Parlament und dem Rat aufgegeben. Die Anwendung der Zugangsfreiheit ist demnach von der sekundärrechtlichen Ausgestaltung abhängig.[221]

Der Zugang zu Dokumenten ist neben dem primärrechtlichen Anspruch als unionsrechtliches Grundrecht in Art. 42 GRCh verankert. Über die Grundrechtsanerkennung in Art. 6 Abs. 1 EUV wird die GRCh als unmittelbar geltendes, gleichrangiges Unionsrecht inkorporiert. Dieses Grundrecht statuiert trotz der systematischen Stellung bei den Bürgerrechten[222] nicht nur ein Recht für Unionsbürgerinnen und Unionsbürger, sondern für jede natürliche oder juristische Person mit Wohnsitz oder satzungsmäßigem Sitz in einem Mitgliedstaat. Jedem Berechtigten ist damit ein Recht auf Zugang zu Dokumenten der Organe, Einrichtungen und sonstigen Stellen der Union eingeräumt. Eine Rechtsentwicklung in Richtung Informationszugangsfreiheit deutet sich auch in der Rechtsprechung zur EMRK an. Der EGMR legt Art. 10 EMRK mittlerweile deutlich extensiver aus. Hat die Rechtsprechung des Gerichts die Informationsfreiheit ursprünglich in der Presse- und Medienfreiheit eingeordnet, ist sie nunmehr auf den Zugang zu

---

[219] *Wegener*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, 4. Aufl. 2011, AEUV, Art. 15 Rn. 11.

[220] *Wegener*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, 4. Aufl. 2011, AEUV, Art. 15 Rn. 11.

[221] *Sobotta*, Transparenz in den Rechtsetzungsverfahren der Europäischen Union, 2001, S. 344; *Krajewski/Rösslein*, in: Grabitz/Hilf/Nettesheim (Hrsg.), AEUV/EUV, 57. Aufl. 2015, AEUV, Art. 15 Rn. 37.

[222] Überschrift des Titel V der Charta der Grundrechte der Europäischen Union.

Datenbanken, in denen amtliche Dokumente gespeichert sind, erweitert.[223] Über Art. 6 Abs. 3 EUV sind die Grundrechte, wie sie in der EMRK gewährleistet sind und wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten ergeben, als allgemeine Grundsätze Teil des Unionsrechts.

2. Verankerung der Informationsfreiheit im Grundgesetz

Aus dem Grundgesetz lässt sich ein verfassungsunmittelbares subjektives Recht auf Informationszugang, wie es auf Bundesebene das Informationsfreiheitsgesetz (IFG) gewährt, dagegen nicht ableiten. Das in Art. 20 Abs. 2 GG verankerte Demokratieprinzip stärkt indes das nationale, einfachgesetzliche Informationszugangsrecht.[224] Der Genese und dem Telos nach ist die demokratische Teilhabe ein Zielwert des Demokratieprinzips, der grundsätzlich bei dem Einzelnen eine ausreichende Informationsgrundlage und folglich auch den Zugang zu Informationen voraussetzt. Die Basis für die zivile Teilhabe wird allerdings im deutschen Verfassungsgefüge traditionell über die Kommunikationsgrundrechte sowie die Presse- und Rundfunkfreiheit geschaffen. Das Verständnis eines Rechts auf Information aus amtlichen Quellen skandinavischer und angloamerikanischer Prägung bricht sich mit Art. 42 GRCh im Anwendungsraum des EU-Rechts aber Bahn.[225]

Auch das Rechtsstaatsprinzip aus Art. 20 Abs. 3 GG lässt sich, wenn auch nur als verstärkendes Argument und nicht als genuine Rechtsgrundlage, für einen Anspruch heranziehen. Für den Bereich der Exekutive ist die Parteiöffentlichkeit (§ 29 VwVfG) Bestandteil des fairen rechtsstaatlichen Verfahrens.[226] Einsichtsansprüche in Vorgänge und Akten außerhalb eines Verwaltungsverfahrens setzen zwar ein zusätzliches berechtigtes Interesse, etwa an der eigenen Rechtsverfolgung, voraus, können jedoch im Einzelfall einen Anspruch auf fehlerfreie Ermessensausübung verleihen.[227]

In Art. 5 Abs. 1 S. 1 GG ist dem Wortlaut nach kein grundrechtlicher Informationszugang verankert. Gleichwohl erstarken in der Literatur die Argumente für ein Grundrecht auf Informationszugangsfreiheit.[228] Das Bundesverfas-

---

[223] EGMR, Az. 3953407 39534/07, Rn. 47; *Dix*, Der verfassungs- und europarechtliche Rahmen des Rechts auf Informationszugang, in: Dreier/Fischer/van Raay/Spiecker gen. Döhmann (Hrsg.), 2016, S. 77 (85 f.).

[224] Dazu *Rossi*, Informationszugangsfreiheit und Verfassungsrecht, 2004.

[225] *Wirtz*/*Brink*, NVwZ 2015, 1166 (1168).

[226] *Kallerhoff*, in: Stelkens/Bonk/Sachs (Hrsg.), VwVfG, 8. Aufl. 2014, § 29 Rn. 1.

[227] VGH München, NVwZ 1999, 889 (890).

[228] *Pernice*, Verfassungs- und europarechtliche Aspekte der Transparenz staatlichen Handelns, in: Dix/Franßen/Kloepfer/Schaar/Schoch/Deutsche Gesellschaft für Informationsfreiheit e.V. (Hrsg.), Informationsfreiheit und Informationsrecht Jahrbuch 2013, 2014, S. 17

sungsgericht und das Bundesverwaltungsgericht sind in ihrer Rechtsprechung bislang restriktiv und verneinen einen verfassungsunmittelbaren Informationszugangsanspruch.[229] Die vom IFG vermittelten Zugangsansprüche seien nicht grundrechtlich fundiert. Sie setzten vielmehr eine rechtspolitische Entscheidung des Gesetzgebers um.[230] Allerdings hat das Bundesverwaltungsgericht einen unmittelbar verfassungsrechtlich verankerten Mindeststandard für ein Informationszugangsrecht der Presse anerkannt.[231] Vor allem die historische Auslegung von Art. 5 Abs. 1 S. 1 GG ergibt, dass der Bezug der Garantie der Informationsfreiheit auf „allgemein zugängliche Quellen" nicht die amtlichen Quellen umfasst.[232] Die ursprüngliche Funktion des Grundrechts sei es, dass die staatlichen Stellen die Einzelnen nicht daran hindern dürfen, sich aus von Privaten aufgebauten und unterhaltenen Informationsquellen zu unterrichten.[233] Der Staat könne daher im Rahmen seiner Aufgaben und Befugnisse Art und Umfang des Zugangs zu Informationsquellen selbst festlegen.[234]

II. Zugang zu Informationen bei den NIS-Stellen

Mangels praxistauglicher Verankerung der Informationsfreiheit im Verfassungsrecht kommt für die weitere Untersuchung der sekundärrechtlichen bzw. einfachgesetzlichen Ausgestaltung des Informationszugangs gesteigerte Bedeutung zu. Die verfassungsrechtlichen Vorgaben können indes als Mindeststandards und Ausgestaltungsaufträge verstanden werden.[235] Sie können als Kriterien für die regelmäßig notwendige Abwägung mit anderen und gegenläufigen verfassungsrechtlich geschützten Interessen und Belangen heranzuziehen sein. Zum anderen besteht in Fällen, in denen bereits für eine Informationsquelle aus dem staatlichen Verantwortungsbereich Regeln hinsichtlich der öffentlichen Zugänglichkeit vorhanden sind, ein Recht auf Informationszugang, wenn dieser nicht in hinreichender Weise eröffnet ist.[236]

(27 ff.); *Wirtz/Brink*, NVwZ 2015, 1166 (1167 ff.); ablehnend und mit eigenem Formulierungsvorschlag für ein neues Grundrecht *Kloepfer/Schärdel*, JZ 2009, 453 (459).

229 BVerfGE 27, 71 (82); BVerfG, NVwZ 1986, 462 (462); BVerwG, NJW 2014, 1126 (1127).

230 BVerwG, NVwZ 2016, 1820 (1820).

231 BVerwG, NVwZ 2013, 1006 (1006).

232 BVerfGE 103, 44 (60 f.).

233 *Wirtz/Brink*, NVwZ 2015, 1166 (1168).

234 BVerwG, NJW 2014, 1126 (1127). Auf Ebene der Länder gibt es einige Ansätze zur verfassungsrechtlichen Regelung der Informationsbeziehungen zwischen Staat und den Bürgern, vgl. Art. 21 Abs. 4 BbgVerf oder Art. 53 SchlHVerf.

235 *Gusy*, JZ 2014, 171 (171).

236 BVerfG, NJW 2008, 977 (978); *Schwemmer*, in: Hillgruber/Epping (Hrsg.), BeckOK GG, 27. Ed. 2015, Art. 5 Rn. 32.

Für die weitere Frage des Zugangs zu Informationen zu NIS-Stellen ist zu bestimmen, ob und auf welcher Grundlage Informationszugang zu den europäischen (1.) und nationalen NIS-Stellen erlangt werden kann (2.).

1. Zugang bei europäischen NIS-Stellen

Bei der Anwendung der NIS-Richtlinie gilt grundsätzlich die Transparenz-Verordnung, der in ihr gewährte Informationszugang umfasst aber nur einen Teilbereich der Eigenverwaltung der Union (a). Die ENISA verfügt über eigene Zugangsregelungen, die auf die Transparenzverordnung verweisen (b).

a) Reichweite der Transparenz-Verordnung und Verhältnis zur NIS-Richtlinie

Die Grundsätze und Bedingungen des primärrechtlichen Rechts auf Zugang zu Dokumenten sind gemäß Art. 15 Abs. 3 UAbs. 1 AEUV nach UAbs. 2 AEUV festzulegen. Art. 15 Abs. 3 UAbs. 2 AEUV erteilt dem Unionsgesetzgeber den Auftrag, die allgemeinen Grundsätze und die aufgrund öffentlicher und privater Interessen geltenden Einschränkungen für die Ausübung des Rechts auf Zugang zu Dokumenten durch eine Verordnung im ordentlichen Gesetzgebungsverfahren festzulegen.

Seit 2001 existiert für die Europäische Union mit der VO (EG) Nr. 1049/2001 (Transparenz-Verordnung) eine „Informationsfreiheitsverordnung", die spiegelbildlich dem Regelungsanliegen des IFG entspricht.[237] Auch wenn die betroffenen Garantien des Primärrechts und der Charta erst zeitlich nach der Transparenz-VO geschaffen wurden, kann die Verordnung als Konkretisierung der Grundrechtsbestimmungen angesehen werden.[238]

Die Transparenz-Verordnung stellt keine allgemeine unionsweite Regelung für den Informationszugang dar. Die Zugangsverpflichtung ist auf das Europäische Parlament, den Rat und die Kommission beschränkt (Art. 1 lit. a VO (EG) Nr. 1049/2001). Der Anwendungsbereich der Transparenz-Verordnung wird vielfach durch Verweise in den Gründungsakten und Zugangsregelungen in Geschäftsordnungen von Unionseinrichtungen ausgedehnt. Für die Mitgliedstaaten hat die Transparenz-Verordnung indes keine direkten Auswirkungen.[239]

Da sowohl Art. 15 Abs. 3 AEUV als auch Art. 42 GRCh nur die Informationsfreiheit bezüglich des Zugangs zu Informationen bei den Stellen der Union gewährleisten, kann die Union den Mitgliedstaaten nur insoweit Vorgaben machen, als dies der Grundsatz der begrenzten Einzelermächtigung (Art. 5 Abs. 1

[237] *Bretthauer*, DÖV 2013, 677 (677).

[238] *Dix*, Der verfassungs- und europarechtliche Rahmen des Rechts auf Informationszugang, in: Dreier/Fischer/van Raay/Spiecker gen. Döhmann (Hrsg.), 2016, S. 77 (85).

[239] Erwägungsgrund 15 VO (EG) Nr. 1049/2001.

S. 1, Abs. 2 EUV) erlaubt. Regelungen der Informationsfreiheit mit Wirkungen in den Mitgliedstaaten können daher nur bereichsspezifisch erfolgen.[240] Umsetzungen in den Mitgliedstaaten waren beispielsweise erforderlich zur Umsetzung der Umweltinformations-Richtlinie 2003/4/EG oder der INSPIRE-Richtlinie 2007/2/EG, die den Mitgliedstaaten die Entscheidung darüber, ob Geodaten zugänglich zu machen sind, abnimmt. Die Informationsfreiheit richtet sich im Übrigen nach den mitgliedstaatlichen Regelungen.[241]

Damit ist zwischen dem Zugang zu Informationen bei NIS-Stellen der Union und den nationalen NIS-Stellen zu unterscheiden.

Fraglich ist, wie sich die NIS-Richtlinie zur Transparenz-Verordnung verhält, da beide gleichrangiges Sekundärrecht darstellen. Regelungsziel der aufgrund von Art. 288 Abs. 2 AEUV unmittelbar geltenden Verordnung ist es, durch Transparenz eine bessere Beteiligung der Bürger am Entscheidungsprozess und eine größere Legitimität, Effizienz und Verantwortung der Verwaltung gegenüber dem Bürger in einem demokratischen System zu gewährleisten.[242] Dem Recht auf Zugang der Öffentlichkeit zu Dokumenten soll die Verordnung „größtmögliche Wirksamkeit" verschaffen (Art. 1 lit. a VO (EG) Nr. 1049/2001). Ob dieses Anspruchs der größtmöglichen Wirksamkeit stellt sich das Problem des Verhältnisses der NIS-Richtlinie zur Transparenz-Verordnung. Die Beziehung der Verordnung zu anderen sekundärrechtlichen Normen ist noch nicht geklärt. Es stellt sich die Frage, ob das Dokumentenzugangsrecht in der Transparenz-Verordnung Gegenstand einer allgemeinen Vorschrift ist, die in einigen Gebieten durch bestimmte besondere Vorschriften aus anderen Unionsregelungen zu ergänzen ist, oder ob die Ausübung des Rechts in der Transparenz-VO für alle Fälle abschließend geregelt ist.[243] Als Spezifikationshinweis findet sich in der NIS-RL nur die Erwägung, dass die Verordnung gelten „sollte".[244] Ein Primat der Transparenz ergibt sich dadurch noch nicht, zumal eine parallele Anwendbarkeit der DS-GVO gegeben ist. Der Europäische Gerichtshof geht, wohl auch weil die Anwendung der Lex-posterior- bzw. Lex-specialis-Regel fehlerhaft wäre,[245] von einer parallelen Anwendbarkeit von Transparenz-VO und anderem Sekundärrecht aus.[246]

---

[240] *Debus*, in: BeckOK IMR, 14. Ed. 2016, IFG, § 1 Rn. 10.

[241] Die Richtlinie 2003/98/EG über die Weiterverwendung von Informationen des öffentlichen Sektors begründet keine Verpflichtung der Mitgliedstaaten, den Informationszugang zu gewähren, Erwägungsgründe 9 und 16 der RL 2003/98/EG, Erwägungsgrund 8 der Änderungsrichtlinie 2013/37/EU. Siehe dazu auch § 5 C. IV. 2.

[242] Erwägungsgrund 2 VO (EG) Nr. 1049/2001.

[243] Dazu GA *Villalón*, Rs. C-365/12, Rn. 37.

[244] Erwägungsgrund 39 NIS-RL.

[245] *Koppensteiner*, EuR 2014, 594 (598 f.).

[246] EuGH, C-28/08, Rn. 65; vgl. aber GA *Sharpston*, C-28/08, Rn. 104.

Der (unverbindliche) Verweis in den Erwägungsgründen zur NIS-RL lässt jedenfalls nicht von vornherein auf einen Normenkonflikt schließen, sodass Abwägungsfragen einer Einzelfallbetrachtung vorbehalten sind. Zugleich ergibt sich dadurch auch für bestimmte Kategorien von Dokumenten keine allgemeine Vermutung der Nichtöffentlichkeit.[247]

Die NIS-Richtlinie schließt somit den Zugang zu Dokumenten über die Netz- und Informationssicherheit beim Europäischen Parlament, dem Rat und der Kommission nicht aus. Zum grundsätzlichen Informationszugang zu den sonstigen NIS-Stellen wie der NIS-Kooperationsgruppe oder dem CSIRTs-Netzwerk, die in der europäischen Zusammenarbeit ein zentrale Rolle spielen, verhält sich die NIS-Richtlinie indes nicht. Insofern kommt für das CSIRTs-Netzwerk in Betracht, dass es anderen Unionseinrichtungen gleichtut und in seiner Geschäftsordnung, die es sich nach Art. 12 Abs. 5 NIS-RL gibt, eine Zugangsregelung aufnimmt, die mit den Bestimmungen der Transparenz-Verordnung und der Vertraulichkeit in Einklang steht.[248] Im Übrigen gilt der Gesetzgebungsauftrag des Art. 15 Abs. 3 AEUV, die Modalitäten des Zugangsrechts sekundärrechtlich auszugestalten. Eine allgemeine Neufassung der Regelungen sollte der Erweiterung des Kreises der Verpflichteten in Art. 15 Abs. 3 UAbs. 1 AEUV berücksichtigen und den Anspruch primärrechtskonform auf sämtliche Organe, Einrichtungen und sonstigen Stellen der Union erweitern.[249]

b) Zugang zu Informationen am Beispiel der ENISA

Für den Zugang zu Informationen bei der ENISA ist mit Art. 18 der Verordnung (EU) Nr. 526/2013 eine Regelung vorhanden, die in Abs. 1 zum einen die Transparenz-VO für anwendbar erklärt und in Abs. 2 bestimmt, dass der Verwaltungsrat eine Durchführungsmaßnahme festlegt. Die Entscheidung der ENISA Nr. MB/2013/14 soll das Zugangsrecht für die Agentur durchführen.

Am Beispiel der ENISA lässt sich untersuchen, zu welchen Informationen Zugang bestehen kann. Maßgeblich für die Reichweite des Anspruchs ist die Auslegung des Begriffs „Dokument".

Der Gegenstand des Zugangsanspruchs sind Dokumente. Aus den Art. 4, 5 und 9 der VO (EG) Nr. 1049/2001 lassen sich begriffliche Unterscheidungen entnehmen. Es gibt Dokumente Dritter, Dokumente der Mitgliedstaaten, sen-

---

[247] Vgl. dazu EuGH, Rs. C-139/07 P, Rn. 62.

[248] Zu dieser Praxis *Krajewski*/*Rösslein*, in: Grabitz/Hilf/Nettesheim (Hrsg.), AEUV/EUV, 57. Aufl. 2015, AEUV, Art. 15 Rn. 42.

[249] Zur Unübersichtlichkeit der Regelungen und der daraus resultierenden Erschwerung, das Recht auf Informationszugang wahrzunehmen, *Gellermann*, in: Streinz (Hrsg.), EUV/AEUV, 2. Aufl. 2012, AEUV, Art. 15 Rn. 9.

sible Dokumente und Dokumente im Besitz von Mitgliedstaaten. Bezüglich der Begriffsbestimmung in Art. 3 a) Transparenz-VO sind unter „Dokument" Inhalte zu verstehen, die einen Sachverhalt mit den Politiken, Maßnahmen oder Entscheidungen aus dem Zuständigkeitsbereich des Organs betreffen. Die Form des Dokuments ist nicht von Belang. Der Begriff bezieht sich auf Inhalte unabhängig davon, ob sie auf Papier, in elektronischer Form oder als Ton-, Bild- oder audiovisuelles Material vorliegen. Umfasst sind daher auch Inhalte aus E-Mails.[250] Im Lichte von Art. 42 GRCh und Art. 2 Abs. 2 Transparenz-VO ist eine weite Auslegung des Begriffs außerdem geboten.[251] Auf den Inhalt des Dokuments kommt es für die Bemessung des Schutzbereichs nicht an.[252] Gegen ein enges Verständnis spricht, dass der Schutz der behördlichen Prozesse allein über die Schrankenbestimmungen erreicht wird.[253] Von dem Anspruch erfasst sind Dokumente, die von einer Stelle der EU verfasst worden oder einer EU-Stelle zugegangen sind. Die von Dritten, etwa von einem Mitgliedstaat oder einer Privatperson erstellten Dokumente sind also ebenfalls grundsätzlich erfasst. Der Informationszugangsanspruch ist aber kein allgemeiner Auskunftsanspruch.[254] Der Zugang zu Dokumenten gilt nur für vorhandene Dokumente, sodass ihre Beschaffung nicht verlangt werden kann.

Der Kreis der Anspruchsberechtigten entspricht in Art. 2 Abs. 1 Transparenz-Verordnung denen des Art. 15 Abs. 3 UAbs. 1 AEUV und Art. 42 GRCh. Art. 2 Abs. 1 Transparenz-VO wiederholt den Kreis, erweitert ihn aber um natürliche und juristische Personen, die keinen Sitz in einem Mitgliedstaat haben.

Der Anspruch auf Zugang zu Dokumenten bei europäischen NIS-Stellen ist demnach weiter, als der Wortlaut „Dokument" vermuten lässt. Durch die weite Auslegung des Begriffs und die Unabhängigkeit vom Inhalt sind NIS-Informationen vom Anspruch auf Informationszugang grundsätzlich erfasst.

2. Zugang bei nationalen NIS-Stellen

Auf nationaler Ebene fallen das BSI (a) und die Bundesnetzagentur (b) als Bundesbehörden in den Anwendungsbereich des IFG. Nachrichtendienste und sonstigen Stellen des Bundes mit einer vergleichbaren Sicherheitsempfindlichkeit sind von dem Anwendungsbereich des IFG ausgenommen (c).

---

[250] *Gellermann*, in: Streinz (Hrsg.), EUV/AEUV, 2. Aufl. 2012, AEUV, Art. 15 Rn. 12.

[251] *Jarass*, Charta der Grundrechte der EU, 2. Aufl. 2013, Art. 42 Rn. 6; *Magiera*, in: Meyer (Hrsg.), Charta der Grundrechte der Europäischen Union, 4. Aufl. 2014, Art. 42 Rn. 9.

[252] *Jarass*, Charta der Grundrechte der EU, 2. Aufl. 2013, Art. 42 Rn. 7.

[253] *Wegener*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, 4. Aufl. 2011, AEUV, Art. 15 Rn. 17; *Schoo*, in: Schwarze/Becker/Hatje/ders. (Hrsg.), EU-Kommentar, 3. Aufl. 2012, EUV, Art. 255 Rn. 9.

[254] *Jarass*, Charta der Grundrechte der EU, 2. Aufl. 2013, Art. 42 Rn. 8.

a) Bundesamt für Sicherheit in der Informationstechnik

Der Anwendungsbereich des IFG ergibt sich in sachlicher und persönlicher Hinsicht aus der Grundnorm, § 1 IFG. Jeder hat nach Maßgabe des IFG gegenüber den Anspruchsverpflichteten einen Anspruch auf Zugang zu amtlichen Informationen. Der Informationsanspruch besteht gegenüber den Behörden des Bundes. Das BSI ist gemäß § 1 Abs. 1 S. 1 BSIG eine Bundesoberbehörde und erfüllt den Behördenbegriff des Zugangsanspruchs.

Der Anspruch ist auf den Zugang zu den der informationspflichtigen Stelle tatsächlich vorliegenden amtlichen Informationen gerichtet. Amtliche Informationen sind nach § 2 Nr. 1 IFG alle amtlichen Zwecken dienende Aufzeichnungen, unabhängig von der Art ihrer Speicherung. Entwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen, gehören nicht dazu. Die Amtlichkeit der Information setzt nicht voraus, dass der Bund Urheber der Information ist. Der Zweck der Information, nicht ihre Herkunft ist entscheidend. Sie müssen in Erfüllung einer öffentlichen Tätigkeit angefallen sein. Bei behördlichen gespeicherten Daten ist das auch dann der Fall, wenn sie zuvor von Privaten erhoben wurden.[255]

Die Vorschrift setzt weder das Bestehen eines Informationsinteresses voraus, noch steht dem Anspruch ein bestimmtes Informationsinteresse entgegen.[256] Ein Informationszugangsanspruch kann also auch bei einem Interesse an sicherheitsbezogenen Informationen bestehen. Der Antrag auf Informationszugang muss jedoch erkennen lassen, zu welchen amtlichen Informationen Zugang begehrt wird. Wegen der fehlenden Kenntnis der Antragsteller von den vorliegenden Informationen dürfen jedoch keine unangemessen hohen Anforderungen gestellt werden. Grundsätzlich unzulässig sind jedoch Informationsanfragen „ins Blaue hinein".[257]

b) Bundesnetzagentur

Die Bundesnetzagentur fällt als Bundesoberbehörde (vgl. § 116 Abs. 1 S. 2 TKG) wie das BSI in den Anwendungsbereich des IFG. Grundsätzlich umfasst der Anspruch auch gegen die Bundesnetzagentur alle Informationen, über welche die Behörde unabhängig von ihrer Speicherung verfügt.[258]

---

[255] *Augsberg*, DVBl. 2007, 733 (739).

[256] *Debus*, in: Gersdorf/Paal (Hrsg.), BeckOK IMR, 11. Ed. 2016, IFG, § 1 Rn. 33.

[257] Vgl. zum Umweltinformationsgesetz VGH Kassel, NVwZ 2007, 348 (350): „Hier hätte es der Darlegung bedurft, welche Umweltinformationen die Antragstellerin in bei der Antragsgegnerin vorhandenen Unterlagen vermutet […]".

[258] Siehe auch *Attendorn*/*Geppert*, in: Geppert/Schütz (Hrsg.), BeckTKG, 4. Aufl. 2013, § 136 Rn. 7.

c) Kein Zugang zu Informationen bei Nachrichtendiensten

Bei den Nachrichtendiensten mit NIS-Bezug besteht dem Grunde nach Informationszugang gemäß §§ 1 Abs. 1 und 3, 2 Nr. 1 IFG. Ausgeschlossen werden jedoch durch § 3 Nr. 8 IFG Ansprüche auf Informationszugang gegenüber den Nachrichtendiensten und sonstigen Stellen des Bundes mit einer vergleichbaren Sicherheitsempfindlichkeit, die sich daraus ergibt, dass die Stellen Aufgaben im Sinne des Sicherheitsüberprüfungsgesetzes wahrnehmen.

Die gesetzlich angeordnete Bereichsausnahme, die eine Einzelprüfung eines Antrags nicht vorsieht, gilt auch für die Gewährung des Informationszugangs durch andere Stellen, bei denen die betreffenden Informationen vorliegen und soweit diese die Geheimhaltung reklamieren.[259] Der Gesetzgeber hatte § 3 Nr. 8 IFG als zusätzlichen Ausschlussgrund aufgenommen, weil er das Gesetz nicht für umfassend genug hielt. Es sollten vielmehr alle Vorgänge und Tätigkeiten in den Nachrichtendiensten erfasst sein.[260] Demnach sind auch alle übermittelten Informationen bei anderen Behörden erfasst.[261]

Ein Informationszugang zu Informationen, die der Bundesnachrichtendienst im Rahmen der strategischen Fernmeldeaufklärung zur Aufklärung von Cybergefahren generiert, scheidet somit von vorneherein aus. Die Bereichsausnahme ist umfassend und betrifft nicht etwa nur personenbezogene Daten. Ein Anspruch auf Zugang zu sicherheitsbezogenen Sachinformationen besteht daher nicht. Jegliche Informationsdistribution seitens des Bundesnachrichtendienstes ist letztlich aber nicht ausgeschlossen. Das IFG formt nicht die informationsrechtliche Stellung der Presse aus und reflektiert nicht ihre besonderen Funktionsbedürfnisse. Solange der Bundesgesetzgeber seinen Gestaltungsauftrag aus dem objektiv-rechtlichen Gewährleistungsgehalt des Art. 5 Abs. 1 S. 2 GG erfüllt, kommt ein unmittelbarer spezifisch presserechtlicher Auskunftsanspruch aus dem Grundrecht in Betracht.[262]

III. Informationsinteresse und Geheimhaltungsbedürfnis

Kaum ein Recht wird schrankenlos gewährleistet. Das Informationsinteresse hat seinen Antipoden im Geheimhaltungsinteresse.[263] Das Zugangsrecht schafft

---

[259] OVG Berlin-Brandenburg, BeckRS 2014, 58830, sub I. 1, hinsichtlich des gegenüber dem Bundeskanzleramt geltend gemachten Anspruchs; bestätigt durch BVerwG, Urteil vom 25.02.2016, Az. 7 C 18.14.

[260] Vgl. BT-Drs. 14/4493, S. 12.

[261] Noch nicht *per se* ausgeschlossen sind damit Anfragen etwa nach dem PresseG oder ArchivG.

[262] BVerwG, NJW 2013, 1006 (1009).

[263] Vgl. für das Lebensmittelrecht *Möstl*, Informationsinteresse und Geheimhaltungsbe-

daher weiterhin geschützte Bereiche für Staatsgeheimnisse, Geschäfts- und Betriebsgeheimnisse, berufliche Schweigepflichten, vertragliche Verschwiegenheitspflichten und sonstige grundrechtlich geschützte Interessen. Die Informationszugangsfreiheit macht die Verwaltung also nur transparent, aber noch nicht gläsern.[264] Die Trennung der Verwaltung in „Vorder- und Hinterbühne", d. h. die Beschränkung zum Schutz öffentlicher und privater Belange, bedarf allerdings einer Rechtfertigung. Der Ausgleich zwischen Informationsfreiheit und Geheimhaltungsinteresse folgt einer Regel-Ausnahme-Struktur. Will die Behörde den Zugang zu bestimmten Informationen verweigern, muss sie das Vorliegen einer Ausnahme vom Zugang darlegen.[265] Der Anspruch ist also in der Regel weit, die Ausnahmetatbestände sind entsprechend ihrer Rechtsnatur eng auszulegen. Die Struktur der Geheimhaltungstatbestände folgt der Geheimhaltungsstrenge. Es bestehen neben den Bereichsausnahmen absolute und relative Informationsverweigerungsgründe. Im Rahmen der absoluten Verweigerungsgründe ist für eine Interessenabwägung kein Raum. Bei relativen Verweigerungsgründen kann trotz der Beeinträchtigung von Schutzinteressen der Zugang dann nicht verweigert werden, wenn ein öffentliches Interesse an der Verbreitung überwiegt. Soweit gesetzlich keine abschließende Entscheidung zugunsten der Geheimhaltung getroffen ist, ist der exakte Ausgleich der gegenläufigen Positionen erforderlich.[266] Ist der Informationszugangsanspruch weit auszulegen, sind im umgekehrten Verhältnis die Ausnahmetatbestände eng auszulegen.[267] Die Einschränkungen des Zugangsrechts sind an dem expliziten Willen des Gesetzgebers zu messen.

Für die weitere Untersuchung der Begrenzung des Informationszugangsrechts durch Geheimhaltungsinteressen ist zunächst das Verhältnis des allgemeinen IFG zum BSIG zu bestimmen (1.). Sodann ist die Bedeutung der bestehenden Ausnahmen für die nicht durch die Sonderregelung aus dem im Übrigen anwendbaren IFG ausgenommenen Bereiche darzustellen (2.). Die im BSIG geregelte informationsfreiheitsrechtliche Sonderbestimmung basiert auf einer unzureichenden Pauschalabwägung (3.).

---

dürfnis als Antipoden im Verbraucherinformationsgesetz?, in: Leible (Hrsg.), Verbraucherschutz durch Information im Lebensmittelrecht, 2010, S. 149 ff. (157, 165 f.).

[264] Zugespitzter bei *Masing*, Transparente Verwaltung, in: VVDStRL 63 (2004), S. 377 (379): „Die Verwaltung ist nicht transparent – und wird es nie sein."

[265] BT-Drs. 15/4493, S. 11 f.

[266] Anschaulich *Gurlit*, Die Verwaltung 44 (2011), 75 (91 ff.).

[267] *Bartelt/Zeitler*, EuR 2003, 487 (493); *Wegener*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, 4. Aufl. 2011, AEUV, Art. 15 Rn. 34; *Schoch*, IFG, 2009, Vorb. §§ 3 bis 6 Rn. 34 ff.

1. Reichweite der Ausnahme vom IFG im BSIG

Nach der allgemeinen informationsfreiheitsrechtlichen Vorschrift § 1 Abs. 3 IFG gehen Regelungen über den Zugang zu amtlichen Informationen in anderen Rechtsvorschriften mit Ausnahme des § 29 VwVfG und § 25 SGB X vor. Spezialgesetzliche Informationszugangsrechte haben vor dem IFG unabhängig davon Vorrang, ob diese tatbestandlich enger oder weiter gefasst sind.[268] Eine solche vorrangige Spezialregelung kann für gegen das BSI und die Bundesnetzagentur gerichtete Informationsansprüche in § 8d BSIG gesehen werden.[269] Die entscheidende kollisionsrechtliche Frage ist, ob mit § 8d BSIG als spezielle Informationszugangsrechtsregelung die Anwendbarkeit des IFG ausgeschlossen ist. Die Frage ist grundsätzlich einfach, im Einzelfall aber häufig schwierig zu beantworten.[270]

Dem Wortlaut nach betrifft § 8d Abs. 1 BSIG die *Auskunft* zu bestimmten Informationen, während mit Abs. 2 der *Zugang* zu Akten geregelt wird. Aufgrund der Differenzierung in der Binnenstruktur der Norm ist hinsichtlich der beiden Informationsfreiheitsarten zu unterscheiden.

Eine informationsfreiheitsrechtliche Spezialnorm setzt einen abstrakt identischen sachlichen Regelungsgegenstand voraus.[271] Um Vorrangwirkung zu zeitigen, muss die betreffende Norm also Informationsrechte nicht nur für den Einzelfall regeln, sondern eine typisierte Regelung für Informationspflichtige nach dem IFG darstellen.[272] Eine Verdrängung soll dann regelmäßig anzunehmen sein, wenn eine bereichsspezifische Regelung vorliegt, die den Informationszugang nur für einen engen, bestimmbaren Personenkreis und damit nicht für „jedermann" öffnen will.[273] Ein vorrangiger Ausschluss sei zudem dort anzunehmen, wo die jeweiligen Rechte die gleichen Anliegen verfolgen „und/oder" identische Zielgruppen erfassen, mithin, wenn der Informationszugang in sachlicher und persönlicher Hinsicht spezifisch beschränkt sein soll.[274] Die Frage, ob die spezialgesetzliche Regelung abschließend ist, muss letztlich in jedem

[268] BT-Drs. 15/4493, S. 8.

[269] Für Auskunftsansprüche Dritter gilt für die Bundesnetzagentur gemäß § 109 Abs. 5 S. 8 TKG die Vorschrift des § 8d BSIG entsprechend. Aus dem Regelungsstandort ergibt sich, dass die Informationsbegrenzung nur für die Informationen aus der Meldepflicht gilt und nicht wie in § 8d BSIG auch für solche Informationen, die sich auf die branchenspezifischen Sicherheitsstandards und deren Erfüllungsnachweise beziehen. Insofern handelt es sich bei § 109 Abs. 5 S. 8 TKG um einen Rechtsfolgenverweis.

[270] *Rossi*, DVBl. 2010, 544 (557).

[271] BVerwG, BeckRS 2013, 46016, Rn. 46.

[272] *Debus*, in: Gersdorf/Paal (Hrsg.), BeckOK IMR, 11. Ed. 2016, IFG, § 1 Rn. 182; VG Hamburg BeckRS 2009, 35841; 2011, 45853.

[273] BfDI, 4. Tätigkeitsbericht 2012–2013, BT-Drs. 19/2000, S. 93.

[274] *Debus*, in: Gersdorf/Paal (Hrsg.), BeckOK IMR, 11. Ed. 2016, IFG, § 1 Rn. 184.

konkreten Einzelfall durch systematische und teleologische Auslegung geklärt werden.[275]

Der Auskunftsanspruch in § 8d Abs. 1 BSIG weicht zwar von dem in § 1 Abs. 1 S. 1 IFG formulierten Regelungsgegenstand ab, da dort der Zugang zu Informationen geregelt wird. Die Auskunft kann als eine individuelle Mitteilung über Tatsachen oder die Rechtslage definiert werden.[276] Sie ist demnach eine reine Wissenserklärung und vom Regelungsanliegen des IFG im Wesentlichen nicht zu trennen. Aus der systematischen Auslegung ergibt sich dann auch, dass die Auskunft eine Unterart des Informationszugangs ist. In sachlicher Hinsicht begrenzt die Regelung den Zugang zu Informationen über die branchenspezifischen Sicherheitsstandards für Betreiber kritischer Infrastrukturen und über deren Erfüllungsnachweise einschließlich Sicherheitsaudits, Prüfungen und Zertifizierungen sowie zu den Meldungen bei IT-Sicherheitsstörungen. Anträge auf Zugang zu diesen Informationen sind nicht bereits für sich unzulässig. Die Begrenzung bezieht sich auf den Modus der Abwägung. Den Anträgen kann das BSI im Rahmen einer Ermessensentscheidung entsprechen, wenn schutzwürdige Interessen dem nicht entgegenstehen und durch die Auskunft keine Beeinträchtigung sonstiger wesentlicher Sicherheitsinteressen zu erwarten ist. In persönlicher Hinsicht bezieht sich die Sonderreglung nicht auf „jeden", sondern auf „Dritte". Unter Dritten sind die nicht am Verfahren beteiligten Personen und nicht öffentliche Institutionen zu verstehen.[277] Eine generelle Begrenzung inhaltlicher Art besteht demnach nur für den Zugang zu personenbezogenen Daten, der gemäß § 8d Abs. 1 S. 2 BSIG nicht gewährt wird. Der Auskunftsanspruch führt letztlich nur zu einer teilweisen Begrenzung in persönlicher, sachlicher und inhaltlicher Hinsicht.

In gleicher Weise wird die Reichweite der Informationszugangsfreiheit durch § 8d Abs. 2 BSIG begrenzt.[278] Der Anspruch wird nur Verfahrensbeteiligten gewährt. Der Verweis auf § 29 VwVfG führt zu weiteren Einschränkungen. Die Einsicht in die Akten muss grundsätzlich für die Geltendmachung der eigenen rechtlichen Interessen erforderlich sein. Durch die Spezialregelung wird im Ergebnis der Zugang zu Akten beim BSI nicht generell ausgeschlossen.

---

[275] BVerwG, BeckRS 2013, 46016, Rn. 46; OVG Münster, BeckRS 2008, 38135; *Rossi*, DVBl. 2010, 554 (557).

[276] *Krajewski*/*Rösslein*, in: Grabitz/Hilf/Nettesheim (Hrsg.), AEUV/EUV, 57. Aufl. 2015, AEUV, Art. 15 Rn. 38.

[277] Darauf beschränkt sich aber BT-Drs. 18/4096, S. 50.

[278] Vgl. die Parallelvorschrift für Informationen über Betreiber kritischer Infrastrukturen im Energiesektor § 11 Abs. 1c S. 5 EnWG.

Der Anwendungsbereich des IFG wird durch das BSIG nur soweit verdrängt, wie die Lex-specialis-Regelung des § 8d BSIG reicht und soweit diese Regelung abschließend ist. Das IFG bleibt im Übrigen anwendbar.[279]

2. Auswirkungen der allgemeinen Ausnahmen vom Informationszugangsrecht

Da trotz der Ausnahmen von der Informationsfreiheit durch § 8d BSIG das IFG im Übrigen Anwendung findet, sind die Auswirkungen der allgemeinen Ausnahmen für den Zugang zu NIS-Informationen zu bestimmen. Die Ausnahmetatbestände in den §§ 3 bis 6 IFG dienen dem Schutz unterschiedlicher Rechtsgüter. Es können grundsätzlich öffentliche Interessen (§§ 3 und 4 IFG) und private Interessen (§§ 5 und 6 IFG) unterschieden werden. Entsprechende Ausnahmeregelung enthält Art. 4 der Transparenz-VO.

Für den Zugang zu Informationen bei Stellen der Union hat die stärkere Verortung des Informationszugangs im Verfassungsrecht praktische Konsequenzen im Abwägungsprozess, da mit anderen kollidierenden Grundrechtsgütern eine praktische Konkordanz herzustellen ist. Die lediglich einfachgesetzliche Verortung der Zugangsfreiheit führt dazu, dass sich das höherrangige Recht prinzipiell durchsetzt.[280] Betrifft ein Informationszugangsanspruch Informationen bei anspruchsverpflichteten Stellen der Union, streiten Art. 42 GRCh und Art. 15 Abs. 1 AEUV auf Ebene des höchstrangingen Rechts gegen kollidierende Rechtsgüter für den Zugang.

Bei der Auslegung des IFG sind die Unionsgrundrechte dagegen nicht in dem Ausmaß zu beachten, wie es etwa für das Umweltinformationsgesetz (UIG) geboten ist. Da die Umweltinformationsfreiheit durch Umweltinformations-RL 2003/4/EG zwingend vorgegeben wird, haben die mitgliedstaatlichen Maßnahmen die Grundrechte der Charta bei der Anwendung und Auslegung des europäischen Rechts gemäß Art. 51 Abs. 1 GRCh zu beachten.[281] Das IFG hat keine unmittelbare Entsprechung im unionsrechtlichen Sekundärrecht.

Für Informationen über die Internetsicherheit sind insbesondere Belange der Sicherheit (a), der Schutz vertraulich erhobener und übermittelter Daten (b), personenbezogener Daten (c), von Betriebs- und Geschäftsgeheimnissen (d) sowie der Schutz des geistigen Eigentums (e) von Bedeutung. Deren Bedeutung wird im Nachfolgenden anhand der Ausnahmetatbestände des IFG untersucht, da die jeweiligen Erwägungen auf die Transparenz-VO übertragbar sind.

---

[279] *Debus*, in: Gersdorf/Paal (Hrsg.), BeckOK IMR, 11. Ed. 2016, IFG, § 1 Rn. 180; *Bundesbeauftragte für Datenschutz und Informationssicherheit*, Anwendungshinweise zum IFG, 2007, S. 4.

[280] Vgl. für das Verhältnis von Datenschutz und Informationsfreiheit *Roßnagel*, MMR 2007, 16 (19).

[281] Vgl. EuGH, C-617/10, Rn. 21.

a) Belange der Sicherheit

Ein Anspruch auf Informationszugang besteht nicht, wenn das Bekanntwerden der Information die Belange der inneren und äußeren Sicherheit oder die öffentliche Sicherheit gefährden kann (§ 3 S. 1 Nr. 1 c), Nr. 2 IFG). Der Vergleich des Ausnahmetatbestands des § 3 Nr. 1 lit. c IFG mit § 3 Nr. 2 IFG ergibt, dass Ersterer sehr eng auszulegen ist. Nur erhebliche Belange werden geschützt.[282] Die Formel der Gefährdung der öffentlichen Sicherheit entspricht dem Begriff der klassischen ordnungsrechtlichen Gefahrenabwehr.[283] Aus der Formulierung „gefährden kann" ergibt sich, dass bereits eine abstrakte Gefahr den Informationszugang ausschließen kann. Die Herausgabe unmittelbar sicherheitskritischer Informationen (etwa über der Behörde bekannte Schwachstellen) dürfte ob dieser generalhaften Ausnahme der Informationsfreiheit aufgrund von Sicherheitsbelangen mit vergleichsweise geringem Begründungsaufwand zu verweigern sein. Eine Berücksichtigung der doppeltrelevanten Natur der Informationsdistribution (die Information kann sowohl der Sicherheitsgewährleistung dienen als auch den Missbrauch erleichtern) ist nicht vorgesehen. Wegen ihres Umfangs können die Ausnahmetatbestände in der Tat zur „Verlustliste der Informationsfreiheit" auch auf dem Gebiet der Internetsicherheit gezählt werden.[284] Der Blick auf die Praxis zeigt indes, dass Anträge nicht von Vorneherein aus Gründen der Sicherheit versagt werden.[285] Informationsanträge an das BSI oder die Bundesnetzagentur sind nicht *per se* aussichtslos.[286]

---

[282] *Rossi*, IFG, 2006, § 3 Rn. 15.

[283] *Jastrow/Schlatmann*, IFG, 2006, § 3 Rn. 63.

[284] *Kloepfer/von Lewinski*, DVBl. 2005, 1277 (1280).

[285] Zum Beispiel wurde die Frage, ob zwischen dem BSI und der US-amerikanischen National Security Agency (NSA) eine Kooperation bestehe, aufgrund von § 3 Nr. 1 a) IFG abgelehnt, weil nachteilige Auswirkungen auf internationale Beziehungen zu befürchten waren. *BSI*, Auskunft vom 17.07.2014 auf Antrag vom 19.06.2014, Az. B21-0100305/001, abrufbar unter: https://fragdenstaat.de/files/foi/18647/2014-07-17_-_bsi_kooperationen.pdf. Eine Ablehnung auf Grundlage des § 3 Nr. 1 c) IFG erging auf eine Anfrage hinsichtlich der Zusendung einer Auflistung aller vom BSI registrierten Domains in maschinenlesbarer Form. Die Auskunft hätte die vom Begriff der inneren und äußeren Sicherheit umfasste Funktionsfähigkeit des Staates und seiner Einrichtungen gefährdet, da zu befürchten wäre, dass diese Informationen für Angriffe in Form von „DNS-Hijacking" oder „DDos" missbraucht würden sowie die systematische Suche nach Schwachstellen erleichtern würde. *BSI*, Auskunft vom 11.09.2015 auf Antrag vom 11.08.2015, Az. B21-0100305/001, abrufbar unter: https://fragdenstaat.de/files/foi/33446/antwort-bsi-2015-09-11_geschwaerzt.pdf.

[286] Ein Blick auf die Statistik der Internetplattform fragdenstaat.de hält 20 erfolgreiche und 7 teilweise erfolgreiche Anträge von 75 Anfragen fest, abrufbar unter: Fragdenstaat.de, https://fragdenstaat.de/behoerde/bundesamt-fur-sicherheit-in-der-informationstechnik/. Aufgrund des weiteren Aufgabenbereichs fällt die Aussagekraft für die Bundesnetzagentur

b) Geheimnisschutz auf Grund öffentlicher Belange

Informationszugangsansprüche können des Weiteren im Interesse des Geheimnisschutzes abgelehnt werden. Zu unterscheiden ist der Geheimnisschutz aufgrund besonderer öffentlicher Belange (Vertraulichkeitspflichten, Berufsgeheimnisse, besondere Amtsgeheimnisse, § 3 Nr. 4 IFG) und aufgrund privater Belange, d. h. von Betriebs- und Geschäftsgeheimnissen (§ 6 S. 2 IFG).[287]

Anders als bei beim Schutz von Betriebs- und Geschäftsgeheimnissen kommt es nicht auf das Interesse, sondern auf die Pflicht zur Geheimhaltung an. Der Geheimnisschutz wird durch besondere Rechtsvorschriften bewirkt. § 3 Nr. 4 IFG ist demnach eine Rezeptionsnorm für fachgesetzliche Regelungen. Sind Informationen durch besondere Rechtsvorschriften geschützt, sind sie nach dem IFG nicht zugänglich.[288] Art und Umfang des Geheimnisschutzes ergeben sich damit aus Spezialgesetzen der Rechtsgebiete.

Ausweislich des Wortlauts von § 3 Nr. 4 IFG können Rechtsvorschriften oder Allgemeine Verwaltungsvorschriften zum Schutz von Verschlusssachen den Informationszugang versperren. Unter „Rechtsvorschrift" sind nicht nur Parlamentsgesetze, sondern auch untergesetzliches Recht zu verstehen.[289] Eine die Vertraulichkeit anordnende Rechtsverordnung muss sich aber auf eine förmliche gesetzliche Rechtsgrundlage zurückführen lassen, die im konkreten Regelungszusammenhang den Erlass von Normen zur Sicherung eines materiellen Geheimnisschutzes umfasst.[290] Eine solche Ermächtigungsgrundlage mit Bezug auf sicherheitsrelevante Informationen findet sich im einfachgesetzlichen NIS-Recht nicht.

Von besonderer Bedeutung ist daher der Schutz von Verschlusssachen. Für deren Schutz genügt noch die formale Einstufung als Verschlusssache. Der Ausschlussgrund des § 3 Nr. 4 IFG setzt vielmehr voraus, dass die Einstufung den materiellen Anforderungen der Einstufungsvorschrift genügt.[291] So konnte der Antrag auf Übermittlung des Quellcodes für den sog. Bundestrojaner nach § 3 Nr. 4 IFG abgelehnt werden, da es sich bei den Informationen um Verschlusssachen im Sinne des § 4 Abs. 1 Sicherheitsüberprüfungsgesetz (SÜG) in Verbindung mit § 2 Verschlusssachen-Anweisung (VSA) handelte. Das öffentliche Geheimhaltungsinteresse war darin begründet, dass die Kenntnisnahme des Quellcodes nicht nur den Erfolg polizeilicher Maßnahmen gefährdet hätte,

---

geringer aus. Von 133 Anfragen waren 59 erfolgreich und 14 teilweise erfolgreich, abrufbar unter: Fragdenstaat.de, https://fragdenstaat.de/behoerde/bundesnetzagentur/.

287 Vgl. BT-Drs. 15/4493, S. 9, 14.

288 *Schoch*, IFG, 2009, § 3 Rn. 204 f.

289 BVerwG, NVwZ 2016, 1820 (1821).

290 OVG Berlin-Brandenburg, BeckRS 2015, 44851, II. 1. a).

291 *Schoch*, IFG, 2009, § 3 Rn. 229.

sondern die Information durch Dritte für IT-Angriffe hätte missbraucht werden können.[292]

§ 3 Nr. 4 IFG macht deutlich, dass das IFG zwar den Grundsatz beschränkter Aktenöffentlichkeit aufhebt, der Zugang aber nur zu Informationen gewährt wird, die zuvor schlicht nichtöffentlich waren. Auch wenn der Grundsatz „So viel Information wie möglich, so viel Geheimnisschutz wie nötig" gelten soll,[293] werden Geheimhaltungsnormen durch das IFG nicht ausgehebelt.

c) Schutz vertraulich erhobener und übermittelter Informationen

Den Schutz des Vertrauens in die Verschwiegenheit der Verwaltung und damit der Kooperation Privater mit öffentlichen Stellen bezweckt § 3 Nr. 7 IFG. Der Anspruch auf Informationszugang besteht nicht, soweit das Interesse des Dritten an einer vertraulichen Behandlung zum Zeitpunkt des Zugangsantrags fortbesteht. Der Ausschlussgrund soll die Bereitschaft zur Kooperation mit der Verwaltung fördern und berücksichtigt dabei insbesondere den Wissensbedarf der Verwaltung.[294] Eine parallele Vorschrift findet sich weder im VIG noch im sonstigen Informationsrecht. Vom Schutz des § 3 Nr. 7 IFG werden alle in die Sphäre des Staates gelangenden Informationen erfasst.[295] Geschützt werden demnach die von NIS-Behörden vertraulich erhobenen und vertraulich an sie übermittelten Daten.[296]

In erster Linie bezweckt § 3 Nr. 7 IFG den Schutz der freiwilligen Informationszusammenarbeit. Insbesondere die Informationen von Hinweisgebern (z. B. Whistleblowern) sollen vor einer unbeeinflussten Herausgabe nach außen geschützt werden.[297] Die Schutzwürdigkeit des Vertrauens besteht dann, wenn der Informationsgeber gegenüber dem Informationsnehmer ausdrücklich oder implizit voraussetzt, dass die Information der Öffentlichkeit nicht zugänglich gemacht wird.[298] Es bleibt aber anhand der Umstände des Einzelfalls zu beurteilen, ob eine Information nicht für die Öffentlichkeit bestimmt ist. Leitfrage bei der Bestimmung ist, ob die in die Sphäre des Staates gelangte Information ohne

---

[292] Bundesamt für Sicherheit in der Informationstechnik, Auskunft vom 09.07.2015 auf Antrag vom 10.06.2015, Az. B21-0100305/001, abrufbar unter: https://fragdenstaat.de/files/foi/30973/ablehnung-bsi_geschwaerzt.pdf.

[293] BT-Drs. 15/4493, S. 11.

[294] OVG Berlin-Brandenburg, Urteil vom 05.10.2010 – 12 B 5/08, BeckRS 2010, 56783, II. 2; vgl. BT-Drs. 15/4493, S. 11.

[295] *Schirmer*, in: Gersdorf/Paal (Hrsg.), BeckOK IMR, 11. Ed. 2016, IFG, § 3 Rn. 187.

[296] *Sellmann*/*Augsberg*, WM 2006, 2293 (2300).

[297] Vgl. *Jastrow*/*Schlatmann*, IFG, 2006, § 3 Rn. 106.

[298] VG Berlin, Urteil vom 22.03.2012 – VG 2 K 102.11, BeckRS 2012, 50035, 2b.

die (Zusicherung der) Vertraulichkeit nicht hätte erhoben werden können bzw. nicht übermittelt worden wäre.[299]

Nicht alle Informationen, die von den NIS-Behörden erhoben oder die ihnen zur Verfügung gestellt werden, können als vertraulich angesehen werden. Würden alle generierten Informationen neben dem verwaltungsrechtlich gewährleisteten Geheimnisschutz dem Vertraulichkeitsschutz zuzuordnen sein, wäre der Zugang zu diesen Informationen durch eine faktische Bereichsausnahme weitgehend gesperrt. Eine solche Ausnahme ist aber nur für die Nachrichtendienste und besondere Sicherheitsbehörden vorgesehen (§ 3 Nr. 8 IFG).[300]

Ein besonderes Vertraulichkeitsinteresse im Sinne dieses Ausnahmetatbestandes dürfte vor allem für die auf freiwilliger Basis übermittelten Sicherheitsvorfälle bestehen. Dies sind insbesondere die Meldungen von Kleinstunternehmen und kleineren Unternehmen, die nicht von der Meldepflicht erfasst sind (Art. 16 Abs. 11 NIS-RL). Vom Schutz vor einer Weitergabe vertraulich gemeldeter Informationen geht neben der durch die Meldung möglichen zivilrechtlichen Schadensminderung eine zusätzliche Anreizwirkung aus. Die informationsfreiheitsrechtliche Ausnahme des § 3 Nr. 7 IFG ist daher nicht nur als kognitive Begrenzung aufzufassen, sondern umgekehrt auch als Bedingung der Generierung von Wissen, da sie es den Unternehmen erleichtert, den Behörden exklusive Informationen zuzuspielen.

d) Datenschutz

Personenbezogene Daten dürfen nur höchst ausnahmsweise gemäß § 5 IFG herausgegeben werden. Darin ist nicht schon für sich eine bloße Abschirmung der Öffentlichkeit von potenziell relevanten Informationen zu sehen. Bei einer generalisierenden Überlegung sorgt die Begrenzung der Informationsdistribution für eine begrüßenswerte Freisetzung „kognitiver Innovationspotentiale“[301], weil der öffentlichen Beobachtung entzogene Sphären eher dazu führen, dass der Einzelne die „Risiken des Scheiterns“ in Kauf nimmt, da so gewonnene Freiheiten zu neuen Handlungen anregen und eine „Ordnung des Experimentierens institutionalisieren“.[302] Der Einzelne kann aufgrund von § 5 IFG grundsätzlich davon ausgehen, dass die ihn betreffenden personenbezogenen Daten geschützt werden.

---

[299] So *Schirmer*, in: Gersdorf/Paal (Hrsg.), BeckOK IMR, 11. Ed. 2016, IFG, § 3 Rn. 189.

[300] Vgl. ferner zur Bundesanstalt für Finanzdienstleistungsaufsicht VGH Kassel, Entscheidung vom 24.03.2010 – 6 A 1832/09, II. 3.

[301] *Augsberg*, Informationsverwaltungsrecht, 2014, S. 219 f.

[302] *Ladeur*, Der Staat gegen die Gesellschaft, 2006, S. 125.

Mit Blick auf die Informationsdistribution zum Zweck der Internetsicherheit kann von § 5 IFG eine erhebliche Begrenzung für den Informationsfluss ausgehen. Die Verweigerung der Herausgabe von Informationen kommt insbesondere dann in Betracht, wenn mit einer weiten Auslegung des Kriteriums der Personenbeziehbarkeit Maschinendaten wie IP-Adressen als personenbezogene Daten zu behandeln sind.[303] Verfügt die NIS-Verwaltung etwa über IP-Adressen von Botnetzwerken, könnten die Daten mit existierenden Informationen zusammengeführt werden, um Botnetz-Beschreibungen und Filter sowohl um weitere IP-Adressen als auch um die Beschreibung der Aktivität des Botnetzes anzureichern.[304] Eine Verwertung der bei der Verwaltung vorhandenen Informationen zum Zwecke des Selbstschutzes kommt dann nur nach einer entsprechenden Abwägung in Betracht. Bei derart abstrakten Gefährdungen für den Einzelnen dürfte allerdings dem Datenschutz regelmäßig kein relativer Vorrang einzuräumen sein. Ein Verlust des Datenschutzes im Sinne der Privatsphäre (*privacy*) ist in diesen Konstellationen typischerweise nicht zu befürchten.

e) Betriebs- und Geschäftsgeheimnisse

Der Schutz von Betriebs- und Geschäftsgeheimnissen ist im IFG besonders stark ausgeprägt.[305] Durch den Einwilligungsvorbehalt in § 6 S. 2 IFG ist der Rechtsinhaber im Vergleich zum datenschutzrechtlich Betroffenen sogar im Ergebnis stärker geschützt.[306] Eine Abwägung der widerstreitenden Interessen der Beteiligten erfolgt nicht (vgl. Art. 4 lit. b) Transparenz-VO).[307] Eine Offenbarungsvermutung wie bei telekommunikationsrechtlichen Beschlusskammerverfahren (§ 136 S. 3 TKG) besteht ebenfalls sind.

Der Begriff der Betriebs- und Geschäftsgeheimnisse wird im IFG nicht näher präzisiert. Aus den Gesetzesbegründungen zu den speziellen Informationsfreiheitsgesetzen geht hervor, dass sich die Gesetzgeber an dem gewachsenen Begriffsverständnis von § 17 UWG orientieren und so eine einheitliche rechtsgebietsübergreifende Begriffsbestimmung ermöglichen wollten.[308] Ob ein Betriebs- oder Geschäftsgeheimnis vorliegt, ist aber auch anhand der Besonder-

---

[303] Siehe § 3 E. II. 1. b).

[304] Vgl. zu dieser Informationsverwertung im Rahmen eines Botnetz-Monitorings *Engeler/Jensen/Obersteller/Deibler/Hansen*, Monitoring durch Informationsfusion und Klassifikation zur Anomalieerkennung, 2014, S. 9.

[305] Vgl. auch die Verankerung in Art. 41 Abs. 2 lit. b GRCh.

[306] Kritisch *Kugelmann*, NJW 2005, 3609 (3612).

[307] BVerwG, NVwZ 2009, 1113 (1114).

[308] Vgl. *Rossi*, IFG, 2006, § 6 Rn. 63; *Kloepfer*, Informationsfreiheitsgesetz und Schutz von Betriebs- und Geschäftsgeheimnissen, Juni 2011, S. 15 f., online abrufbar.

heiten des jeweiligen Sach- und Rechtsgebiets zu bestimmen.[309] Es kann somit auf Ausführungen zum viergliedrigen Schutztatbestand und auf das Beispiel des Schutzes von IT-Sicherheitslücken verwiesen werden.[310]

Bei der Entscheidung über die Offenlegung ist zu beachten, dass der Schutz der Geheimnisse kein grundsätzlicher, sondern ein funktionaler Schutz ist. Soweit ein berechtigtes Interesse des Unternehmens an der Nichtverbreitung nicht gegeben ist, scheidet der Schutz nach § 6 S. 2 IFG aus. Informationen über betrügerische Geschäftspraktiken etwa unterfallen *per se* nicht dem Schutzbereich.[311] Ist die Offenlegung des exklusiven, in der Regel technischen Wissens nicht geeignet, die Wettbewerbsposition des Unternehmens nachteilig zu beeinflussen, fehlt es regelmäßig an einem berechtigten Interesse.[312] Daten von Monopolunternehmen sind demnach grundsätzlich nicht schutzwürdig.

Im Ergebnis wird das Informationsinteresse aufgrund des Einwilligungsvorbehalts, der letztlich ein Vetomechanismus ist, nur selten zur Geltung kommen.[313]

f) Geistiges Eigentum

Das geistige Eigentum ist vor dem Informationszugang durch den absoluten Ausschlusstatbestand des § 6 S. 1 IFG geschützt. Soweit der Schutz geistigen Eigentums entgegensteht, besteht der Anspruch auf Informationszugang nicht. Zum geistigen Eigentum gehören technikbezogene gewerbliche Schutzrechte wie die des gewerblichen Rechtsschutzes in Form von Marken-, Patent-, Gebrauchsmuster- und Geschmacksmusterrechten sowie geistige Schöpfungen im Sinne des Urheberrechts.[314]

Der Ausschlussgrund kann etwa dann Wirkungen zeitigen, wenn vorhandene Quellcodes zum Zwecke des Reviews herausverlangt werden. Der Informationszugang kann verweigert werden, sofern der Code oder das Programm urheberrechtlich geschützt ist. Das BSI darf aber auf Grundlage von § 7a Abs. 2 S. 2

---

309 Vgl. Gesetzesbegründung, BT-Drs. 15/4493, S. 14.

310 Siehe § 3 E. III. 2.

311 *Heußner*, Informationssysteme im Europäischen Verwaltungsverbund, 2007, S. 321.

312 BVerwG, NVwZ 2009, 1113 (1113); *Stancke*, BB 2013, 1418 (1424).

313 Verständlich ist die Regelung vor dem Hintergrund, dass eine Sicherheitsbehörde schnell an ihre Wissensgrenze stößt, wenn sie bei der Entscheidung des Zugangs zu Betriebs- und Geschäftsgeheimnissen eine wirtschaftspolitische Grundsatzentscheidung trifft. Vergleichbare Regelungen wie § 3 S. 2 des Verbraucherinformationsgesetzes (VIG) zeigen hingegen, dass ein Einwilligungsvorbehalt rechtspolitisch nicht zwingend ist. Vgl. *Spindler*, ZGR 2011, 690 (695); *Kloepfer*/*Greve*, NVwZ 2011, 577 (578).

314 *Guckelberger*, in: Gersdorf/Paal (Hrsg.), BeckOK IMR, 11. Ed. 2016, IFG, § 6 Rn. 4.

BSIG Zugang zu den aus Produktuntersuchungen gewonnenen Erkenntnissen gewähren.

Im Einzelfall kann es durchaus fraglich sein, ob der Informationsfreiheit Schutzrechte Dritter entgegengehalten werden können. So kann bei Urheberrechten das dem Urheber zustehende Veröffentlichungsrecht nach § 12 UrhG bereits dadurch verbraucht sein, dass der Urheber selbst sein Werk an die Behörde weitergibt und es somit im Sinne von § 12 UrhG bereits veröffentlicht.[315] Wird über die Einsicht in Akten hinaus auch die Herstellung von Vervielfältigungsstücken begehrt, kann daneben die Beeinträchtigung des Vervielfältigungsrechts nach § 16 UrhG mit dem Argument bezweifelt werden, dass mit Blick auf § 53 UrhG, wonach eine Vervielfältigung nur zum privaten Gebrauch zulässig ist und dessen Abs. 6 die Weitergabe von Kopien weitgehend ausschließt, eine Beeinträchtigung des Urheberrechts nicht zu befürchten ist.[316] Erhält die Behörde ein Dokument mit Zustimmung des Rechtsinhabers, ist zudem der Eingriff in das Verbreitungsrecht nach § 17 UrhG fraglich, da hinsichtlich des übergebenen Dokuments eine Erschöpfung nach § 17 Abs. 2 UrhG vorliegen kann.[317]

Grundsätzlich in Betracht kommt auch, dass sich die NIS-Behörde auf eigene geistige Eigentumsrechte beruft, da § 6 IFG nicht zwischen öffentlichen und privaten Interessen differenziert. Sofern sie aber überhaupt schutzfähig sind, sprechen die verfassungsrechtlichen Wertungen zum Informationszugang dafür, dass die Behörde insbesondere dann nicht von ihren Verwertungsrechten Gebrauch macht, wenn die Werke und Schriftstücke mit Steuermitteln geschaffen wurden.

Soweit die NIS-Behörde eine Datenbank selbst erstellt oder verwaltet, kommt als Schranke des Informationszugangs das Recht des Datenbankherstellers im Sinne der RL 96/9/EG bzw. des § 87a UrhG grundsätzlich nicht in Betracht, da das Recht unternehmensbezogen ist und die Tätigkeit der NIS-Behörden nicht als wirtschaftlich zu qualifizieren ist.[318]

---

[315] *Raue*, JZ 2013, 280 (285).

[316] *Wiebe*/*Ahnefeld*, CR 2015, 127 (130); *Raue*, JZ 2013, 280 (283).

[317] *Raue*, JZ 2013, 280 (287). Der EuGH, C-128/11, hat offen gelassen, ob der Erschöpfungsgrundsatz auch digitale Güter und übertragene Datensätze erfasst. Dazu *Marly*/*Wirz*, EuZW 2017, 16 (19).

[318] Zwar kommen öffentliche Stellen als Inhaber dieses *sui-generis*-Rechts in Betracht, allerdings nur, soweit sie auch eine wirtschaftliche Tätigkeit ausüben, vgl. EuGH, C-138/11, Rn. 36 ff.

3. Pauschalabwägung der Interessen im BSIG

Vor dem Hintergrund des differenzierten Regelwerks des IFG zum Schutz der der Informationsfreiheit entgegenstehenden Interessen stellt sich die Frage der Erforderlichkeit der Regelungen in § 8d BSIG.

Die NIS-Behörde darf ein Auskunftsverlangen ablehnen, wenn schutzwürdige Interessen des betroffenen Betreibers kritischer Infrastrukturen dem nicht entgegenstehen und durch die Auskunft keine Beeinträchtigung wesentlicher Sicherheitsinteressen[319] zu erwarten ist. Problematisch dabei ist, dass ermessenslenkende Maßstäbe nur für die Ausschlussgründe genannt werden und nicht für legitime Interessen der informationsinteressierten Dritten. Eine Abwägung mit privaten oder öffentlichen Interessen ist dem Wortlaut nach nicht vorgesehen. Durch die Regelung wird eine Auskunft bereits dann ausgeschlossen, wenn schutzwürdige Interessen entgegenstehen. Der Antrag auf Auskunft könnte bereits bei geringsten Sicherheitsinteressen des Betreibers abgelehnt werden, selbst wenn dem gewichtigere Sicherheitsinteressen eines anfragenden Unternehmens, das sich selbst besser schützen möchte, gegenüberstehen. Die Interessen des betroffenen Betreibers haben selbst bei einem „überwiegenden" Informationsinteresse Vorrang. Dem Wortlaut nach wäre auch eine Teilauskunft unmöglich, „soweit" schutzwürdige Interessen nicht entgegenstehen.

Die starre Regelung ist vor dem Hintergrund der rechtspraktischen Schwierigkeiten zu verstehen, die sich im informationsfreiheitsrechtlichen Interessenausgleich stellen. Für die Geheimhaltung sind stets konkrete Schutzinteressen anzuführen, während ein konkretes Informationsinteresse dem in der Regel nicht gegenübergestellt werden kann, weil der Zugangsanspruch gerade nicht vom Antragsteller die Geltendmachung eines besonderen Interesses verlangt.

Einer zu pauschalen Abwägungsmaxime, die den Informationszugangsanspruch bereits bei einem schutzwürdigen substanziierten Geheimhaltungsinteresse zurücktreten lässt, ist aber entgegenzuhalten, da es sich bei einem Informationszugangsanspruch um ein mehrpoliges Rechtsverhältnis handeln kann, dessen Bescheidung die Einbeziehung privater und öffentlicher Interessen verlangt.[320] Eine solche pauschale Abwägung widerstreitender, begründeter Interessen kann einen im Einzelfall schonenderen Ausgleich der Grundrechtspositionen vereiteln.

Zwar sind für Zugangsansprüche auch im Kontext der Internetsicherheit das Informations- und Geheimhaltungsinteressen jeweils ihre Antipoden, die konfligierenden Interessen können sich aber auf den gleichen Schutzzweck bezie-

---

[319] Vgl. Art. 1 Abs. 6 NIS-RL.

[320] Vgl. aber VG Braunschweig, BeckRS 2013, 48838 (Rn. 43); kritisch *Wegener*, NVwZ 2015, 609 (615).

hen. Verlangt ein Betreiber kritischer Infrastrukturen Informationen über von einem anderen Betreiber gemeldete IT-Schwachstellen einschließlich der getroffenen Abhilfemaßnahmen, so dient dies nicht nur der Befriedigung der Neugier, sondern selbst der Härtung der Sicherheit in kritischen Infrastrukturen. Wird die Auskunft gewährt, dient dies folglich zum einen dem privaten Interesse des Betreibers und zum anderen dem öffentlichen Interesse an der Sicherheit der kritischen Infrastrukturen. Denkbar ist daneben, dass der Informationszugang der Präzisierung der IT-Sicherheitsstrategien oder der Bestimmung weiterer Forschungs- und Entwicklungsanstrengungen dient.

Der pauschale Ausgleich multipolarer Interessen in § 8d BSIG verhindert von vorneherein den Grundrechtsvoraussetzungsschutz durch Informationsvorsorge im Einzelfall, obwohl das Informationshandeln durch Gewährung des Informationszugangs neben den begrenzt verfügbaren rechtlichen Maßnahmen eine der wenigen tatsächlichen Möglichkeiten darstellt, die Grundrechte des Einzelnen und die Gewährleistungsverantwortung des Staates zu verwirklichen. Die Konturierung und Rationalisierung der Abwägung durch grundrechtlich geschützte Positionen (bei Bürgern nicht zuletzt das Grundrecht auf Gewährleistung der Integrität und der Vertraulichkeit informationstechnischer Systeme) schließt die starre Regelung des § 8d BSIG aus.

Soweit für den pauschalen Vorrang der Schutzinteressen des Betreibers das Interesse an seiner Reputation angeführt werden kann, ist zu bedenken, dass nicht jede Auskunft über eine Information im Rahmen der Meldepflicht zu einem Reputationsverlust führt. Im Gegenteil, die Information über die erfolgreiche Abwehr eines Cyberangriffs kann für das Ansehen eines Unternehmens sogar förderlich sein. Kam es infolge eines Angriffs zu einem Ausfall oder eine Beeinträchtigung, so dürfte ein Imageschaden zudem erst dann drohen, wenn damit die Information verbunden ist, dass dem Unternehmen ein bestimmtes Verhalten oder Unterlassen vorzuwerfen ist.

Für einen hohen Schutz der Betreiberinteressen sprechen indessen die sich aus der Auskunft ergebenden Haftungsrisiken. Eine erlangte Information kann der Beweisführung des Geschädigten in einem zivilrechtlichen Haftungsprozess dienen. Allein das Risiko eines Haftungsprozesses könnte das Vertrauen der meldepflichtigen Unternehmen in die Vertraulichkeit der übermittelten Informationen und damit die Funktionsfähigkeit des Meldesystems als solches erschüttern.[321] Unionsrechtlich sprechen Art. 14 Abs. 3 S. 2 und Art. 16 Abs. 3

[321] Im US-amerikanischen *Cybersecurity Information Sharing Act* von 2015 (*CISA*), H.R. 2029 – Consolidated Appropriations Act, 2016, Division N, ist gemäß Sec. 104 d) (4) (B) (ii) die Offenlegung eines *thread indicator* oder der *defense measure* über alle Informationsfreiheitsgesetze (*freedom of information law*, *open government law*, *open meetings law*, *open records law*, *sunshine law* oder vergleichbare Gesetze) generell ausgeschlossen. Dies ist auf

S. 2 NIS-RL für die Schutzwürdigkeit dieser Interessen. Allerdings sollen die Mitgliedstaaten den Betreibern nur Schutz vor einer erhöhten Haftung bieten. Die allgemeine Haftung ist nicht prinzipiell auszuschließen. Gegen die undifferenzierte Anerkennung des grundsätzlich berechtigten Interesses am Schutz der Vertraulichkeit der übermittelten Informationen im Rahmen der Informationsfreiheit spricht schließlich, dass diesem schon durch die Möglichkeit Rechnung getragen wird, Sicherheitsvorfälle nach § 8b Abs. 4 BSIG pseudonym über eine Kontaktstelle zu melden.

Neben dem Auskunftsanspruch ist der Zugang zu Akten nach § 8d Abs. 2 BSIG gänzlich undifferenziert geregelt. Der Informationszugangsanspruch ist absolut und ausnahmslos mit der Begründung eingeschränkt, es handele sich um „hochsensible, kumulierte sicherheitskritische Informationen, die einem besonders hohen Schutzbedürfnis unterliegen" und deren Risikopotential die Zugänglichkeit von vorneherein einschränke.[322] Dabei erscheint die Beschränkung auf alle Akten zu Lasten einer Einzelfallabwägung unangemessen, denn das IFG stellt bereits differenzierende Möglichkeiten bereit, die Offenlegung zu verhindern, wenn ein solcher Schaden zu befürchten ist.

IV. Bereitstellung und Verwendung der Informationen

Die informationsverwaltungsrechtliche Bedeutung des Informationszugangs wird davon beeinflusst, welche Qualität die Informationen, zu denen Zugang besteht, aufzuweisen haben. Angesichts der Menge und der (subjektiven) Komplexität der Daten kann es sinnvoll sein, die Informationen, zu denen ein Zugangsanspruch besteht, so bereitzustellen, dass sie nicht nur für Menschen, sondern auch von Maschinen lesbar sind. Für die Frage, in welchem Umfang die Informationen zirkulieren können und ob sie kommerziell für neue Sicherheitsprodukte verwertet werden können, ist zu bestimmen, welche Anforderungen an die Verwendung der bereitgestellten Informationen zu stellen sind.

Im Gegensatz zu den Publikumsinformationen können an die Qualität der zugänglich gemachten Informationen grundsätzlich keine besonderen Anforde-

---

erhebliche Kritik gestoßen, vgl. *Sweren-Becker*, Congress Working in the Dark on Cybersecurity Bill, American Civil Liberties Union (ACLU) vom 17.11.2015, online abrufbar; vgl. aber *Zheng*/*Lewis*, Cyber Threat Information Sharing: Recommendations for Congress and the Administration, 2015, S. 5. Im Wesentlichen ist die Pauschalausnahme aber damit zu begründen, dass einerseits in einem sehr weitreichenden Ausmaß mit öffentlichen Stellen Informationen geteilt werden können und andererseits, dass das Gesetz die Informationen als auf freiwilliger Basis mitgeteilt ansieht. Für einen solchen Informationsaustausch würde § 3 Nr. 7 IFG einen ähnlichen Ausschluss für den Informationszugang darstellen.

[322] BT-Drs. 18/4096, S. 51 f.

rungen gestellt werden (1.). Werden Daten über das Internet zur Verfügung gestellt, sind diese unter bestimmten Voraussetzungen maschinenlesbar bereitzustellen (2.). Die Weiterverwendung bereitgestellter Informationen kann von den NIS-Behörden grundsätzlich nicht weiter beeinflusst werden (3.).

1. Anforderungen an die Informationen

Die über das Informationsfreiheitsrecht zugänglichen Daten und Informationen sind regelmäßig Nebenprodukte der öffentlichen Aufgabenerfüllung, weil die Daten ursprünglich zu einem anderen sachlichen Zweck erhoben wurden. Daher liegen die Informationen nicht von vorneherein in einer zur Veröffentlichung besonders geeigneten Form vor. Wohl aus dem Grund, dass die Informationsfreiheit unter dem Aspekt der demokratischen Kontrolle und Partizipation der Bürger und der Akzeptanz administrativer Entscheidungen verstanden wird, sind die Anforderungen an das Qualitätsniveau der zugänglichen Informationen im allgemeinen Informationsfreiheitsrecht auch entsprechend gering, da den genannten Zwecken auch so Genüge getan wird.[323] „Für andere, für weiter gehende Verwendungszwecke erweist sich das Informationsfreiheitsrecht […] dagegen eher als Fundgrube denn als Fachhandel."[324]

Im Unterschied zu den Publikumsinformationen besteht im Rahmen des Informationszugangs grundsätzlich keine Richtigkeitsgewähr (vgl. § 7 Abs. 3 S. 2 IFG).[325] Die Behörden trifft keine amtliche Beschaffungs- und Aufbereitungspflicht.[326] Sie haben auch nicht den Inhalt der Informationen zu prüfen.[327] Die Informationsbegehrenden haben die Informationsbestände so anzunehmen, wie sie vorhanden sind.

Weitergehende Anforderungen an die Bereitstellung der vorhandenen Informationen folgen lediglich aus allgemeinen Rechtsgrundsätzen. Der Anspruch der Vollständigkeit der Daten bezieht sich nur auf den Bestand der vorliegenden Informationen. Der Verzicht des Gesetzgebers auf weitere Anforderungen an die Information trägt der Eigenheit der gesellschaftlichen Wissensproduktion Rechnung. Der Wert und die Verarbeitung von Informationen sind stets an die

---

[323] Vgl. *Schoch*, EuZW 2011, 388 (394); *Rossi*, NVwZ 2013, 1263 (1264), der allenfalls in § 7 Abs. 1 S. 3 IFG eine schwache mittelbare Beschränkung der Nutzung erkennt.

[324] *Rossi*, NVwZ 2013, 1263 (1264).

[325] Vgl. dagegen Art. 8 RL 2003/4/EG bzw. § 7 Abs. 3 UIG. Danach gewährleisten die informationspflichtigen Stellen, soweit möglich, dass alle Umweltinformationen, die von ihnen oder für sie zusammengestellt werden, auf dem gegenwärtigen Stand exakt und vergleichbar sind.

[326] *Gurlit*, Die Verwaltung 44 (2011), 75 (90).

[327] *Rossi*, NVwZ 2013, 1263 (1265).

Rezeption gebunden, weshalb eine unverarbeitete Weitergabe die weitere Verarbeitung am wenigsten verfälscht.

2. Weiterverwendung zugänglicher Informationen

Einen Beitrag zur Sicherheitsgewährleistung kann die Distribution von sicherheitsbezogenen Informationen schließlich leisten, wenn sich das wirtschaftliche Potenzial der Daten dergestalt realisiert, dass Informationen zur Entwicklung innovativer und besserer IT-Sicherheitsprodukte oder Dienstleistungen beitragen können. Es stellt sich also die Frage, ob auf Grund des Informationsfreiheitsrechts zusätzliche Anforderungen an die weitere Nutzung der von NIS-Behörden zugänglich gemachten Daten zu stellen sind.

Grundlage für das Recht zur Weiterverwendung von Informationen der öffentlichen Hand ist die Public-Sector-Information-Richtlinie 2003/98/EG (PSI-Richtlinie), die durch das Informationsweiterverwendungsgesetz (IWG) umgesetzt wird.[328] Die PSI-Richtlinie von 2003 bezweckt, einen unionsweiten Mindeststandard für die Nutzung von Dokumenten öffentlicher Stellen zu schaffen (Art. 1 Abs. 1 RL 2003/98/EG). Hintergrund der Regelungen zur Weiterverwendungsfreiheit von Daten ist die Anerkennung, dass auch staatlichen Informationen ein wirtschaftlicher Wert zukommen kann.[329]

Vom Anwendungsbereich erfasst sind nach § 2 Abs. 1 IWG öffentliche Stellen. Als öffentliche Stellen gelten nach § 2 Abs. 1 Nr. 1 b) IWG juristische Personen des öffentlichen oder privaten Rechts, die zu einem bestimmten Zweck gegründet wurden, im Allgemeininteresse liegende Aufgaben nichtgewerblicher Art erfüllen und die überwiegend durch öffentliche Stellen finanziert oder beherrscht werden. Erfasst sind also grundsätzlich auch NIS-Stellen.

Weiterverwendung ist nach Art. 2 Nr. 4 PSI-Richtlinie bzw. § 2 Nr. 3 IWG jede Nutzung der Informationen für kommerzielle oder nichtkommerzielle Zwecke, die über die Erfüllung öffentlicher Aufgaben hinausreicht und die in der Regel auf die Erzielung von Entgelt gerichtet ist. Regelmäßig keine Weiterverwendung stellen die intellektuelle Wahrnehmung einer Information und die Verwertung des dadurch erlangten Wissens dar.[330] Im Schwerpunkt liegt somit dann eine Weiterverwendung vor, wenn durch Verarbeitung und Aufbereitung ein Mehrwertprodukt entsteht, das sich durch ein neues, angereichertes Mehrwertangebot (*added value*) auszeichnet. Zwar wird durch die PSI-Richtlinie bzw. das IWG kein Anspruch auf Zugang zu Informationen begründet, Art. 3

---

328 Vgl. BT-Drs. 16/2452, S. 7.

329 Vgl. *Püschel*, Informationen des Staates als Wirtschaftsgut, 2006, S. 21 ff.

330 Vgl. Legaldefinition des Art. 2 Nr. 4 Richtlinie 2003/98/EG.

Abs. 1 PSI-Richtlinie bzw. § 1 Abs. 2a IWG.[331] Das IWG gilt nicht für Informationen, an denen kein oder nur ein eingeschränktes Zugangsrecht besteht, § 1 Abs. 2 Nr. 1 IWG.[332] Durch die Änderungsrichtlinie 2013/37/EU und die Novellierung des IWG 2015 ist aber ein echter Anspruch auf Weiterverwendung eingeführt worden. Nach § 3 IWG a. F. war Voraussetzung der Weiterverwendung von Informationen, dass die öffentliche Stelle die Weiterverwendung bereits einmal gestattet hatte. Es bestand kein Recht auf erstmalige Weiterverwendung.[333] Mit dem in § 2a S. 1 IWG festgeschriebenen Grundsatz der Weiterverwendung besteht nunmehr ein Anspruch des Antragstellers auf Weiterverwendung zugänglicher Informationen.[334]

Der Weiterverwendungsanspruch ist demnach grundsätzlich abhängig von der Frage der Zulässigkeit des Informationszugangs. Der Weiterverwendung können die Gegenrechte entgegengehalten werden, die auch beim Informationszugang zu beachten waren. Die Zwecke der Weiterverwendung bereitgestellter, nicht geschützter Informationen können von den NIS-Behörden im Übrigen grundsätzlich nicht weiter beeinflusst werden.[335] Das Informations- und Weiterverwendungsfreiheitsrecht enthält weder positive Verwendungsbestimmungen noch etabliert es Verwendungsbeschränkungen. Soweit NIS-bezogene Informationen einmal herausgegeben werden, sind diese grundsätzlich allgemein zu-

---

[331] Erwägungsgrund Erwägungsgründe 7 und 8 der RL 2013/37/EU zur Änderung der RL 2003/98/EG.

[332] Nach *Brummund-Dieckhoff*, Die Abgrenzung von Zugang und Weiterverwendung, in: Dreier/Fischer/van Raay/Spiecker gen. Döhmann (Hrsg.), Informationen der öffentlichen Hand – Zugang und Nutzung, 2016, S. 251 (253) baut das IWG auf die Regelungen zu den Informationszugangsgesetzen auf. Die Anwendbarkeit erfordert nach dieser Auffassung ein subjektiv-öffentliches Recht auf Informationszugang. Nach BVerwG, NVwZ 2016, 1183 (1184) liegt § 1 Abs. 2 Nr. 1 IWG mit Blick auf Erwägungsgrund 8 RL 2013/37/EG eine objektiv-rechtliche Sichtweise zugrunde. Es muss nicht notwendig ein Anspruch auf Zugang zu der betreffenden Information bestehen, um den Anwendungsbereich der Richtlinie zu eröffnen. Es reicht auch aus, wenn die Information im Einklang mit einschlägigen Zugangsregelungen bereits tatsächlich zugänglich gemacht worden ist.

[333] BR-Drs. 358/06, S. 29.

[334] Für eine weite Auslegung bereits *Eifert*, Staatliche Informationsinfrastrukturen – Organisation im gegliederten Verwaltungsraum und private Weiterverwendung der Verwaltungsinformationen, in: Lipowicz/Schneider (Hrsg.), Perspektiven des deutschen, polnischen und europäischen Informationsrechts, 2011, S. 71 (85).

[335] Die öffentliche Stelle kann im Übrigen nach Art. 8 RL 2003/98/EG in Verbindung mit RL 2013/37/EU bzw. § 4 IWG Nutzungsbestimmungen zur Weiterverwendung vorsehen. Siehe *Wiebe*/*Ahnefeld*, CR 2015, 199 (204 ff.). Ferner *Richter*/*Süssner-Job*, Öffentlich- oder zivilrechtliche Ausgestaltung der Informationsordnung – am Beispiel des Zugangs zu und der Weiterverwendung von staatlichen Informationen, in: Dreier/Fischer/van Raay/Spiecker gen. Döhmann (Hrsg.), Informationen der öffentlichen Hand – Zugang und Nutzung, 2016, S. 297 (297 ff.).

gänglich und können zu eigenen Zwecken weiterverarbeitet werden. Der voraussetzungslose Informationszugang erfolgt gerade ohne Begründung. Die zur Verfügung gestellten Informationen können auch ihrerseits veröffentlicht werden. Allenfalls in der Abwägung vor Gewährung des Informationszugangs kann die Behörde berücksichtigen, dass mit der Herausgabe von Informationen nicht nur über eine individuelle, sondern auch über die allgemeine Offenbarung entschieden wird.[336] Für die gewerbliche Weiterverwendung kommt es außerdem nicht etwa darauf an, ob die Behörde Innovationspotenzial auf Märkten sieht. Es ist Sache des Antragsstellers, die Informationen zu veredeln und kommerziell zu verwenden.[337]

3. Maschinenlesbare Bereitstellung von Daten

Auch wenn zugänglich gemachte Informationen im Einzelfall nicht die Qualität aufweisen, die für die Erfüllung des hinter dem Zugangsanspruch verfolgten Zwecks erforderlich ist, kann es zumindest wünschenswert sein, den Zugang zu den Informationen in einer Art und Weise zu erhalten, die es ermöglicht, das Wertschöpfungspotenzial öffentlicher Daten durch Informationstechnik tatsächlich zu realisieren Für den Einsatz von Informationstechnik, etwa in der Interpretation von Informationen, ist es erforderlich, dass die Daten maschinenlesbar sind.

Hinsichtlich der Form des Informationszugangs ergibt sich aus § 7 Abs. 3 S. 1 IFG, dass Auskünfte auch elektronisch erteilt werden können. Auch wenn sich die Vorschrift nicht nur auf Auskünfte, sondern ebenso auf sonstige Arten des Informationszugangs bezieht,[338] ergibt sich aus ihr noch nicht, dass Informationen maschinenlesbar bereitzustellen sind. Die Gesetzesbegründung verweist auf § 3a VwVfG,[339] weshalb darauf geschlossen werden kann, dass es § 7 Abs. 3 S. 1 IFG nicht vorrangig auf die Maschinenlesbarkeit ankommt, sondern darauf, dass auch Zugang zu elektronischen Dokumenten gewährt werden kann.

Anforderungen für das Offenlegen von Daten sind hingegen im E-Government-Gesetz des Bundes (EGovG) vorgesehen. Das Gesetz dient nicht vorrangig der Öffnung der Verwaltung, sondern der Verwaltungsmodernisierung.[340] Nach § 12 Abs. 1 EGovG sind die Behörden des Bundes verpflichtet, grundsätz-

---

[336] *Rossi*, Informationszugangsfreiheit und Verfassungsrecht, 2004, S. 166 ff.

[337] *Eifert*, Staatliche Informationsinfrastrukturen – Organisation im gegliederten Verwaltungsraum und private Weiterverwendung von Verwaltungsinformationen, in: Lipowicz/Schneider (Hrsg.), Perspektiven des deutschen, polnischen und europäischen Informationsrechts, 2011, S. 71 (84 f.).

[338] *Sicko*, in: BeckOK IMR, IFG, 14. Edition 2016, § 7 Rn. 62.

[339] BT-Drs. 15/4493, S. 15.

[340] Dazu *Lederer*, Open Data, 2015, S. 103.

lich maschinenlesbare Formate zu verwenden, wenn Daten über öffentlich zugängliche Netze zur Verfügung gestellt werden, an denen ein Nutzungsinteresse, insbesondere ein Weiterverwendungsinteresse im Sinne des IWG, zu erwarten ist. Ein Format ist nach § 12 Abs. 1 S. 2 EGovG maschinenlesbar, wenn die enthaltenen Daten durch Software automatisch ausgelesen und verarbeitet werden können. Bei der Vorgabe handelt es sich um einen Mindeststandard, Regelungen in anderen Rechtsvorschriften über andere technische Formate gehen nach § 12 Abs. 3 EGovG vor, soweit sie die Maschinenlesbarkeit gewährleisten.

Die Gewährleistung der Maschinenlesbarkeit ist eine Verfahrens- bzw. Organisationsvorgabe.[341] Auch durch § 12 Abs. 1 S. 1 EGovG wird keine Veröffentlichungspflicht begründet. Sinn und Zweck der Vorschrift ist gleichwohl die möglichst weitreichende Weiterverwendung frei zugänglicher amtlicher Informationen.[342] Die allgemeinen und fachspezifischen Schranken für die Veröffentlichung von Daten bleiben daher gemäß § 12 Abs. 5 EGovG unberührt.[343]

Mit § 12 EGovG besteht damit für NIS-Behörden eine Bestimmung, aus der sich ergibt, dass die veröffentlichen Daten maschinenlesbar bereitzustellen sind. Sie bezieht sich allerdings nicht auf Informationen, die auf Grundlage eines Informationszugangsanspruchs bereitgestellt werden, sondern nur auf solche, die freiwillig im Internet veröffentlicht werden. Als praktischer Anwendungsfall kommt hier in Betracht, zu veröffentlichende Sicherheitsvorfälle in maschinenlesbarem Format bereitzustellen.[344]

Zu den Modalitäten der Bereitstellung der Informationen enthält daneben das Weiterverwendungsrecht Bestimmungen. Art. 5 Abs. 1 RL 2013/37/EU schreibt fest, dass Informationen in allen verfügbaren (§ 3 Abs. 2 S. 1 IWG: „angefragten") Formaten und Sprachen, in denen sie bei der öffentlichen Stelle vorliegen, zur Weiterverwendung zur Verfügung zu stellen sind. Soweit möglich und sinnvoll, sind sie im offenen und maschinenlesbaren Format zusammen mit den zugehörigen Metadaten zur Verfügung zu stellen. § 2 Nr. 5 und 6 IWG definiert genauer, was unter offenem Format und maschinenlesbarem Standard zu verstehen ist. Die Bestimmung der Maschinenlesbarkeit entspricht der in § 12 Abs. 1 EGovG.

---

341 *Habammer*/*Denkhaus*, MMR 2013, 358 (360).

342 *Schoch*, IFG, 2. Aufl. 2016, Einl. Rn. 321.

343 *Roßnagel*, NJW 2013, 2710 (2713).

344 Nach Erwägungsgrund 40 NIS-RL wird außerdem das Sekretariat des CSIRTs-Netzwerks aufgefordert, eine Webseite zu unterhalten, auf der allgemeine Informationen über größere in der Union aufgetretene Sicherheitsvorfälle mit einem besonderen Schwerpunkt auf den Interessen und dem Bedarf von Unternehmen der allgemeinen Öffentlichkeit zur Verfügung gestellt werden.

Die Verpflichtung der Bereitstellung der Informationen ist aber anders als im Anwendungsbereich von § 12 Abs. 1 EGovG auf das Zumutbare beschränkt. Nach § 3 Abs. 2 IWG sind die Informationen entsprechend bereitzustellen, wenn damit für die öffentliche Stelle kein unverhältnismäßiger Aufwand verbunden ist. Im Übrigen stellt Art. 5 Abs. 2 RL 2013/37/EU klar, dass eine ansonsten nicht gebotene fortlaufende Erstellung oder Speicherung von Dokumenten allein zum Zwecke der Weiterverwendung nicht gefordert ist.

Im Ergebnis ist damit rechtlich indiziert, dass zugängliche Informationen maschinenlesbar bereitzustellen sind. Nach § 12 Abs. 1 EGovG gilt dies zwar nur für freiwillig von der Behörde im Internet veröffentlichte Informationen. Aus § 3 Abs. 2 S. 1 IWG ergibt sich dies aber grundsätzlich für weiterverwendbare Informationen im Rahmen des der Behörde zumutbaren Aufwands.

D. Zwischenergebnis

Die Untersuchung der staatlichen Distribution von Informationen mit einem Bezug zur Internetsicherheit wird im Ausgangspunkt durch den Befund ausgelöst, dass die öffentlichen Stellen durch die zahlreichen Informationserhebungsinstrumente über eine wachsende Datenbasis verfügen und die Weitergabe der vorhandenen Informationen einen Beitrag zur Internetsicherheit leisten kann.

Auch für die Sicherheitsgewährleistung kann das Konzept der Offenheit des Staates (Open Government Data) herangezogen werden, das nicht lediglich ein demokratietheoretisches Wohlwollen ausdrückt, sondern den grundrechtlich verankerten Schutzauftrag der Informationsvorsorge im Vorfeld rechtlicher Mechanismen zur Gefahrenabwehr zu erfüllen bezweckt und das Wertschöpfungspotenzial frei verwendbarer Informationen, das insofern auch bei sicherheitsbezogenen Informationen besteht, berücksichtigt. Die Betrachtung des Transparenzgedankens in der Debatte um freie Software oder in der sog. Kryptokontroverse macht deutlich, dass das allgemeine Zurückhalten von sicherheitsbezogenen Informationen (*security through obscurity*) nicht von vorneherein eine höhere Sicherheit verspricht und insofern Informationsdistribution einen Beitrag zur Sicherheitsgewährleistung zu leisten vermag (*security by transparency*).

Ein sicherheitsspezifischer Mehrwert kann dabei zum einen durch aktives staatliches Informationshandeln, das auf bestimmte Verhaltensreaktionen beim Adressaten zielt, erreicht werden, und zum anderen durch reaktives Informationshandeln in Form des antragsbasierten Zugangs zu den von NIS-Behörden generierten Informationen und deren Weiterverwendung durch Private.

Aktives staatliches Informationshandeln setzt im grundrechtssensiblen Bereich grundsätzlich eine Rechtsgrundlage voraus. Das BSI als zentrale NIS-Be-

hörde verfügt indes über keine allgemeine Rechtsgrundlage, die grundrechtssensible Öffentlichkeitsinformationen erlaubt.

Die öffentlichkeitsbezogene Information kann auf Grundlage verschiedener Regelungen erfolgen, die entsprechend der Zielrichtung des Informationshandelns unterschieden werden können.

Der Wissensvermittlung durch Aufklärung der Öffentlichkeit über Sicherheitsprobleme dienen die Berichte des BSI und der Bundesnetzagentur. Soweit die Berichte der Datenschutzbehörden die Datensicherheit betreffen, dienen auch sie der Aufklärung. Die Berichtspflichten sind aufgrund ihrer kalendarischen Zyklen zwar nicht geeignet, proaktiv Einzelfallinformationen über aktuelle Sicherheitslagen zu veröffentlichen, gleichwohl kann durch Berichte für Risiken und Gefahren sensibilisiert werden. Die Datenschutzbehörden können sich zu diesem Zweck von sich aus zu jeder Frage mit einer Stellungnahme an die Öffentlichkeit richten.

Die Veröffentlichung von Informationen über konkrete Sicherheitsvorfälle ist für die Herstellung des Problembewusstseins von besonderer Bedeutung. Für Sicherheitsvorfälle bei Telekommunikationsnetzbetreibern und -diensteanbietern besteht eine Informationsbefugnis der Bundesnetzagentur, mit Blick auf Anbieter digitaler Dienste und Betreiber kritischer Infrastrukturen besteht seitens des Gesetzgebers Umsetzungsbedarf. Die mitgliedstaatlichen NIS-Behörden müssen die Öffentlichkeit über einzelne Sicherheitsvorfälle in digitalen Diensten oder kritischen Infrastrukturen zur Sensibilisierung, Verhütung oder Bewältigung von Sicherheitsvorfällen nach Anhörung der Anbieter und Betreiber unterrichten dürfen (Art. 14 Abs. 6 bzw. Art. 16 Abs. 7 NIS-Richtlinie). Die bestehenden Rechtsgrundlagen bilden diese unionsrechtliche Erlaubnis nicht ab. Perspektivisch erscheint es sinnvoll, die Informationen über Sicherheitsvorfälle aus allen Mitgliedstaaten auf europäischer Ebene zu aggregieren und zentral zu publizieren. Bei Sicherheitsvorfällen, die den Schutz personenbezogener Daten betreffen, erfolgt die Information nicht durch die Behörde, sondern grundsätzlich durch die datenschutzrechtlich Verantwortlichen. Die Information der Öffentlichkeit dient hier im Übrigen vorrangig dazu, den Betroffenen zu erreichen, wenn eine direkte Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre. Als Defizit zu bewerten ist, dass dieser Modus der Publikumsinformation für Telekommunikationsunternehmen von vornherein nicht besteht.

Eher für den Markt von IT-Sicherheitsprodukten und Dienstleistungen von Bedeutung sind die Veröffentlichung der Sicherheitskataloge für Telekommunikationsunternehmen und der Erkenntnisse aus Untersuchen von IT-Produkten und -systemen. Für die Anbieter von Sicherheitstechnik im Telekommunikationsbereich wird eine gewisse Transparenz hinsichtlich der Sicherheitserforder-

nisse geschaffen. Über die Sicherheit von auf dem Markt bereitgestellter oder zur Bereitstellung vorgesehener Produkte können Hersteller, Vertreiber oder Anwender informiert werden. Die Veröffentlichung von Produktinformationen ist zwar nicht unionsrechtlich induziert, kann sich aber an ein europäisches Publikum richten.

Von besonderer Relevanz ist die Warn- und Empfehlungsbefugnis des BSI. Am Beispiel der Warnung vor Sicherheitslücken kann die Janusköpfigkeit von sicherheitsrelevanten Informationen verdeutlicht werden. Die Veröffentlichung von Informationen über Sicherheitslücken bewegt sich zwischen dem Ideal der Publizität und den Interessen der weiteren Sicherheitsbehörden. Sie dient grundsätzlich dazu, dass Unternehmen und Bürger rechtzeitig eigene Schutzmaßnahmen ergreifen. Gleichwohl können so bekannt gewordene Schwachstellen auch durch Angreifer ausgenutzt werden. Überdies können Sicherheitsbehörden ein Interesse daran haben, dass sog. Zero-Day-Exploits nicht bekannt werden, damit eigene Operationen nicht gefährdet werden. Als ermessensleitende Strategie bietet sich demnach die verantwortungsbewusste Veröffentlichung (*Responsible Disclosure*) an, nach der Sicherheitslücken nicht pauschal mit einer kurzfristigen Notifizierung der Unternehmen veröffentlich werden, sondern in jedem Einzelfall geprüft wird, mit welchen Gefahren eine Veröffentlichung verbunden ist. Auf Grundlage von § 7 BSIG lässt sich diese Strategie umsetzen, da das Ermessen des BSI nicht gebunden ist. Im Falle einer Veröffentlichung oder Empfehlung haben die Behörden der möglichen Gefahr vorzubeugen, dass das Informationshandeln zu eigendynamischen Verstärkereffekten führt und an die Stelle von Aufklärung ein edukatorisches oder durch bestimmte Produktempfehlungen ein wirtschaftslenkendes Staatshandeln tritt, welches mit unabsehbaren Übertragungseffekten (Spill-over-Effekten) verbunden ist. Zu fordern ist hier insbesondere die Berücksichtigung gesicherter verhaltenswissenschaftlicher Erkenntnisse.

Von besonderer praktischer Bedeutung sind die individualbezogenen Informationen. Die Befugnis, Informationen gezielt an die Betreiber kritischer Infrastrukturen weiterzugeben, schließt den Kreislauf gemeldeter Informationen und trägt so zur Rechtfertigung von Meldepflichten bei. Die über die Meldepflichten generierten Daten werden mit Betreibern kritischer Infrastrukturen, die nicht Urheber der Meldung sind, geteilt. Auf diese Weise können Betreiber aus dem System der Meldepflichten für sich einen konkreten Nutzen ziehen, wodurch insgesamt ein stärkerer Anreiz zur Erfüllung der Meldepflichten geschaffen wird. Das BSI bedient sich zur Bereitstellung individualbezogener Information sinnvoller informeller Plattformen. Hinsichtlich des die NIS-Behörden ergänzenden Informationshandelns der Datenschutzbehörden ist die Benachrichtigung des Betroffenen von einer Datenschutzverletzung nicht vorgesehen. Eine

bestehende Regelung dazu wie im deutschen Recht hätte aber Bestand. Darüber hinaus ist die Datenschutzbehörde zu Sensibilisierungs- und Beratungsleistungen verpflichtet, die auch Fragen der Datensicherheit betreffen können. Die Praktikabilität dieser Pflichten ist aber bereits angesichts der behördlichen Ressourcen zweifelhaft.

Das reaktive Informationshandeln ist die zweite Säule der Informationsdistribution. Der Informationszugangsanspruch ist im europäischen Primärrecht stärker als im Grundgesetz angelegt. Mangels einer harmonisierenden, bereichsspezifischen Unionsregelung des Informationszugangs, ist hinsichtlich des Zugangs zu europäischen und nationalen NIS-Stellen zu unterscheiden. Auf europäischer Ebene besteht lediglich für die ENISA eine Zugangsregelung, die auf die Transparenz-Verordnung verweist. Eine Grundlage für den Zugang zu Informationen des CSIRTs-Netzwerk oder der Kooperationsgruppe besteht nicht. Bedeutung und Nutzen der Auskunftsverlangen hinsichtlich der beim BSI und der Bundesnetzagentur vorhandenen Informationen über die Sicherheit kritischer Infrastrukturen bleiben allerdings aufgrund der nur unzureichend ausgestalteten Pauschalabwägung des Gesetzgebers begrenzt, da die Betreiberinteressen grundsätzlich vorgehen, selbst dann, wenn das Interesse des Antragstellers gewichtig und das einer Auskunft entgegenstehende Interesse nur gering ist. Der Zugang zu Akten in diesen Angelegenheiten ist gänzlich ausgeschlossen. Damit werden Anfragen gar nicht erst geprüft, obwohl sie für den Anfragenden oder die Öffentlichkeit von grundsätzlicher und hoher Bedeutung sein können und im allgemeinen Informationszugangsrecht ein differenziertes System an Ausnahmetatbeständen besteht, das eine einzelfallgerechte Entscheidung ermöglicht. Außerhalb der Ansprüche im Zusammenhang mit kritischen Infrastrukturen zeigt die Praxis aber, dass Zugangsanfragen häufig entsprochen wird.

Sind NIS-Informationen zugänglich, können sie grundsätzlich weiterverwendet werden, durchaus auch zu kommerziellen Zwecken. Die freie Weiterverwendung leistet insofern einen Beitrag zur Gewährleistung der Internetsicherheit, die durch Rekombination und Veredelung von Informationen zur Weiterentwicklung bestehender und Entwicklung innovativer und besserer Sicherheitsprodukte und Dienstleistungen führen kann.

Im Kern besteht damit spätestens seit den Novellierungen durch das IT-Sicherheitsgesetz ein Regelungsbestand, der als IT-Informationsrecht bezeichnet werden kann. Die Regeln zur Distribution staatlichen Wissens ergänzen die Vorgaben der Informationspflichten, die Unternehmen vor allem bei Daten- und Sicherheitsverletzungen treffen und bei denen die Informationsweitergabe ebenfalls zwar administrative Aufgabe ist, aufgrund der Nähe zu den Informationen aber den Privaten überlassen wird (vgl. § 109a Abs. 4 TKG). Das IT-In-

formationsrecht schafft bei den Privaten die Voraussetzungen zum Selbstschutz und ist ein Faktor neuer Wertschöpfung in der (Weiter-)Entwicklung von IT-Sicherheitsprodukten.

§ 6 Zusammenfassende Bewertung und Fazit

Die Gesamtbetrachtung ergibt zusammengefasst folgendes Ergebnis:

A. Beitrag des Informationsverwaltungsrechts zur Netz- und Informationssicherheit

Ausgangspunkt der Untersuchung war die Überlegung, dass sich das verfassungsrechtliche Ziel der Union, den Bürgerinnen und Bürgern einen Raum der Freiheit, der Sicherheit und des Rechts ohne Binnengrenzen zu bieten, mit Blick auf das Internet als Herausforderung darstellt. Nicht zuletzt aufgrund der technischen und logischen Komplexität sind Sicherheitsprobleme immanent. Eine absolute Sicherheit kann nicht gewährleistet werden. Die Gewährleistung der Sicherheit von Netz- und Informationssystemen ist daher als Risikomanagement zu begreifen. Über die Risiken und Gefahren besteht allerdings eine epistemische Unsicherheit und damit ein Wissensproblem. Das Wissen über die Sicherheit und die Sicherheitsprobleme ist auf verschiedene private Akteure, insbesondere die Infrastrukturbetreiber und Diensteanbieter, dezentral verstreut. Die Gewährleistung der Sicherheit durch technische Internetregulierung erscheint von vorneherein wegen der prinzipiell globalen Natur des Internets und der damit verbundenen tatsächlichen wie rechtlichen Begrenzungen nicht als eine aussichtsreiche Regulierungsstrategie. So wie das Internet keine *terra nullius* oder ein herrschaftsfreier Raum ist, ist das Recht in der Sicherheitsgewährleistung nicht machtlos.

Da Informationen über die Sicherheit (z. B. die Kenntnis über eine Sicherheitslücke, einen Sicherheitsvorfall oder über neue Angriffsarten) eine zentrale Ressource in der Sicherheitsgewährleistung sind, bietet sich als Ansatz der Sicherheitsgewährleistung auf europäischer wie nationaler Ebene Informationsverwaltungsrecht an. Es handelt sich dabei um einen Aspekt des Verwaltungsrechts, der auf Informationen als operative Basis der administrativen Entscheidungsfindung und Gegenstand des Verwaltungshandelns verweist.

Mit einem informationsverwaltungsrechtlichen Fokus auf das Paradigma Information und Wissen lassen sich die auf Erkenntnisgewinnung (Generierung),

informationelle Zusammenarbeit in der Union (Transfer) und Partizipation an den generierten Informationen und dem gewonnenen Wissen (Distribution) bezogenen rechtlichen Instrumentarien herausarbeiten.

I. Erkennung von Gefahren und systemischen Risiken

Die Informationsgenerierung durch Informationsbeibringungspflichten und Informationsbefugnisse erlaubt es der NIS-Administrative, ein Lagebild über die Sicherheit in wesentlichen Internetinfrastrukturen und -diensten zu erstellen und entscheidungsrelevantes Wissen zu produzieren. Die Informationsbasis bildet die Voraussetzung für die Wahrnehmung staatlicher Schutzpflichten und die Erfüllung der Gewährleistungsverantwortung. Die zentralen Informations- und Wissensakteure in der Generierung von Informationen über die Netz- und Informationssicherheit sind die mitgliedstaatlichen NIS-Behörden und auf europäischer Ebene die Europäische Agentur für Netz- und Informationssicherheit. In Deutschland kommt dem Bundesamt für Sicherheit in der Informationstechnik als zentrale Stelle für die Sicherheit in der Informationstechnik kritischer Infrastrukturen die zentrale Rolle in der Informationsgenerierung zu. Daneben sind die Bundesnetzagentur und die Nachrichtendienste wichtige Akteure im Bereich der Netz- und Informationssicherheit.

Die rechtlichen Instrumente zur Informationsgenerierung sind weitgehend unionsrechtlich harmonisiert. Trotz ihrer hohen Bedeutung für die Internetsicherheit sind Hard- und Softwarehersteller von Informationsbeibringungspflichten nicht erfasst. Aus epistemischer Sicht scheint deren Einbeziehung in den Pflichtenkanon für eine ganzheitliche Sicherheitsbetrachtung geboten. Ebenso sollte hinsichtlich der noch nicht abschließend beantworteten Frage nach der Regulierung von Over-the-Top-Telekommunikationsdiensten berücksichtigt werden, dass die Anwendbarkeit des Telekommunikationsrechts der Schutzpflicht zur Informationsgewinnung und der verfassungsrechtlichen Gewährleistungsverantwortung Rechnung tragen würde.

Die den NIS-Behörden beizubringenden Sicherheitsnachweise, die Meldepflichten, die Befugnis zur Untersuchung von IT-Produkten und die nachrichtendienstliche Kompetenz zur Untersuchung der Internetdatenverkehre sind insgesamt geeignet, systemische Risiken und Gefahren für die Internetsicherheit zu erkennen. Soweit die NIS-Verwaltung in der Wissensgenerierung auf verwaltungsexterne Expertise zurückgreift, ist in der Verwaltung ein spezifisches Meta-Wissen erforderlich, um außeradministratives Wissen erfolgreich zu übernehmen.

Weder gesetzlich ersichtlich noch durch die NIS-Behörden im Wege der weiteren Durchführung besonders konkretisiert ist die technisch-organisatorische

Rahmenarchitektur der Informationsgenerierungsprozesse. Die Durchführung der Meldepflicht aus § 109a TKG bei Verletzungen der Datensicherheit ist hier paradigmatisch. Die Informationen werden lediglich durch das Ausfüllen einer editierbaren PDF-Datei per E-Mail gemeldet. Vor dem Hintergrund des mit der Informationsgewinnung verfolgten Zwecks der effektiven Produktion entscheidungsrelevanten Wissens und der relevanten ökonomischen Dimension erscheint die Informationsgenerierung im Bereich der Netz- und Informationssicherheit insgesamt ausbaubedürftig. Die gemeldeten Informationen werden durch die fehlende Zentralisierung meist isoliert voneinander gehandhabt und bearbeitet. Der dadurch bei den meldepflichtigen Unternehmen und bei den zuständigen NIS-Behörden entstehende Mehraufwand führt zu einem Fehlerrisiko bei der Informationsverwertung. In Ermangelung geeigneter (automatisierter) Informationssysteme mit hohem Routinegrad im Umgang mit Melde- und Informationsflüssen müssen die Informationspflichten manuell erfüllt werden. Die dadurch entstehende Erhöhung des Verwaltungsaufwands bindet zusammen mit der Einhaltung sonstiger Compliance-Vorgaben in den verpflichteten Unternehmen Ressourcen, was Innovation und Agilität verhindert. Da Angreifer ohne Beachtung rechtlicher Vorgaben agieren und nur die real existierenden Schwachstellen in den Fokus nehmen, scheint vor diesem Hintergrund die Entwicklung und Realisierung von Verfahren und Standards für eine vernetzte und übergreifende Architektur geboten, die den sicheren Datenaustausch zwischen den meldepflichtigen Unternehmen und der Verwaltung effektiviert. Die Untersuchung der durch den Schutz personenbezogener wie unternehmensbezogener Daten gezogenen Grenzen zeigt, dass dem Aufbau einer serviceorientierten Architektur (SOA)[1] grundsätzlich keine rechtlich durchgreifenden Bedenken entgegenstehen. Der im Nationalen Cyber-Abwehrzentrum verfolgte Ansatz, Informationen verschiedener Sicherheitsbehörden unter einem Dach zu fusionieren, weist hinsichtlich der Erkenntnisgewinnung in die richtige Richtung.

II. Europäisierte Informationskooperation auf Vertrauensbasis

Die informationelle Zusammenarbeit auf nationaler, aber insbesondere auch auf europäischer Ebene ist für die Sicherheitsgewährleistung von besonderer Bedeutung. Aufgrund der NIS-Richtlinie sind auf europäischer Ebene die Voraussetzungen sowohl für eine strategische als auch für die operative Kooperation geschaffen. Die verfahrensrechtliche Ausgestaltung deckt die relevanten Berei-

[1] Unter einer serviceorientierten Architektur wird in der Informationstechnik ein Architekturmuster aus dem Bereich der verteilten Systeme verstanden, dessen Funktion es ist, Dienste und Einzelaufgaben zu koordinieren und so Leistungen zu höheren Diensten zusammenzufassen und anderen Organisationsabteilungen zur Verfügung zu stellen.

che des Risikomanagements im Bereich der Sicherheitsgewährleistung ab. Sie ist darauf angelegt, Informationen und Wissen in expliziter und impliziter Form zur Prävention und Detektion von Sicherheitsrisiken und -vorfällen und zur Reaktion auf dieselben auszutauschen.

Der zum großen Teil reflexiv organisierte Wissensaustausch trägt der Erkenntnis Rechnung, dass die bloße Übermittlung einer Nachricht im Sinne des *information sharing* noch keine Zusammenarbeit im bezweckten Sinne darstellt. Grenzüberschreitende Übungen der Reaktion auf Sicherheitsvorfälle beispielsweise erlauben den Austausch impliziten Wissens und die erforderliche Harmonisierung einer gemeinsamen Kontextualisierung von Informationen. Die durch horizontale und vertikale Informationsbeziehungen möglichen gegenseitigen Beobachtungen lassen die europäische NIS-Kooperation insgesamt als Lernverbund erscheinen, der zum Kapazitätenaufbau beiträgt und die Unzulänglichkeit der Mitgliedstaaten zu einem nicht unerheblichen Teil kompensiert. Insgesamt sind die Verfahrens- und Organisationsstrukturen geeignet, zur Bildung einer europäischen Wissensgemeinschaft (*epistemic community*) beizutragen und jene Beschränkungen partiell aufzuheben, die aufgrund der begrenzten Rationalität (*bounded rationality*) entstehen und Individuen wie Organisationen, d. h. hier die mitgliedstaatlichen NIS-Akteure, auf eine selektive Berücksichtigung vorhandener Informationen festlegen. Die zentrale Leistung der informationsverwaltungsrechtlichen Strukturen besteht darin, den Aufbau notwendigen Vertrauens unter den europäischen NIS-Akteuren durch die Schaffung einer erwartungsstabilisierenden Informationsordnung zu fördern.

Eine effektive europäische Systemaufsicht ermöglicht das europäische NIS-Verwaltungsrecht indes nicht. Eine aktive und zentralisierte Aggregation der in den Mitgliedstaaten gesammelten Informationen dergestalt, dass ähnlich dem nationalen Ansatz ein europäisches Lagebild über die Sicherheit geschaffen wird, ist rechtlich nicht vorgesehen. Das europäische Ganze im Bereich der Netz- und Informationssicherheit ist insgesamt noch nicht mehr als die Summe seiner mitgliedstaatlichen Teile. Solange eine effiziente Agentur für europäische Probleme in der Gewährleistung der Netz- und Informationssicherheit, die Informationen auf einer höheren Ebene verwerten kann, nicht etabliert ist, mag die Sorge um das Ganze begründet bleiben. Die in der NIS-Richtlinie angelegte Struktur der NIS-Kooperation bewirkt jedoch, dass aus dem gemeinsamen Handeln der Mitgliedstaaten Synergie statt Paralyse entstehen kann. Dass perspektivisch der Aufbau eines dichter integrierten NIS-Informationssystems außerhalb der binnenmarktrechtlichen Harmonisierungskompetenz unter dem Vertrag von Lissabon nicht ausgeschlossen ist, macht Art. 83 Abs. 2 lit. a AEUV deutlich, der es dem Unionsgesetzgeber erlaubt, das Einholen, Speichern, Verarbeiten, Analysieren und Austauschen sachdienlicher Informationen zu regeln,

wobei der dort genannte Zweck der polizeilichen Zusammenarbeit weit verstanden werden kann und informationsverwaltungsrechtliche Regelungen im Vorfeld polizeilicher Gefahren nicht von vorneherein ausschließt. Die ENISA, die im Rahmen der strategischen Kooperation eine im Wesentlichen unterstützende Funktion einnimmt, könnte in einer stärker operativ ausgerichteten Zusammenarbeit die Rolle als zentrale Stelle für die Netz- und Informationssicherheit in der Union einnehmen.

Die operative Bewältigung von grenzüberschreitenden Sicherheitsvorfällen ist daher maßgeblich auf bilaterale horizontale Informationsbeziehungen angewiesen. Der Austausch sicherheitskritischer Informationen beruht zu einem maßgeblichen Teil auf Freiwilligkeit. Eine Symmetrie von Problemen und Lösungen besteht im Ergebnis auf europäischer Ebene nicht.

Mit der Internationalisierung der Technologie nimmt im europäischen Kontext die Bedeutung des Informationsaustausches weiter zu. Das Schaffen vertrauensfördernder Voraussetzungen sollte perspektivisch den Wechsel vom Prinzip, einen Kommunikationspartner nur bei Bedarf in Kenntnis zu setzen (Need-to-know-Prinzip), zum Informationsaustauschparadigma (Need-to-share-Prinzip) bewirken. Gerade für IT-Sicherheitslücken, die nicht allen an der Informationskooperation Teilnehmenden bekannt sind, wäre eine Informationspflicht erforderlich, soweit das Wissen um die Schwachstelle diese beheben könnte. Jede nicht im europäischen Kooperationsnetz geteilte Information, derer es aber in anderen Mitgliedstaaten bedarf, führt zu einer ineffektiven Ressourcennutzung, weil sie in den Mitgliedstaaten ggf. parallel gewonnen und ausgewertet wird. Damit einher geht die Gefahr, dass bei nicht koordinierten Reaktionen, etwa bei Frühwarnungen, die Gefahren abweichend eingeschätzt werden. Darüber hinaus kann es bei unterschiedlichen Sicherheitsniveaus in den Mitgliedstaaten zu nicht intendierten Wettbewerbsverzerrungen im Binnenmarkt kommen.

Eine Herausforderung im europäischen Wissensmanagement wird ferner darin liegen, neben dem Austausch von Datenbeständen den Austausch von implizitem Wissen, d. h. von solchem Wissen, das lokal besteht und personal vermittelt wird und nicht einfach artikuliert werden kann, weiterzuentwickeln. Eine Verdichtung der Kooperation im Bereich der Netz- und Informationssicherheit, etwa in Form eines kontinuierlichen Informationsaustausches in Echtzeit, ist auf Grundlage des Vertrags von Lissabon grundsätzlich möglich. Die effektive Durchführung des Unionsrechts ist von gemeinsamem Interesse. Der für die „Verbesserung der Fähigkeiten der Verwaltung“ in Art. 197 Abs. 2 AEUV ausdrücklich vorgesehene Austausch von Informationen und von Beamten kann dafür als programmatisch verstanden werden.

III. Zugang zu und freie Weiterverwendung von generierten Informationen und produziertem Wissen als Teil der Sicherheitsgewährleistung

Die Distribution von Informationen ist die Reaktion auf die gestiegene gesellschaftliche Relevanz von Wissen. Der Beitrag des Informationsverwaltungsrechts liegt hier nicht in der Ermöglichung demokratischer Teilhabe, sondern in der Gewährleistung der Internetsicherheit durch Bewusstseinsbildung (*awareness raising*) bei Nutzern und Anwendern hinsichtlich allgemeiner Sicherheitsprobleme durch aktive Information der Öffentlichkeit oder betroffener Kreise. Soweit es die Veröffentlichung von konkreten Sicherheitsvorfällen ermöglicht, wird damit ein zentrales Problem der Gewährleistung der Netz- und Informationssicherheit adressiert. Die Öffentlichkeit kann durch die Publikation von Sicherheitsvorfällen überhaupt erst in die Lage versetzt werden, sich ein näher an der Wirklichkeit ausgerichtetes Bild von den bestehenden Sicherheitsproblemen zu machen und politischen Handlungsbedarf zu identifizieren.

An der Handlungsform der Warnung lässt sich das grundlegende Problem der Veröffentlichung sicherheitskritischer Informationen darstellen. Der Informationsdistribution liegt aufgrund der Doppelnatur von sicherheitsbezogenen Informationen ein Spannungsverhältnis zwischen Transparenz und Geheimhaltung zugrunde. Die Warnung vor Sicherheitslücken etwa kann dem Schutz vor Cybergefahren dienen, zugleich aber den Missbrauch durch Angreifer begünstigen. Offenheit als informationsverwaltungsrechtliches Mittel zur Gewährleistung der Internetsicherheit ist zwar nicht von vorneherein ausgeschlossen und nicht unsicherer als der Ansatz pauschaler behördlicher Geheimhaltung (s*ecurity through obscurity*). Geheimhaltung ist jedoch dort sinnvoll, wo die Distribution im Sinne einer Publikumsinformation kontraproduktiv wäre. Die Responsible Disclosure als die verantwortungsvolle Veröffentlichung sicherheitskritischer Information in Form von Vorabinformationen der durch die Veröffentlichung unmittelbar Betroffenen steht für eine angemessene Strategie im Umgang mit der Janusköpfigkeit sicherheitskritischer Informationen.

Ein behutsames Informationshandeln ist auch beim Ausspruch von Empfehlungen einzufordern. Mit staatlicher Autorität ausgesprochene Empfehlungen können wirksame Steuerungseffekte hinsichtlich des Verbraucherverhaltens in Bezug auf IT-Produkte bewirken. Mit ihnen können aber auch nicht intendierte Spill-over-Effekte bewirkt werden. Staatliches Informationshandeln muss daher vor allem risikobezogene Informationen möglichst unter Berücksichtigung gesicherter verhaltenswissenschaftlicher Erkenntnisse darstellen.

Der Zugang zum Informationsbestand der Verwaltung ermöglicht grundsätzlich die Partizipation nicht am Verfahren beteiligter Interessierter. Da die Ver-

waltung Informationen ohne Richtigkeitsgewähr und Aufbereitungspflicht weitergeben kann, kommt ihr hier die Rolle eines Informationsintermediärs zu. Für die europäische Ebene ist hier jedoch für einen Zugang zu Informationen zu allen NIS-Stellen auf den Gesetzgebungsauftrag des Art. 15 Abs. 3 AEUV zu verweisen. Für eine nicht nur von der ENISA ausgehende Informationsdistribution, für die eine Zugangsregelung besteht, ist eine sekundärrechtliche Ausgestaltung der Informationsfreiheit erforderlich, die den Zugangsanspruch entsprechend dem primärrechtlich vorgesehenen Kreis der Verpflichteten auf sämtliche NIS-Stellen erweitert. Aufgrund der weitreichenden besonderen und allgemeinen Reichweitenverkürzungen und Ausnahmen vom Zugang zu NIS-Informationen bleibt das kognitive und wirtschaftliche Potenzial der Informationsdistribution solange verkürzt, wie sich nicht die Einsicht Bahn gebrochen hat, dass die Öffnung der Verwaltung und der Zugang zu sicherheitsbezogenen Informationen Teil der Problemlösung in der Gewährleistung der Internetsicherheit ist.

Um die eruptive Kraft, die zugänglichen und wirtschaftlich weiterverwendbaren NIS-Informationen innewohnt, entfalten zu können, sind Anforderungen an die interne Informationsorganisation der NIS-Verwaltung, auch wenn sie nicht unmittelbar rechtlich vorgegeben wird, zu stellen. Die verwaltungsinterne Perspektive auf Vorgänge (in Akten) muss erweitert werden um die ergebnisorientierte Perspektive, dass Informationen Gegenstand des verwaltungsexternen Zugriffs sein können und sollten. Die strukturierten, formalisierten und informalen Informations- und Wissensbestände sollten von vorneherein inhaltlich so aufbereitet werden, dass sie leicht, rasch und in für maschinelle Verarbeitung geeigneter Form zugänglich gemacht und technisch-organisatorische Maßnahmen zum Schutz von Gegenrechten ergriffen werden können.

B. Intelligente Datenverarbeitung und Operationalisierung von Nichtwissen

Die untersuchten informationellen und kognitiven Regelungsstrukturen der Administrative bilden bei einer Gesamtbetrachtung eine Informationsordnung, die eine Risikoerkennung und Wissensproduktion prinzipiell ermöglicht und die daher einen Beitrag zur Bewältigung der Komplexitäts- und Wissensprobleme, welche der Gewährleistung der Sicherheit von Netz- und Informationssystemen inhärent sind, leisten kann. Die rechtlichen Instrumente zur Wissensgenerierung, wie etwa die Meldepflichten, dienen dazu, aus Sicherheitsvorfällen, die in der Vergangenheit liegen, zu lernen, um zukünftig auf ähnlich gelagerte Angriffe und sonstige Sicherheitsvorfälle vorbereitet zu sein und diesen mit weiter-

entwickelten Abwehrstrategien wirksam zu begegnen. Daraus folgt für das Informationsverwaltungsrechts der NIS-Verwaltung die besondere Aufgabe, neuartige Informationsquellen (z. B. Sensorik in den Netzen), technische Weiterentwicklungen sowie Datenverarbeitungs- und Kommunikationsmedien zu rezipieren. Konkret bedeutet dies vor allem den Übergang zur intelligenten Datenverarbeitung, die nicht lediglich durch die quantitative Steigerung der verarbeiteten Datenmenge, sondern durch ein spezifisches Rückkopplungsverhältnis von Technik und Inhalt charakterisiert ist. „Es ist nicht mehr wie in der Vergangenheit zu unterstellen, dass das technische System invariant ist und seine Form der Verwaltung der Inhalte aufprägt, vielmehr wird die Form sehr viel stärker durchlässig für die von den Inhalten vorgegebenen Bedingungen."[2]

Zuletzt ist neben der Produktion, dem Austausch und der Weitergabe von Wissen eine Operationalisierung von Nichtwissen und Ungewissheit erforderlich. Die Produktion von Wissen bringt als Kehrseite immer auch Unwissen und mithin Ungewissheit und folglich Unsicherheit mit sich.[3] Ungewissheit muss als Gewissheit berücksichtigt werden, die nicht durch zusätzliches Wissen aufgehoben wird.[4] Mit dem Nichtwissen ist als bekannte Variable zu operieren.[5] Analysen aus beobachteten Daten dürfen daher zum einen nicht überbewertet und das Auftreten kontingenter Imponderabilien darf zum anderen nicht unterschätzt werden. Auch mit ausdifferenzierten informationsverwaltungsrechtlichen Instrumenten bedarf es neben der erforderlichen Risikoerkenntnis und Wissensproduktion einer Strategie für den Umgang mit der Gewissheit von Ungewissheit und für Handeln unter Bedingungen des Nichtwissens.[6] „Es sollte aber

---

[2] *Ladeur*, Die Kommunikationsinfrastruktur der Verwaltung, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band II, 2. Aufl. 2012, § 21 Rn. 89.

[3] Pointiert *Luhmann*, Soziologie des Risikos, 1991, S. 37: „Je mehr man weiß, desto mehr weiß man, was man nicht weiß, und desto eher bildet sich ein Risikobewußtsein aus."

[4] *Augsberg*, Informationsverwaltungsrecht, 2014, S. 237 ff.; *Hofmann-Riem*, Verwaltungsrecht in der Informationsgesellschaft – Einleitende Problemskizze, in: Hoffmann-Riem/Schmidt-Aßmann (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, 2000, S. 9 (13).

[5] Dass ein vollständiger Informationsstand über Sachverhalte (z. B. Marktsituation) nicht erreicht werden kann, beschreibt *Ladeur*, Privatisierung öffentlicher Aufgaben und die Notwendigkeit der Entwicklung eines neuen Informationsverwaltungsrechts, in: Hoffmann-Riem/Schmidt-Aßmann (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, 2000, S. 225 (244 ff.); *ders.*, CR 2000, 433 (434 f.) dazu, dass die Behörden die Ungewissheit dennoch möglichst gering zu halten versuchen.

[6] Vgl. *Scherzberg*, Wissen, Nichtwissen und Ungewissheit im Recht, in: Engel/Halfmann/Schulte (Hrsg.), Wissen – Nichtwissen – Unsicheres Wissen, 2002, S. 113 (115 f.); *Hoffmann-Riem*, Wissen als Risiko – Unwissen als Chance, in: Augsberg (Hrsg.), Ungewissheit als Chance, 2009, S. 17 (19.).

klar sein, dass sich keine Entscheidung auf vollständige Informationen stützen kann; Entscheidung unter Nichtwissen ist die Regel, nicht die Ausnahme."[7]

Das Nichtwissensmanagement betrifft sowohl die epistemische Unsicherheit über Cybergefahren für die Netz- und Informationssicherheit als auch die Ermessensausübung im Rahmen des staatlichen Informationshandelns in der IT-Sicherheit. Ziel der Ausgestaltung eines Nichtwissensmanagements muss die Aufrechterhaltung der administrativen Entscheidungsfähigkeit sein. Tendenziell kann die Maxime sogar lauten, dass der Entscheidungsspielraum nicht zu verengen, sondern zu erhöhen ist.[8] Die Erweiterung des Handlungsspielraums berücksichtigt die Erkenntnis, dass Ungewissheit nur durch eine andere Ungewissheit ersetzt werden kann. Aus verfahrensrechtlicher Sicht ist das bewusste Akzeptieren von Unwägbarkeiten und Risiken Voraussetzung für das Lernen und für neue Erkenntnisgewinne und insofern in der NIS-Zusammenarbeit für den Informationsaustausch zu fordern.[9] Konkret folgt daraus eine stärkere Ausrichtung auf die Zeitdimension. Im Gegensatz zur Sachdimension ist nicht „die richtige" Entscheidung zu suchen, sondern danach zu fragen, ob das Handeln notfalls revidierbar ist.[10] Als Grenze des staatlichen Informationshandelns gilt dann vor allem das aus der grundrechtlichen Abwägungslehre bekannte Prinzip, dass irreversible Schäden an Rechtsgütern grundsätzlich zu verhindern sind.

---

[7] *Schulz*, Beurteilungsspielräume als Wissensproblem, Rewi 2012, 330 (343).

[8] Vgl. *Luhmann*, Organisation und Entscheidung, 2000, S. 199.

[9] Vgl. *Appel*, Methodik des Umgangs mit Ungewissheit, in: Schmidt-Aßmann/Hoffmann-Riem (Hrsg.), Methoden der Verwaltungsrechtswissenschaft, 2003, S. 329 (333 f.).

[10] Vgl. *Augsberg*, Informationsverwaltungsrecht, 2014, S. 277; zur Frage des Maßes an Prävention in der resilienten Gesellschaft und mit kritischem Blick auf den sicherheitsrechtlichen Abwägungsdiskurs *Würtenberger*, Grundzüge eines Rechts der Zivilen Sicherheit, in: Gusy/Kugelmann/ders., Rechtshandbuch Zivile Sicherheit, 2017, S. 611 (630).

Literaturverzeichnis

Abelson, *Harold*, *Anderson, Ross*, *Bellovin*, *Steven*, *Benaloh*, *Josh*, *Blaze*, *Matt*, *Diffie*, *Whitfield*, *Gilmore*, *John*, *Green*, *Matthew*, *Landau*, *Susan*, *Neumann*, *Peter*, *Rivest*, *Ronald*, *Schiller*, *Jeffrey*, *Schneider*, *Bruce*, *Specter*, *Michael*, *Weitzner*, *Daniel*: Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications, Computer Science and Artificial Intelligence Laboratory Technical Report, MIT, Juli 2015, S. 1, online abrufbar: https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf (zuletzt abgerufen am 30. April 2017).

Aden, *Menno*: Wissenszurechnung in der Körperschaft, Neue Juristische Wochenschrift 1999, S. 3098–3099.

Albers, *Marion*: Information als neue Dimension im Recht, Rechtstheorie 33 (2002), S. 61–89.

Dies.: Umgang mit personenbezogenen Informationen und Daten, in: Hoffmann-Riem, Wolfgang, Schmidt-Aßmann, Eberhard, Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts, Band II: Informationsordnung – Verwaltungsverfahren – Handlungsformen, 2. Auflage, München 2012, § 22, S. 107–234.

Dies.: Die Komplexität verfassungsrechtlicher Vorgaben für das Wissen der Verwaltung. Zugleich ein Beitrag zur Systembildung im Informationsrecht, in: Collin, Peter, Spiecker gen. Döhmann, Indra (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, Tübingen 2008, S. 50–69.

Alexy, *Robert*: Theorie der Grundrechte, Baden-Baden 1985.

Andersson, *Jan Joel*/*Malm*, *Andreas*: Public-Private Partnership and the Challenge of Critical Infrastructure Protection, in: Dunn, Myriam, Mauer, Victor (Hrsg.), International CIIP Handbook 2006 Vol. II: Analyzing Issues, Challenges, and Prospects, Zürich 2006, S. 139–169.

Appel, *Ivo*: Methodik des Umgangs mit Ungewissheit, in: Schmidt-Aßmann, Eberhard, Hoffmann-Riem, Wolfgang (Hrsg.), Methoden der Verwaltungsrechtswissenschaft, Baden-Baden 2003, S. 329–336.

Armstrong, *Robert*/*Mayo*, *Jackson*/*Siebenlist*, *Frank*: Complexity Science Challenges in Cybersecurity, Albuquerque, Livermore 2009.

Arndt, *Hans-Wolfgang*/*Fetzer*, *Thomas*/*Scherer*, *Joachim*/*Graulich*, *Kurt* (Hrsg.): TKG Telekommunikationsgesetz Kommentar, 2. Auflage, Berlin 2015.

Article 29 Data Protection Working Party: Opinion 03/2013 on purpose limitation, WP 203, 00569/13/EN, 2. April 2013, online abrufbar: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (zuletzt abgerufen am 30. April 2017).

Artikel-29-Datenschutzgruppe: Die Zukunft des Datenschutzes: Gemeinsamer Beitrag zu der Konsultation der Europäischen Kommission zu dem Rechtsrahmen für das Grundrecht auf den Schutz der personenbezogenen Daten, WP 168, 02356/09/DE, 1. Dezember 2009,

online abrufbar: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_de.pdf (zuletzt abgerufen am 30. April 2017).

Dies.: Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", WP 136, 20. Juni 2007.

Attendorn, *Thorsten*: Die institutionelle Bedeutung des GEREK in der TK-Regulierung – Ein kleiner Schritt in Richtung des Europäischen Regulierungsverbunds?, Computer und Recht 2011, S. 721–725.

Auer-Reinsdorf, *Astrid*/*Conrad*, *Isabell*: IT- und Datenschutzrecht, 2. Auflage, München 2016.

Augsberg, *Ino*: Informationsverwaltungsrecht: Zur kognitiven Dimension der rechtlichen Steuerung von Verwaltungsentscheidungen, Tübingen 2014.

Augsberg, *Steffen*: Europäisches Verwaltungsorganisationsrecht und Vollzugsformen, in: Terhechte, Jörg Philipp (Hrsg.), Verwaltungsrecht der Europäischen Union, Baden-Baden 2011, § 6, S. 201–272.

Ders.: Der Staat als Informationsmittler – Robin Hood oder Parasit der Wissensgesellschaft?, Deutsches Verwaltungsblatt 2007, S. 733–741.

Bader, *Johann*/*Ronellenfitsch*, *Michael* (Hrsg.): Beck'scher Online-Kommentar VwVfG, 30. Edition, Stand 01.01.2016, München 2016.

Badura, *Peter*/*Danwitz*, *Thomas von*/*Herdegen*, *Matthias*/*Sedemund*, *Jochim*/*Stern*, *Klaus* (Hrsg.): Beck'scher PostG-Kommentar, 2. Auflage, München 2004.

Baecker, *Dirk*: Organisation als System: Aufsätze, Frankfurt am Main 1999.

Bäcker, *Matthias*: Strategische Telekommunikationsüberwachung auf dem Prüfstand, Kommunikation & Recht 2014, S. 556–561.

Ders./*Giesler*, *Volkmar*/*Harms*, *Monika*/*Hirsch*, *Burkhard*/*Kaller*, *Stefan*/*Wolff*, *Heinrich Amadeus*: Bericht der Regierungskommission zur Überprüfung der Sicherheitsgesetzgebung in Deutschland, Bundesministerium des Inneren, Bundesministerium der Justiz, August 2013, online abrufbar: https://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2013/regierungskommission-sicherheitsgesetzgebung.pdf?__blob=publicationFile (zuletzt abgerufen am 30. April 2017).

Bär, *Wolfgang*: Auskunftsanspruch über Telekommunikationsdaten nach den neuen §§ 100g, 100h StPO, MultiMedia und Recht 2002, S. 358–364.

Ballaschk, *Julia*: In the Unseen Realm: Transnational Intelligence Sharing in the European Union – Challenges to Fundamental Rights and Democratic Legitimacy, Stanford Journal of International Law 2015, Volume 51, Issue 1, S. 19–51.

Balthasar, *Alexander*: Was heißt „völlige Unabhängigkeit" bei einer staatlichen Verwaltungsbehörde? Zugleich eine Auseinandersetzung mit dem Urteil des EuGH vom 9.3.2010, C-518/07 (Kommission/Deutschland), Zeitschrift für öffentliches Recht 2012, S. 5–45.

Bambauer, *Derek*: Sharing Shortcomings, Loyola University Chicago Law Journal 2015, Arizona Legal Studies Discussion Paper Nr. 15–26, online abrufbar: https://pdfs.semanticscholar.org/daa1/b94a574375313317e9c1ce429382f783ba29.pdf (zuletzt abgerufen am 30. April 2017).

Bamberger, *Heinz Georg*, *Roth*, *Herbert* (Hrsg.): Beck'scher Online-Kommentar BGB, 37. Edition, Stand 01.11.2015, München 2015.

Bangemann, *Martin*: Europa und die globale Informationsgesellschaft: Empfehlungen für den Europäischen Rat (Bangemann-Bericht), Brüssel 1994.

Barlow, *John Perry*: A Declaration of the Independence of Cyberspace, 08.02.1996, online abrufbar: https://www.eff.org/de/cyberspace-independence (zuletzt abgerufen am 30. April 2017).

Bartelt, *Sandra*, *Zeitler*, Helge Elisabeth: Zugang zu Dokumenten der EU, Europarecht 2003, S. 487–503.

Bateson, *Gregory*: Geist und Natur. Eine notwendige Einheit. Frankfurt 1987 (Original: Mind and Nature, 1979), 4. Auflage 1995.

Bauer, *Hartmut*: Die Bundestreue: zugleich ein Beitrag zur Dogmatik des Bundesstaatsrechts und zur Rechtsverhältnislehre, Tübingen 1992.

Bauer, *Johannes*/*van Eeten*, *Michael*: Cybersecurity: Stakeholder incentives, externalities, and policy options, Telecommunications Policy 33 (10), S. 706–709.

Baumann, *Peter*: Erkenntnistheorie, 3. Auflage, Stuttgart, Weimar 2015.

Becker, *Florian*/*Blackstein*, *Ylva*: Der transparente Staat – Staatliche Verbraucherinformation über das Internet, Neue Juristische Wochenschrift 2011, S. 490–494.

Bendiek, *Annegret*: Europäische Cybersicherheitspolitik, Studie der Stiftung Wissenschaft und Politik, Berlin 2012.

Berliner, *Markus*: Informationsbefugnisse der Bundesnetzagentur im Telekommunikationsrecht, Baden-Baden 2012.

Berger, Cathleen: Zwischen Strafverfolgung und nachrichtendienstlicher Analyse. Konsequenzen aus der Europäisierung der Cybersicherheitspolitik für Deutschland, integration 4/2013, S. 307–325.

Bergmann, *Jan* (Hrsg.): Handlexikon der Europäischen Union, 5. Auflage, Baden-Baden 2015.

Bergt, *Matthias*: BGH bestätigt: Webserver-Logfiles nicht nach § 100 Abs. 1 TKG erlaubt, CR-online Blog, 28.10.2014, online abrufbar: http://www.cr-online.de/blog/2014/10/28/bgh-bestaetigt-webserver-logfiles-nicht-nach-§-100-abs-1-tkg-erlaubt/ (zuletzt abgerufen am 30. April 2017).

Best, *Richard Jr.*: Intelligence Information: Need-to-know vs. Need-to-Share, Congressional Research Service 2011, online abrufbar: https://www.fas.org/sgp/crs/intel/R41848.pdf (zuletzt abgerufen am 30. April 2017).

Beucher, *Klaus*/*Utzerath*, *Julia*: Cybersicherheit – Nationale und internationale Regulierungsinitiativen Folgen für die IT-Compliance und die Haftungsmaßstäbe, MultiMedia und Recht 2013, 362–367.

Biendl, *Michael*: Die Vorratsdatenspeicherung in Europa, Deutschland und Bayern – eine vergleichende Betrachtung und Bewertung aus Sicht der IT-Sicherheit, 2011, online abrufbar: http://epub.uni-regensburg.de/24116/1/Biendl-IT-Sicherheit-VDS.pdf (zuletzt abgerufen am 30. April 2017).

Bizer, *Johann*: Die Kryptokontroverse – Innere Sicherheit und Sicherungsinfrastrukturen, in: Hammer, Volker (Hrsg.), Sicherungsinfrastrukturen: Gestaltungsvorschläge für Technik, Organisation und Recht, Berlin, Heidelberg 1995, S. 179–216.

Bockemühl, *Jan* (Hrsg.): Handbuch des Fachanwalts Strafrecht, 6. Auflage, Neuwied 2015.

Böcking, *David*: Geplante Meldepflicht: Firmen verweigern direkte Auskunft über Cyberangriffe, 19.08.2014, online abrufbar: http://www.spiegel.de/wirtschaft/unternehmen/it-sicherheit-wirtschaft-will-angriffe-nicht-direkt-an-staat-melden-a-986999.html (zuletzt abgerufen am 30. April 2017).

Böse, *Martin*: Wirtschaftsaufsicht und Strafverfolgung, Tübingen 2005.

Bötticher, *Astrid*: Open Source Intelligence. Ein Diskussionsbeitrag, in: Lange, Hans-Jürgen, Bötticher, Astrid (Hrsg.), Cyber-Sicherheit, Wiesbaden 2015, S. 181–212.

Bogdandy, *Armin von*: Die Informationsbeziehungen im europäischen Verwaltungsverbund, in: Hoffmann-Riem, Wolfgang, Schmidt-Aßmann, Eberhard, Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts, Band II: Informationsordnung – Verwaltungsverfahren – Handlungsformen, 2. Auflage, München 2012, § 25, S. 365–434.

Ders.: Grundprinzipien, in: Bogdandy, Armin von, Bast, Jürgen (Hrsg.), Europäisches Verfassungsrechts, 2. Auflage, Berlin, Heidelberg 2009, S. 13–71.

Bräutigam, *Peter*/*Wilmer*, *Stefan*: Big brother is watching you? – Meldepflichten im geplanten IT-Sicherheitsgesetz, Zeitschrift für Rechtspolitik 2015, S. 38–42.

Brandt, *Edmund*: Umweltaufklärung und Verfassungsrecht, Taunusstein 1994.

Bredt, *Stephan*: Die demokratische Legitimation unabhängiger Institutionen: vom funktionalen zum politikfeldbezogenen Demokratieprinzip, Tübingen 2006.

Bretthauer, *Sebastian*: Informationszugang im Recht der Europäischen Union, Die Öffentliche Verwaltung 2013, S. 677–685.

Breuer, *Rüdiger*: Schutz von Betriebs- und Geschäftsgeheimnissen im Umweltrecht, Neue Zeitschrift für Verwaltungsrecht 1986, S. 171–178.

Breyer, *Patrick*: (Un-)Zulässigkeit einer anlasslosen, siebentägigen Vorratsdatenspeicherung, MultiMedia und Recht 2011, S. 573–578.

Brink, *Stefan*/*Eckhardt*, *Jens*: Wann ist ein Datum ein personenbezogenes Datum? – Anwendungsbereich des Datenschutzrechts, Zeitschrift für Datenschutz 2015, S. 205–211.

Brink, *Stefan*/*Schmidt*, *Stephan*: Die rechtliche (Un-)Zulässigkeit von Mitarbeiterscreenings, MultiMedia und Recht 2010, S. 592–596.

Britz, *Gabriele*: Europäisierung des grundrechtlichen Datenschutzes?, Europäische Grundrechte-Zeitschrift 2009, S. 1–11.

Dies.: Vom Europäischen Verwaltungsverbund zum Regulierungsverbund? – Europäische Verwaltungsentwicklung am Beispiel der Netzzugangsregulierung bei Telekommunikation, Energie und Bahn, Europarecht 2006, S. 46–77.

Brodowski, *Dominik*/*Freiling*, *Felix*: Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, Berlin 2011.

Bröhmer, *Jürgen*: Transparenz als Verfassungsprinzip: Grundgesetz und Europäische Union, Tübingen 2004.

Brückner, *Annette*: Öffentliche Anhörung von Sachverständigen zum Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes BT-Drucksache 16/11967, Innenausschuss Wortprotokoll 94. Sitzung, Protokoll Nr. 16/94.

Bull, *Hans Peter*: Trennungsgebot und Verknüpfungsbefugnis – Zur Aufgabenteilung der Sicherheitsbehörden, in: Hendler, Reinhard, Ibler, Martin, Soria, José Martinez (Hrsg.), „Für Sicherheit, für Europa“: Festschrift für Volkmar Götz zum 70. Geburtstag, Göttingen 2005, S. 341–358.

Bullinger, *Martin*: Wettbewerbsgefährdung durch präventive Wirtschaftsaufsicht – Gefährdung des Entwicklungsvorsprungs zulassungspflichtiger neuer Industrieprodukte, Neue Juristische Wochenschrift 1978, S. 2121–2127.

Ders.: Wettbewerbsgerechtigkeit bei präventiver Wirtschaftsaufsicht – Verfassungsrechtlicher Schutz des Entwicklungsvorsprungs zulassungspflichtiger neuer Industrieprodukte, Neue Juristische Wochenschrift 1987, S. 2173–2181.

Bumke, *Christian*: Publikumsinformation. Erscheinungsformen, Funktionen und verfassungsrechtlicher Rahmen einer Handlungsform des Gewährleistungsstaates, Die Verwaltung 37 (2004), S. 3–33.

Ders.: Grundrechte. Theorie, Praxis, Dogmatik, in: Hoffmann-Riem, Wolfgang, Offene Rechtswissenschaft, Tübingen 2010, S. 435–466.

Ders.: Relative Rechtswidrigkeit: Systembildung und Binnendifferenzierungen im Recht, Tübingen 2004.

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Die Lage der IT-Sicherheit in Deutschland 2014, Bonn 2014.

Dass. (Hrsg.): Die Lage der IT-Sicherheit in Deutschland 2016, Bonn 2016.

Dass. (Hrsg.): IT-Grundschutzkataloge, Bonn 2014.

Dass. (Hrsg.): Handhabung von Schwachstellen, BSI-CS 019, Version 1.20, Bonn 2015, online abrufbar: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_019.pdf?__blob=publicationFile&v=2 (zuletzt abgerufen am 17. April 2017).

Bundesbeauftragte der Bundesregierung für Informationstechnik: Migrationsleitfaden, Leitfaden für die Migration von Software, Version 4.0, Berlin März 2012, online abrufbar: http://www.cio.bund.de/SharedDocs/Publikationen/DE/Architekturen-und-Standards/migrationsleitfaden_4_0_download.pdf?__blob=publicationFile (zuletzt abgerufen am 30. April 2017).

Bundesbeauftragte für Datenschutz und Informationssicherheit: Anwendungshinweise zum Informationsfreiheitsgesetz (IFG), überarbeitete Fassung, Stand 1. August 2007, online abrufbar: http://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO2.pdf?__blob=publicationFile (zuletzt abgerufen am 30. April 2017).

Bundeskriminalamt (Hrsg.): Cybercrime Bundeslagebild 2014, Wiesbaden 2014.

Bundesministerium des Inneren (Hrsg.): Open Government Data Deutschland, Eine Studie zu Open Government in Deutschland im Auftrag des Bundesministerium des Inneren, Juli 2012, online abrufbar: https://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/ModerneVerwaltung/opengovernment.pdf?__blob=publicationFile (zuletzt abgerufen am 30. April 2017).

Dass. (Hrsg.): Cyber-Sicherheitsstrategie für Deutschland, Berlin 2016, online abrufbar: https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (zuletzt abgerufen am 30. April 2017).

Bundesministerium der Justiz (Hrsg.): Handbuch der Rechtsförmlichkeit, 3. Auflage, Bonn 2008, online abrufbar: http://hdr.bmj.de/sitemap.html (zuletzt abgerufen am 30. April 2017).

Bundesministerium für Wirtschaft und Energie, *Bundesministerium des Inneren*, *Bundesministerium für Verkehr und digitale Infrastruktur* (Hrsg.): Digitale Agenda 2014–2017, München 2014.

Bundesnetzagentur (Hrsg.): Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Telekommunikationsgesetz (TKG), Stand 07.01.2016, Version 1.1, online abrufbar: http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/KatalogSicherheitsanforderungen.pdf?__blob=publicationFile&v=6 (zuletzt abgerufen am 30. April 2017).

Dies. (Hrsg.): Umsetzung des § 109 Absatz 5 TKG zur Mitteilung einer Sicherheitsverletzung (Umsetzungskonzept), Stand 29.01.2014, Version 2.0, online abrufbar: http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/mitteilungeinersicherheitsverletzung/Umsetzungskonzept_§_109_(5)_TKG_Mitteilung_Sicherheitsverletzung.pdf?__blob=publicationFile&v=3 (zuletzt abgerufen am 30. April 2017).

Dies. (Hrsg.): Leitfaden zur Erstellung eines Sicherheitskonzepts gemäß § 109 Abs. 3 TKG, Stand Januar 2006.

Dies. (Hrsg.): Tätigkeitsbericht nach § 121 Abs. 1 TKG vom 07.12.2015, Telekommunikation 2014/2015, online abrufbar: https://www.bundesnetzagentur.de/SharedDocs/Downloads/

DE/Allgemeines/Bundesnetzagentur/Publikationen/Berichte/2015/TB_TK_2015.pdf?__blob=publicationFile&v=3 (zuletzt abgerufen am 30. April 2017).

Calliess, *Christian*/*Ruffert*, *Matthias* (Hrsg.): EUV/AEUV, Kommentar, 4. Auflage, München 2011.

Canaris, *Claus-Wilhelm*/*Larenz*, *Karl*: Methodenlehre der Rechtswissenschaft, 4. Auflage, Berlin 2014.

Cencini, *Andrew*/*Yu*, *Kevin*/*Chan*, *Tony*: Software Vulnerabilities: Full-, Responsible-, and Non-Disclosure, Dezember 2005, online abrufbar: https://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/software_vulnerabilities_by_cencini_yu_chan.pdf (zuletzt abgerufen am 30. April 2017).

Chang, *Frederik*: Is Your Data on the Healthcare.gov Website Secure?, Written Testimony before the Committee on Science, Space and Technology, U.S. House of Representatives, November 2013, online abrufbar: http://docs.house.gov/meetings/SY/SY00/20131119/101533/HHRG-113-SY00-Wstate-ChangF-20131119.pdf (zuletzt abgerufen am 30. April 2017).

Chiesa, *Raoul*/*Ducci*, *Stefania*/*Ciappi*, *Silvio*: Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking, Boca Raton 2009.

Claasen, *Kai-Dieter*: Gute Verwaltung im Recht der Europäischen Union: eine Untersuchung zu Herkunft, Entstehung und Bedeutung des Art. 41 Abs. 1 und 2 der Europäischen Grundrechtecharta, Berlin 2008.

Clark, *Dave*: A Cloudy Crystal Ball – Visions of the Future, in: Davies, Megan, Clark, Cythia, Legare, Debra (Hrsg.), Proceedings of the Twenty-Fourth Internet Engineering Task Force, Massachusetts Institute of Technology, NEARnet, Cambridge, MA 1992, S. 539–543.

Collin, *Peter*/*Lutterbeck*, *Klaus-Gert*: Handlungsorientierungen moderner Verwaltung – eine Problemdarstellung, in: Collin, Peter, Lutterbeck, Klaus-Gert (Hrsg.), Eine intelligente Maschine? Handlungsorientierungen moderner Verwaltung (19./20 Jh.), Baden-Baden 2009, S. 11–34.

Ders./*Spiecker gen. Döhmann*, *Indra*: Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts – ein Problemaufriss, in: Spiecker gen. Döhmann, Indra, Collin, Peter (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, Tübingen 2008, S. 3–25.

Comey, *James*: Going Dark: Are Technology, Privacy and Public Safety on a Collision Course?, Speech at Brookings Institution, 16.10.2014, online abrufbar: https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course (zuletzt abgerufen am 30. April 2017).

Cormack, *Andrew*: Incident Response and Data Protection, 2011.

Czakert, *Ernst*: Die gesetzliche Umsetzung des Common Reporting Standards in Deutschland, Deutsches Steuerrecht 2015, S. 2697–2702.

Däubler, *Wolfgang*/*Klebe*, *Thomas*/*Wedde*, *Peter*/*Weichert*, *Thilo* (Hrsg.): Bundesdatenschutzgesetz, Kompaktkommentar zum BDSG, 5. Auflage, Frankfurt am Main 2016.

Dainotti, *Alberto*/*Squarcella*, *Claudio*/*Aben*, *Emile*/*Claffy*, *Kimberly*/*Chiesa*, *Marco*/*Russo*, *Michele*/*Pescapè*, *Antonio*: Analysis of Country-wide Internet Outages Caused by Censorship, Institute of Electrical and Electronics Engineers/Association for Computing Machinery Transactions on Networking Volume 22 Issue 6 (2014), S. 1964–1977.

Dammann, *Ulrich*/*Simitis*, *Spiros*: EG-Datenschutzrichtlinie, Kommentar, Baden-Baden 1997.

Dannecker, *Christoph*: Internet-Pranger auf Verdacht: Zur Bedeutung der Unschuldsvermutung für die Information der Öffentlichkeit über lebensmittelrechtliche Verstöße nach § 40 Abs. 1a Nr. 2 LFGB, JuristenZeitung 2013, S. 924–933.

Ders.: Der nemo tenetur-Grundsatz – prozessuale Fundierung und Geltung für juristische Personen, Zeitschrift für die gesamte Strafrechtswissenschaft 127 (2015), S. 370–409.

Danwitz, *Thomas von*: Europäisches Verwaltungsrecht, Berlin 2008.

Ders.: Verwaltungsrechtliches System und europäische Integration, Tübingen 1996.

Dau, *Klaus*: Rechtsgrundlagen für den MAD – Das Gesetz über den Militärischen Abschirmdienst, Die Öffentliche Verwaltung 1991, S. 661–670.

David, *Antje*: Inspektionen als Instrument der Vollzugskontrolle im Europäischen Verwaltungsverbund, in: Schmidt-Aßmann, Eberhard, Schöndorf-Haubold, Bettina (Hrsg.), Der Europäische Verwaltungsbund. Formen und Verfahren der Verwaltungszusammenarbeit in der EU, Tübingen 2005, S. 237–264.

David, *Antje*: Inspektionen als Instrument der Vollzugskontrolle im Europäischen Verwaltungsverbund, in: Schmidt-Aßmann, Eberhard, Hoffmann-Riem, Wolfgang (Hrsg.). Strukturen des Europäischen Verwaltungsrechts, Baden-Baden 1999, S. 237–264.

Deleuze, *Gilles*/*Guattari*, *Félix*: Tausend Plateaus: Kapitalismus und Schizophrenie, Nachdr. Der 6. Auflage, Berlin 2010.

Dickow, *Marcel*/*Bashir*, *Bashir*: Sicherheit im Cyberspace, in: Aus Politik und Zeitgeschichte 43–45/2016, 2016, S. 15–20.

Dietlein, *Johannes*: Die Lehre von den grundrechtlichen Schutzpflichten, Berlin 2005.

Di Fabio, *Udo*: Risikoentscheidungen im Rechtsstaat: zum Wandel der Dogmatik im öffentlichen Recht, insbesondere am Beispiel der Arzneimittelüberwachung, Tübingen 1994.

Djeffal, *Christian*: Neue Sicherungspflicht für Telemediendiensteanbieter: Webseitensicherheit jetzt Pflicht nach dem IT-Sicherheitsgesetz, MultiMedia und Recht 2015, S. 716–721.

Dörner, *Dietrich*: Die Logik des Misslingens: strategisches Denken in komplexen Situationen, 11. Auflage, Reinbek bei Hamburg 2012.

Dörr, *Oliver*: Die Anforderungen an ein zukunftsfähiges Infrastrukturrecht, in: VVDStRL 73 (2013), S. 323–361.

Dombert, *Matthias*/*Räuker*, *Kaya*: Am Beispiel der deutschen Sicherheitsarchitektur: Zum Grundrechtsschutz durch Organisation, Die Öffentliche Verwaltung 2014, S. 414–421.

Dombrowsky, *Wolf*: Schutz kritischer Infrastrukturen als Grundproblem einer modernen Gesellschaft, in: Kloepfer, Michael (Hrsg.), Schutz kritischer Infrastrukturen, Baden-Baden 2010, S. 27–38.

Dreier, *Horst* (Hrsg.): Grundgesetz Kommentar, Band II: Artikel 20–82, 3. Auflage, Tübingen 2015.

Ders. (Hrsg.): Grundgesetz Kommentar, Band III: Artikel 83–146, 2. Auflage, Tübingen 2008.

Dreier, *Thomas*: Urheberrecht auf dem Weg zur Informationsgesellschaft – Anpassung des Urheberrechts an die Bedürfnisse der Informationsgesellschaft, Gewerblicher Rechtsschutz und Urheberrecht 1997, S. 859–866.

Ders./*Fischer*, *Veronika*/*van Raay*, *Anne*/*Spiecker gen. Döhmann*, *Indra* (Hrsg.): Informationen der öffentlichen Hand – Zugang und Nutzung, Baden-Baden 2016.

Drexl, *Josef*/*Kreuzer*, *Karl* (Hrsg.): Europarecht im Informationszeitalter: 5. Würzburger Europarechtstage im Juni 1999, Baden-Baden 2000.

Droste, *Bernadette*: Handbuch des Verfassungsschutzrechts, Hannover 2007.

Druey, *Jean Nicolas*: Information als Gegenstand des Rechts: Entwurf einer Grundlegung, Zürich 1995.

Düsseldorfer Kreis: Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 26./27.11.2009: Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten, Stralsund 2009.

Duisberg, *Alexander*/*Picot*, *Henriette*: Rechtsfolgen von Pannen in der Datensicherheit, Computer und Recht 2009, S. 823–828.

Dunn Cavelty, *Myriam*: Cyber(Un)Sicherheit: Grundlagen, Trends und Herausforderungen, Internet in der Politik, Politische Bildung 1/12 (2012), S. 66–84.

Dies./*Suter*, *Manuel*: Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection, International Journal of Critical Infrastructure Protection 2009, S. 179–187.

Dutzler, *Barbara*: Der Status des ESZB aus demokratietheoretischer Sicht, Der Staat 41 (2002), S. 495–522.

Dworkin, *Ronald*: Taking rights seriously, Cambridge, MA 1978.

Eberle, *Carl-Eugen*: Organisation der automatisierten Datenverarbeitung in der öffentlichen Verwaltung: eine Untersuchung unter besonderer Berücksichtigung organisationsrechtlicher Fragen, Berlin 1976.

Eckert, *Claudia*: IT-Sicherheit: Konzept – Verfahren – Protokolle, München 2000.

Eckhardt, *Jens*: Datenschutz und Überwachung im Regierungsentwurf zum TKG, Computer und Recht 2003, S. 805–813.

Ders.: Öffentliche Sicherheit, in: Heun, Sven-Erik (Hrsg.), Handbuch Telekommunikationsrecht, 2. Auflage, Köln 2007, S. 61–138.

Ders.: Der Referentenentwurf zum IT-Sicherheitsgesetz – Schutz der digitalen Zukunft?, Zeitschrift für Datenschutz 2014, S. 599–605.

Eckhardt, *Jens*/*Schmitz*, *Peter*: Informationspflicht bei „Datenschutzpannen", Datenschutz und Datensicherheit 2010, S. 390–397.

Ehlers, *Dirk*/*Pünder*, *Hermann* (Hrsg.): Allgemeines Verwaltungsrecht, 15. Auflage, Berlin 2015.

Ehmann, *Eugen*/*Helfrich*, *Marcus*: EG-Datenschutzrichtlinie: Kurzkommentar, Köln 1999.

Eidenmüller, *Horst*: Liberaler Paternalismus, JuristenZeitung 2011, S. 814–821.

Ders.: Effizienz als Rechtsprinzip: Möglichkeiten und Grenzen der ökonomischen Analyse des Rechts, 4. Auflage, Tübingen 2015.

Eifert, *Martin*: Grundversorgung mit Telekommunikationsleistungen im Gewährleistungsstaat, Baden-Baden 1998.

Ders.: Regulierte Selbstregulierung und die lernende Verwaltung, Die Verwaltung 2001, Beiheft 4, S. 137–157.

Ders.: Europäischer Verwaltungsverbund als Lernverbund, in: Spiecker gen. Döhmann, Indra, Collin, Peter (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, Tübingen 2008, S. 159–175.

Ders.: Die gerichtliche Kontrolle der Entscheidungen der Bundesnetzagentur, Zeitschrift für das gesamte Handels- und Wirtschaftsrecht 174 (2010), S. 449–485.

Ders.: Staatliche Informationsinfrastrukturen – Organisation im gegliederten Verwaltungsraum und private Weiterverwendung der Verwaltungsinformation, in: Lipowicz, Irena, Schneider, Jens-Peter (Hrsg.), Perspektiven des deutschen, polnischen und europäischen Informationsrechts: Ergebnisse einer deutsch-polnischen Alexander von Humboldt-Institutspartnerschaft, Göttingen 2011, S. 71–87.

Ders.: Regulierungsstrategien, in: Hoffmann-Riem, Wolfgang, Schmidt-Aßmann, Eberhard, Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts, Band I: Methoden – Maßstäbe – Aufgaben – Organisation, 2. Auflage, München 2012, § 19, S. 1319–1394.

Ders.: Nudging: Eine politische Aufgabe, in: Theorie und Praxis der sozialen Arbeit 66 (2015), S. 178–180.

Eikenberg, *Katharina*: Article 296 (ex 223) E.C. and External Trade in Strategic Goods, European Law Review 25 (2000), S. 117–138.

Einziger, *Kurt*/*Skopik*, *Florian*/*Fiedler*, *Roman*: Keine Cyber-Sicherheit ohne Datenschutz, Datenschutz und Datensicherheit 2015, S. 723–729.

Engel, *Christoph*: Vertrauen: ein Versuch, in: Preprint aus der Max-Planck-Projektgruppe Recht der Gemeinschaftsgüter 12/1999, online abrufbar: https://www.coll.mpg.de/pdf_dat/1999_12online.pdf (zuletzt abgerufen am 5.3.2016).

Ders.: Der egalitäre Kern des Internet. Eine vernachlässigte Herausforderung für Steuerungstheorie und Steuerungspraxis, in: Ladeur, Karl-Heinz (Hrsg.), Innovationsoffene Regulierung des Internet. Neues Recht für Kommunikationsnetzwerke, Baden-Baden 2003, S. 25–38.

Ders.: Verhaltenswissenschaftliche Analyse: eine Gebrauchsanweisung für Juristen, in: ders., Christoph, Englerth, Markus, Lüdemann, Jörn, Spiecker gen. Döhmann, Indra (Hrsg.), Recht und Verhalten – Beiträge zu Behavioral Law and Economics, Tübingen 2007, S. 363–406.

Engeler, *Malte*/*Jensen*, *Meiko*/*Obersteller*, *Hannah*/*Deibler*, *Daniel*/*Hansen*, *Marit*: Monitoring durch Informationsfusion und Klassifikation zur Anomalieerkennung – Ausarbeitung aus Perspektive des Datenschutzes und der Datensicherheit zur Zulässigkeit sowie zum Einsatz und zur Gestaltung von Anomalie erkennenden Verfahren in Internet-Infrastrukturen, Kiel 2014, online abrufbar: https://www.datenschutzzentrum.de/uploads/projekte/D5.2_MonIKA_Datenschutz-Ausarbeitung_Anomalieerkennung_Final_pub_v1.1.pdf (zuletzt abgerufen am 30. April 2017).

Englerth, *Markus*: Behavioral Law and Economics – eine kritische Einführung, in: Engel, Christoph, ders., Lüdemann, Jörn, Spiecker gen. Döhmann, Indra (Hrsg.), Recht und Verhalten – Beiträge zu Behavioral Law and Economics, Tübingen 2007, S. 60–132.

Enquete-Kommission Internet und digitale Gesellschaft (Deutscher Bundestag): Teilbericht der Enquete-Kommission auf BT-Drs. 17/12541, Projektgruppe Zugang, Struktur und Sicherheit im Netz, A-Drs. 17(24)064.

Epiney, *Astrid*: Die Rechtsprechung des EuGH im Jahr 2014 – Europäisches Verfassungsrecht, Neue Zeitschrift für Verwaltungsrecht 2015, S. 704–715.

Eßer, *Martin*: Unternehmen trifft weiter keine Pflicht zur Vorratsdatenspeicherung – EuGH verbietet anlasslose TK-Datenspeicherung, Datenschutz-Berater 2014, S. 102–103.

Ders./*Kramer*, *Philipp*/*Lewinski*, *Kai von* (Hrsg.): Auernhammer BDSG, Bundesdatenschutzgesetz und Nebengesetze, 4. Auflage, Köln 2014.

Europäische Kommission: Grünbuch über die Informationen des öffentlichen Sektors in der Informationsgesellschaft, KOM(1998) 585, Brüssel 1998.

European Data Protection Supervisor: Opinion on the Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy on a ‚Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace', and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union, Brüssel 2013, online abrufbar: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2013/13-06-14_Cyber_security_EN.pdf (zuletzt abgerufen am 30. April 2017).

European Network and Information Security Agency (Hrsg.): A flair for sharing – encouraging information exchange between CERTs, A study into the legal and regulatory aspects of information sharing and cross-border collaboration of national/governmental CERTSs in Europe, Initial Edition 1.0, November 2011, online abrufbar: https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/legal-information-sharing (zuletzt abgerufen am 30. April 2017).

Dies. (Hrsg.): Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches, Final Version 1.0, Dezember 2015, online abrufbar: https://www.enisa.europa.eu/activities/cert/support/information-sharing/cybersecurity-information-sharing (zuletzt abgerufen am 30. April 2017).

Dies. (Hrsg.): Technical Guideline on Security measures for Article 4 and Article 13 a, Version 1.0, Dezember 2014, online abrufbar: https://resilience.enisa.europa.eu/article-13/guideline-on-security-measures-for-article-4-and-article-13a/TechnicalGuidelineonSecuritymeasuresforArticle4andArticle13a_version_1_0.pdf (zuletzt abgerufen am 30. April 2017).

Dies. (Hrsg.): Technical Guideline on Incident Reporting: Technical guidance on the incident reporting in Article 13a, Version 2.1, Oktober 2014, online abrufbar: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/guidelines/Technical%20Guidelines%20on%20Incident%20Reporting (zuletzt abgerufen am 30. April 2017).

Dies. (Hrsg.): Understanding the importance of the Internet Infrastructure in Europe – Guidelines for enhancing the Resilience of eCommunication Networks, Dezember 2013.

Dies. (Hrsg.): Recommendations for technical implementation of Art. 4, April 2012, online abrufbar: https://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn/art4_tech (zuletzt abgerufen am 30. April 2017).

Dies. (Hrsg.): Data breach notifications in the EU, 2011, online abrufbar: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/dbn (zuletzt abgerufen am 30. April 2017).

Dies. (Hrsg.): Actionable information for security incident response, November 2014, online abrufbar: https://www.enisa.europa.eu/activities/cert/support/actionable-information/actionable-information-for-security (zuletzt abgerufen am 30. April 2017).

Everson, *Michelle*: Independent Agencies: Hierarchy Beaters?, European Law Journal 1995, S. 180–204.

Federal Civil Defense Administration (Hrsg.): Impact of Air Attack in World War II: Selected Data for Civil Defense Planning. Division II: Effects on the General Economy, Volume 1: Economic Effects – Germany, Washington 1953.

Federrath, *Hannes*/*Pfitzmann*, *Andreas*: Datensicherheit, in: Schulte, Martin, Schröder, Rainer (Hrsg.), Handbuch des Technikrechts, 2. Auflage, Berlin 2011, S. 857–886.

Fehling, *Michael*: Mitbenutzungsrecht Dritter bei Schienenwegen, Energieversorgungs- und Telekommunikationsleitungen vor dem Hintergrund staatlicher Infrastrukturverantwortung, Archiv des öffentlichen Rechts 121 (1996), S. 60–95.

Feik, *Rudolf*: Öffentliche Verwaltungskommunikation: Öffentlichkeitsarbeit, Aufklärung, Empfehlung, Warnung, Wien 2007.

Feiler, Lukas: Information Security Law in the EU and the U.S.: A Risk- Based Assessment of Regulatory Policies, Wien, New York 2011.

Ders.: Outages of Critical Information Infrastructure under EU and U.S. Law – Transparency versus Secrecy, Journal of Internet Law, September 2011, S. 1, 15–23.

Ferris, *John*: Signals Intelligence in War and Power Politics, in: Johnson, Loch, The Oxford Handbook of National Security Intelligence, Oxford 2010, S. 155–171.

Fischer, *Eric*: Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions, Congressional Research Service 2013.

Fischer, *Wolfgang*: www.InfrastrukturInternet-Cyberterror.Netzwerk: Analyse und Simulation strategischer Angriffe auf die kritische Infrastruktur Internet, Jülich 2007.

Fleischer, *Holger*: Informationsasymmetrie im Vertragsrecht: eine rechtsvergleichende und interdisziplinäre Abhandlung zu Reichweite und Grenzen vertragsschlußbezogener Aufklärungspflichten, München 2001.

Foerster, *Heinz von*: The Curious Behavior of Complex Systems: Lessons from Biology, in: Linstone, Harold, Simmonds, Walter Henry Clive (Hrsg.), Futures Research: New Directions, Reading, MA 1977, S. 104–113.

Forgó, *Nikolaus*: Grundzüge des Informationssicherheitsrechts, in: Grützmacher, Malte, Conrad, Isabell (Hrsg.), Recht der Daten und Datenbanken im Unternehmen, Zugleich Festgabe Jochen Schneider zum 70. Geburtstag, Köln 2014, S. 1053–1060.

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.: Stellungnahme des FIfF zum IT-Sicherheitsgesetz der Bundesregierung vom 17.12.2014, online abrufbar: http://cyberpeace.fiff.de/Uploads/Uploads/FIfF_Stellungnahme_IT-Sicherheitsgesetz.pdf (zuletzt abgerufen am 30. April 2017).

Frank, *Torben*: Der Schutz von Unternehmensgeheimnissen im Öffentlichen Recht, Frankfurt am Main 2009.

Franzius, *Claudio*: Gewährleistung im Recht: Grundlagen eines europäischen Regelungsmodells öffentlicher Dienstleistungen, Tübingen 2009.

Frenz, *Walter*: Verwaltungskooperation mit der Union im Lichte von Art. 197 AEUV und des Lissabon-Urteils, Die Öffentliche Verwaltung 2010, S. 66–73.

Frenz, *Walter*: Handbuch Europarecht, Band 4: Europäische Grundrechte, Berlin 2009.

Freund, *Bernhard*: Anmerkung zum Urteil des EuGH vom 24.11.2011, Rs. C-468/10, Computer und Recht 2012, S. 32–33.

Freund, *Matthias*: Infrastrukturgewährleistung in der Telekommunikation, Neue Zeitschrift für Verwaltungsrecht 2003, S. 408–415.

Fung, *Archon*/*Graham*, *Mary*/*Weil*, *David*: Full Disclosure: The Perils and Promise of Transparency, Cambridge 2007.

Gärditz, *Klaus Ferdinand*: Hochschulorganisation und verwaltungsrechtliche Systembildung, Tübingen 2009.

Ders.: Regulierungsrechtliche Auskunftsanordnungen als Instrument der Wissensgenerierung, Deutsches Verwaltungsblatt 2009, S. 69–77.

Ders.: Europäisches Regulierungsverwaltungsrecht auf Abwegen, Archiv des öffentlichen Rechts Band 135 (2010), S. 251–288.

Ders.: Anmerkung zur Entscheidung des BVerfG vom 24.04.2013, 1 BvR 1215/07 – Zur Frage der Verfassungswidrigkeit des Antiterrordateigesetzes, JuristenZeitung 2013, S. 633–636.

Galetta, *Diana-Urania*/*Hofmann*, *Herwig*/*Schneider*, *Jens-Peter*: Information Exchange in the European Administrative Union: An Introduction, European Public Law 20 (2014), S. 65–70.

Gallwas, *Hans-Ullrich*: Zum Prinzip der Erforderlichkeit im Datenschutzrecht, in: Haft, Fritjof, Hassemer, Winfried, Neumann, Ulfrid, Schild, Wolfgang, Schroth, Ulrich (Hrsg.), Strafgerechtigkeit: Festschrift für Arthur Kaufmann zum 70. Geburtstag, Heidelberg 1993, S. 819–829.

Gander, *Hans-Helmuth*/*Perron*, *Walter*/*Poscher*, *Ralf*/*Riescher*, *Gisela*/*Würtenberger*, *Thomas*: Resilienz in der offenen Gesellschaft – Symposium des Centre for Security and Society, Baden-Baden 2012.

Garvin, *David*: Das lernende Unternehmen I: Nicht schöne Worte – Taten zählen, Harvard Business Manager 1/1994, S. 74–85.

Gaycken, *Sandro*: Cybersicherheit in der Wissensgesellschaft – Zum Zusammenhang von epistemischer und physischer Unsicherheit, in: Daase, Christopher, Engbert, Stefan, Junk, Julian (Hrsg.), Verunsicherte Gesellschaft – Überforderter Staat – Zum Wandel der Sicherheitskultur, Frankfurt am Main 2013, S. 109–131.

Ders.: Offizielle Versionen versus mögliche Wahrheiten – Cybersecurity und das Problem der Geheimhaltung, in: Haupter (Hrsg.), Der digitale Dämon, München 2013, S. 49–59.

Ders.: Öffentliches Fachgespräch des Ausschusses „Digitale Agenda" des Deutschen Bundestages zum Thema IT-Sicherheit, Ausschussdrucksache 18(24)10.

Ders./Lindner, *Felix*: Zero Day Governance –A(n Inexpensive) Solution to the Cyber Security Problem, in: Harvard – MIT Cyber Dialogue: What is Stewardship in Cyberspace, April 2012, online abrufbar: http://www.cyberdialogue.citizenlab.org/wp-content/uploads/2012/2012papers/CyberDialogue2012_gaycken-lindner.pdf (zuletzt abgerufen am 30. April 2017).

Geppert, *Martin*/*Schütz*, *Raimund* (Hrsg.): Beck'scher TKG-Kommentar, 4. Auflage, München 2013.

Gerhard, *Julia*: (Grund-)Recht auf Verschlüsselung?, Baden-Baden 2010.

Gerlach, *Carsten*: Sicherheitsanforderungen für Telemediendienste – der neue § 13 Abs. 7 TMG, Computer und Recht 2015, 581–589.

Ders.: Personenbezug von IP-Adressen – Praktische Konsequenzen aus dem Urteil des LG Berlin vom 31.1.2013, Computer und Recht 2013, S. 478–484.

Gercke, *Marco*: Die Entwicklung des Internetstrafrechts 2014/2015, ZUM 2015, 772–782.

Ders.: Der Entwurf für eine EU-Richtlinie über Netz- und Informationssicherheit (NIS), Computer und Recht 2016, S. 28–30.

Gersdorf, *Hubertus*/*Paal*, *Boris* (Hrsg.): Beck'scher Online-Kommentar Informations- und Medienrecht, 11. Edition, Stand 01.02.2016, München 2016.

Geschäftsstelle des UP KRITIS (Hrsg.): Umsetzungsplan Kritische Infrastrukturen, Öffentlich-Private-Partnerschaft zum Schutz Kritischer Infrastrukturen – Grundlagen und Ziele, Frankfurt am Main 2014.

Giesen, *Thomas*: Zivile Informationsordnung im Rechtsstaat: Aufräumen!, Recht der Datenverarbeitung 2010, S. 266–274.

Görisch, *Christoph*: Demokratische Verwaltung durch Unionsagenturen: Ein Beitrag zur Konkretisierung der europäischen Verfassungsstrukturprinzipien, Tübingen 2009.

Gola, *Peter*/*Schomerus*, *Rudolf* (Hrsg.): BDSG Bundesdatenschutzgesetz, Kommentar, 12. Auflage, München 2015.

Grabitz, *Eberhard*/*Hilf*, *Meinhard*/*Nettesheim*, *Martin* (Hrsg.): Das Recht der Europäischen Union: EUV/AEUV, 57. Auflage, München 2015.

Gräfer, *Jens*/*Schmitt*, *Thomas*: Die Befugnisse der Kartell- und Regulierungsbehörden zur Durchführung von Enqueteuntersuchungen, Netzwirtschaften & Recht 2007, S. 2–7.

Graf, *Jürgen-Peter* (Hrsg.): Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, 23. Edition, Stand 16.11.2015, München 2015.

Gramm, *Christof*: Aufklärung durch staatliche Publikumsinformation, Der Staat 30 (1991), S. 51–80.

Grassmuck, *Volker*: Freie Software: Zwischen Privat- und Gemeineigentum, 2. Auflage, Bonn 2004.

Greenawalt, *Tim*: Die Indienstnahme privater Netzbetreiber bei der Telekommunikationsüberwachung in Deutschland: Spannungsfeld zwischen staatlichen Kontrollbefugnissen und wirtschaftlicher Betätigungsfreiheit, Berlin 2009.

Greenberg, *Andy*: The Shadow Brokers Mess Is What Happens When The NSA Hoards Zero-Days, Wired vom 17.08.2016, online abrufbar: https://www.wired.com/2016/08/shadow-brokers-mess-happens-nsa-hoards-zero-days/.

Grimm, *Dieter*: Der Datenschutz vor einer Neuorientierung, JuristenZeitung 2013, S. 585–592.

Groeben, *Hans von der*/*Schwarze, Jürgen*/*Hatje*, *Armin* (Hrsg.): Europäisches Unionsrecht: Vertrag über die Europäische Union, Vertrag über die Arbeitsweise der Europäischen Union, Charta der Grundrecht der Europäischen Union, Band 4, 7. Auflage, Baden-Baden 2015.

Gröpl, *Christoph*/*Windthorst*, *Kay*/*Coelln*, *Christian von*: Grundgesetz: Studienkommentar, 2. Auflage, München 2015.

Gröschner, *Rolf*: Öffentlichkeitsaufklärung als Behördenaufgabe, Deutsches Verwaltungsblatt 1990, S. 619–629.

Ders.: Transparente Verwaltung – Konturen eines Informationsverwaltungsrechts, Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer 63 (2004), S. 344–370.

Groß, *Thomas*: Ressortforschung, Agenturen und Beiräte – zur notwendigen Pluralität der staatlichen Wissensinfrastruktur, in: Röhl, Hans Christian (Hrsg.), Wissen – Zur kognitiven Dimension des Rechts, Die Verwaltung, Beiheft 9, Berlin 2010, S. 135–155.

Ders.: Die Verwaltungsorganisation als Teil organisierter Staatlichkeit, in: Hoffmann-Riem, Wolfgang, Schmidt-Aßmann, Eberhard, Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts, Band I: Methoden – Maßstäbe – Aufgaben – Organisation, 2. Auflage, München 2012, § 13, S. 905–952.

Grunwald, *Jürgen*: Neuere Entwicklungen des EU-Statistikrechts, in: Meng, Werner, Ress, Georg, Stein, Torsten (Hrsg.), Europäische Integration und Globalisierung – Festschrift zum 60-jährigen Bestehen des Europa-Instituts, Baden-Baden 2011, S. 185–197.

Guckelberger, *Annette*: Veröffentlichung der Leistungsempfänger von EU-Subventionen und unionsgrundrechtlicher Datenschutz, Europäische Zeitschrift für Wirtschaftsrecht 2011, S. 126–130.

Dies.: Rechtliche Anforderungen an die aktive Informationsvorsorge des Staates im Internet, in: Hill, Hermann, Schliesky, Utz (Hrsg.), Die Vermessung des virtuellen Raums, Baden-Baden 2012, S. 73–118.

Gurlit, *Elke*: Konturen eines Informationsverwaltungsrechts, Deutsches Verwaltungsblatt 2003, S. 1119–1134.

Dies.: Amtliche Verbraucherinformation – Symphonisches Werk oder Kakofonie?, Zeitschrift für Rechtspolitik 2015, S. 16–18.

Dies.: Das Informationsverwaltungsrecht im Spiegel der Rechtsprechung, Die Verwaltung 44 (2011), S. 75–103.

Gussone, *Peter*/*Michalczyk*, *Roman*: Der Austausch von Informationen im ECN – Wer bekommt was wann zu sehen?, Europäische Zeitschrift für Wirtschaftsrecht, S. 130–134.

Gusy, *Christoph*: Grundrechtsschutz vor staatlichen Informationseingriffen, Verwaltungsarchiv 1983, S. 91–111.

Ders.: Neutralität staatlicher Öffentlichkeitsarbeit – Voraussetzungen und Grenzen, Neue Zeitschrift für Verwaltungsrecht 2015, S. 700–704.

Ders.: Verwaltung durch Information, Neue Juristische Wochenschrift 2000, S. 977–986.

Ders.: Informationszugangsfreiheit – Öffentlichkeitsarbeit – Transparenz, JuristenZeitung 2014, S. 171–179.

Ders.: Informationsbeziehungen zwischen Staat und Bürger, in: Hoffmann-Riem, Wolfgang, Schmidt-Aßmann, Eberhard, Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts, Band II: Informationsordnung – Verwaltungsverfahren – Handlungsformen, 2. Auflage, München 2012, § 23, S. 221–304.

Haase, *Martin Sebastian*: Datenschutzrechtliche Fragen des Personenbezugs, Tübingen 2015.

Habammer, *Christoph*/*Denkhaus*, *Wolfgang*: Das E-Government-Gesetz des Bundes: Inhalt und erste Bewertung – Gelungener Rechtsrahmen für elektronische Verwaltung?, MultiMedia und Recht 2013, S. 358–362.

Hämmerli, *Bernhard*/*Renda*, *Andrea*: Protecting Critical Infrastructure in the EU, Centre for European Policy Studies Task Force Report, Brüssel 2010.

Härting, *Niko*: Internetrecht, 5. Auflage, Köln 2014.

Ders.: Zweckbindung und Zweckänderung im Datenschutzrecht, Neue Juristische Wochenschrift 2015, S. 3284–3288.

Ders.: Öffentlichkeitsarbeit einer Landesbehörde, Computer und Recht 2011, S. 585–588.

Ders.: Jan Philipp Albrecht setzt sich durch: Datenschutzrecht soll ausnahmslos für Maschinendaten gelten, CRonline Blog, 9.12.2015, online abrufbar: http://www.cr-online.de/blog/2015/12/09/jan-philipp-albrecht-setzt-sich-durch-datenschutzrecht-soll-ausnahmslos-fuer-maschinendaten-gelten/ (zuletzt abgerufen am 30. April 2017)

Hagen, *Silvia*: IPv6: Grundlagen – Funktionalität – Integration, 2. Auflage, Maur 2009.

Hahn, *Dietger*: Frühwarnsysteme, Krisenmanagement und Unternehmensplanung, in: Frühwarnsysteme, Albach, Horst, Hahn, Dietger, Mertens, Peter (Hrsg.), Zeitschrift für Betriebswirtschaft-Ergänzungsheft Nr. 2 1979, S. 25–46.

Hanloser, *Stefan*: Europäische Security Breach Notification, Multimedia und Recht 2010, S. 300–303.

Ders.: Datenschutz-Compliance: Security Breach Notification bei Datenpannen, Corporate Compliance Zeitschrift 2010, S. 25–29.

Harte-Bavendamm, *Henning*/*Henning-Bodewig*, *Frauke* (Hrsg.): UWG, Gesetz gegen den unlauteren Wettbewerb, Kommentar, 3. Auflage, München 2013.

Hartmann, *Alexander*: Unterlassungsansprüche im Internet: Störerhaftung für nutzergenerierte Inhalte, München 2009.

Hatje, *Armin*: Die gemeinschaftsrechtliche Steuerung der Wirtschaftsverwaltung: Grundlagen, Erscheinungsformen, verfassungsrechtliche Grenzen am Beispiel der Bundesrepublik Deutschland, Baden-Baden 1998.

Hayek, *Friedrich von*: The Use of Knowledge, The American Economic Review, Volume 35 (1945), S. 519–530.

Ders.: Die Theorie komplexer Phänomene, in: Kerber, Wolfgang (Hrsg.), Die Anmaßung von Wissen, Tübingen 1996, S. 281–306.

Heckel, *Christian*: Behördeninterne Geheimhaltung, Neue Zeitschrift für Verwaltungsrecht 1994, S. 224–229.

Heckmann, *Dirk*: Rechtspflichten zur Gewährleistung von IT-Sicherheit im Unternehmen – Maßstäbe für ein IT-Sicherheitsrecht, MultiMedia und Recht 2006, S. 280–285.

Heidrich, *Joerg*/*Wegener*, *Christoph*: Datenschutzrechtliche Aspekte bei der Weitergabe von IP-Adressen, Datenschutz und Datensicherheit 2010, S. 172–177.

Heimburg, *Sibylle von*: Verwaltungsaufgaben und Private: Funktionen und Typen der Beteiligung Privater an öffentlichen Aufgaben unter besonderer Berücksichtigung des Baurechts, Berlin 1982.

Heinickel, *Caroline*/*Feiler*, *Lukas*: Der Entwurf für ein IT-Sicherheitsgesetz – europarechtlicher Kontext und die (eigentlichen) Bedürfnisse der Praxis, Computer und Recht 2014, S. 708–714.

Heinson, *Dennis*: Compliance durch Datenabgleiche, Betriebs-Berater 2010, S. 3084–3090.

Heintzen, *Markus*: Behördliches Informationshandeln bei ungewissem Sachverhalt, Natur und Recht 1991, S. 301–306.

Helmbrecht, *Udo*: Öffentliche Anhörung von Sachverständigen zum Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes BT-Drucksache 16/11967, Innenausschuss Wortprotokoll 94. Sitzung, Protokoll Nr. 16/94.

Henning, *Brita*: Wissenszurechnung im Verwaltungsrecht. Am Beispiel der verwaltungsrechtlichen Regelungen der Ausschlußfristen bei der Rücknahme und dem Widerruf von Verwaltungsakten, Baden-Baden 2003.

Herdegen, *Matthias*: Price Stability and Budgetary Restraints in the Economic and Monetary Union: the Law as Guardian of Economic Wisdom, Common Market Law Review 1998, S. 9–32.

Hermes, *Georg*: Staatliche Infrastrukturverantwortung: rechtliche Grundstrukturen netzgebundener Transport- und Übertragungssysteme zwischen Daseinsvorsorge und Wettbewerbsregulierung am Beispiel der leitungsgebundenen Energieversorgung in Europa, Tübingen 1998.

Hermes, *Georg*: Abhängige und unabhängige Verwaltungsbehörden – ein Überblick über die Bundesverwaltung, in: Masing, Johannes, Marcou, Gérard (Hrsg.), Unabhängige Regulierungsbehörden: Organisationsrechtliche Herausforderungen in Frankreich und Deutschland, Tübingen 2010, S. 53–86.

Herrmann, *Stephanie*: Informationspflichten gegenüber der Verwaltung: dargestellt am Recht der Gefahrenabwehr, Frankfurt am Main 1997.

Herzmann, *Karsten*: Konsultationen: eine Untersuchung von Prozessen kooperativer Maßstabskonkretisierung in der Energieregulierung, Tübingen 2010.

Heun, *Sven-Erik*: Einführung: Grundlagen und Struktur des TKG, Marktzutritt und Übergangsrecht, in: Ders. (Hrsg.), Handbuch Telekommunikationsrecht, 2. Auflage, Köln 2015.

Ders.: IT-Unternehmen als Telekommunikationsanbieter, Computer und Recht 2008, S. 79–85.

Ders.: Das neue Telekommunikationsgesetz 2004, Computer und Recht 2004, S. 893–907.

Heußner, *Kristina*: Informationssysteme im Europäischen Verwaltungsverbund, Tübingen 2007.

Hill, *Jonah Force*: Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers, Berkman Center Research Paper; Harvard Belfer Center for Science and International Affairs Working Paper, 2012, online abrufbar: http://ssrn.com/abstract=2439486 (zuletzt abgerufen am 30. April 2017).

Hillenbrand-Beck, *Renate*: Datenschutzkontrolle – Aufsichtsbehörden, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003, Kapitel 5.4., S. 816–850.

Hillgruber, *Christian*/*Epping*, *Volker* (Hrsg.): Beck'scher Online-Kommentar Grundgesetz, 27. Edition, München, Stand: 01.03.2015.

Hirschfeld Davis, *Julie*: Hacking of Government Computers Exposed 21.5 Million People, New York Times vom 09.07.2015, online abrufbar: http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html?_r=0 (zuletzt abgerufen am 30. April 2017).

Hobe, *Stephan*: Cyberspace – der virtuelle Raum, in: Isensee, Josef, Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts, Band XI: Bundesstaat, 3. Auflage, Heidelberg 2009, § 231, S. 249–274.

Höhne, *Focke*: Benachrichtigungspflichten bei unrechtmäßiger Kenntniserlangung von Daten durch Dritte – Informationspflichten bei Datenpannen nach der BDSG-Novelle II gemäß § 42a BDSG, § 15a TMG und § 93 Abs. 3 TKG, juris Praxisreport-IT-Recht 20/2009 Anmerkung 3.

Hoeren, *Thomas*: Tractatus germanico-informaticus – Some Fragmentary Ideas on DRM und information law, in: Lodder, Arno, Meijboom, Alfred, Osterbaan, Dinant (Hrsg.), IT Law – The Global Future: Achievements, Plans and Ambitions, Papers from the 20th anni-

versary International IFCLA conference, Amsterdam, June 1 and 2, 2006, Amsterdam 2006, S. 149–160.

Ders.: Das Telemediengesetz, Neue Juristische Wochenschrift 2007, S. 801–806.

Ders.: Anonymität im Web – Grundfragen und aktuelle Entwicklungen, Zeitschrift für Rechtspolitik 2010, S. 251–253.

Ders.: Internet und Recht – Neue Paradigmen des Informationsrechts, Neue Juristische Wochenschrift 1998, S. 2849–2854.

Ders. (Hrsg.): Big Data und Recht, München 2014.

Hoffmann-Riem, *Wolfgang*: Verfahrensprivatisierung als Modernisierung, Deutsches Verwaltungsblatt 1996, S. 225–232.

Ders.: Verwaltungsrecht in der Informationsgesellschaft – Einleitende Problemskizze, in: Hoffmann-Riem, Wolfgang, Schmidt-Aßmann, Eberhard (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, Baden-Baden 2000, S. 9–58.

Ders.: Strukturen des Europäischen Verwaltungsrechts – Perspektiven der Systembildung, in: Schmidt-Aßmann, Eberhard, Hoffmann-Riem, Wolfgang (Hrsg.), Strukturen des Europäischen Verwaltungsrechts, Baden-Baden 1999, S. 317–382.

Ders.: Wissen als Risiko – Unwissen als Chance, in: Augsberg, Ino (Hrsg.), Ungewissheit als Chance, Tübingen 2009, S. 17–38.

Ders.: Eigenständigkeit der Verwaltung, in: Hoffmann-Riem, Wolfgang, Schmidt-Aßmann, Eberhard, Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts, Band I: Methoden – Maßstäbe – Aufgaben – Organisation, 2. Auflage, München 2012, § 10, S. 677–778.

Ders.: Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JuristenZeitung 2008, S. 1009–1022.

Ders.: Regulierungswisssen in der Regulierung, in: Bora, Alfons, Reinhardt, Carsten, Henkel, Anna (Hrsg.), Wissensregulierung und Regulierungswissen, Weilerswist 2014, S. 135–156.

Ders.: Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 22. Mai 2014, MAT-A SV 2/1 neu zu A-Drs. 54, abrufbar unter: https://www.bundestag.de/blob/280846/04f34c512c86876b06f7c162e673f2db/mat_a_sv-2-1neu--pdf-data.pdf (zuletzt abgerufen am 30. April 2017).

Hofmann, *Ekkehard*: Externer Sachverstand im Verwaltungsverfahren, in: Spiecker gen. Döhmann, Indra, Collin, Peter (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, Tübingen 2008, S. 176–195.

Hofmann, *Herwig*/*Rowe*, *Gerard*/*Türk*, *Alexander*: Administrative law and policy of the European Union, Oxford 2011.

Hofmann, *Herwig*/*Türk*, *Alexander*: Policy implementation, in: Hofmann, Herwig, Türk, Alexander (Hrsg.), EU Administrative Governance, Cheltenham, UK, Northampton, MA, USA 2006. S. 74–112.

Hofmann, *Jeanette*: (Trans-)Formations of Civil Society in Global Governance Contexts – Two case studies on the problem of self-organization, in: Schuppert, Gunnar Folke (Hrsg.), Global Governance and the Role of Non-State Actors, Baden-Baden 2006, S. 179–202.

Dies.: Internet Governance: Eine regulative Idee auf der Suche nach ihrem Gegenstand, in: Schuppert, Gunnar Folke (Hrsg.), Governance-Forschung – Vergewisserung über Stand und Entwicklungslinien, Baden-Baden 2005, S. 277–301.

Dies.: Constellations of Trust and Distrust in Internet Governance, in: Report of the Expert Group ‚Risks of Eroding Trust – Foresight on the Medium-Term Implications for European Research and Innovation Policies (TRUSTFORESIGHT)', Europäische Kommission, Brüssel 2015, online abrufbar: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2608414 (zuletzt abgerufen am 30. April 2017).

Holznagel, *Bernd*: Die Erhebung von Marktdaten im Wege des Auskunftsersuchens nach dem TKG: Befugnisse der Regulierungsbehörde für Telekommunikation und Post, München 2001.

Ders.: Informationsbeziehungen in und zwischen Behörden, in: Hoffmann-Riem, Wolfgang, Schmidt-Aßmann, Eberhard, Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts, Band II: Informationsordnung – Verwaltungsverfahren – Handlungsformen, 2. Auflage, München 2012, § 24, S. 321–364.

Ders./*Schulz*, *Christian*: Die Auskunftsrechte der Regulierungsbehörde aus § 72 TKG und § 45 PostG, MultiMedia und Recht 2002, S. 364–370.

Hombergs, *Anne*: Europäisches Verwaltungskooperationsrecht auf dem Sektor der elektronischen Kommunikation, Münster 2006.

Horchert, *Judith*: E-Mail- Check beim BSI: Verunsicherte Bürger legen Behördenseite lahm, Spiegel Online, 21.01.2014, online abrufbar: http://www.spiegel.de/netzwelt/web/online-konten-geknackt-mail-adressen-check-beim-bsi-in-der-kritik-a-944739.html (zuletzt abgerufen am 30. April 2017).

Hornung, *Gerrit*: Ein neues Grundrecht, Computer und Recht 2008, S. 299–306.

Ders.: Informationen über „Datenpannen" – Neue Pflichten für datenverarbeitende Unternehmen, Neue Juristische Wochenschrift 2010, S. 1841–1845.

Ders.: Neue Pflichten für Betreiber kritischer Infrastrukturen: Das IT-Sicherheitsgesetz des Bundes, Neue Juristische Wochenschrift 2015, S. 3334–3340.

Ders.: Die Krypto-Debatte: Wiederkehr einer Untoten, MultiMedia und Recht 2015, S. 145–146.

Ders.: Stellungnahme zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages am 20. April 2015 zum Gesetzentwurf der Bundesregierung für das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 25. Februar 2015, Ausschussdrucksache 18(4)284 G, 18. April 2015, online abrufbar: https://www.bundestag.de/blob/370484/06b3a5ce693527f16886863d502ea7ca/18-4-284-g-data.pdf (zuletzt abgerufen am 30. April 2017).

Ders./*Schnabel*, *Christoph*: Verfassungsrechtlich nicht schlechthin verboten – Das Urteil des Bundesverfassungsgerichts in Sachen Vorratsdatenspeicherung, Deutsches Verwaltungsblatt 2010, S. 824–833.

Huber, *Bertold*: Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite, Neue Juristische Wochenschrift 2013, S. 2572–2577.

Ders.: BND-Gesetzreform – gelungen oder nachbesserungsbedürftig?, in: Zeitschrift für Rechtspolitik 2016, S. 162–167.

Huber, *Edith*/*Hellwig*, *Otto*/*Quirchmayr*, *Gerald*: Wissensaustausch und Vertrauen unter Computer Emergency Response Teams – eine europäische Herausforderung, in: Datenschutz und Datensicherheit 2016, S. 162–166.

Hunziker, *Stefan*/*Rihs*, *Simon*: Risikoexposition bei Einsatz von Open-Source und proprietären Browsern, Datenschutz und Datensicherheit 2006, S. 332–338.

Hutter, *Michael*: Global Regulation oft he Internet Domain Name System: Five Lessons from the ICANN Case, in: Ladeur, Karl-Heinz (Hrsg.), Innovationsoffene Regulierung des Internets – Neues Recht für Kommunikationsnetzwerke, Baden-Baden 2003, S. 39–52.

Immenga, *Ulrich*/*Mestmäcker*, *Ernst-Joachim* (Hrsg.): Wettbewerbsrecht, Band 2: GWB/Teil 1: §§ 1–96, 130, 131, Kommentar zum Deutschen Kartellrecht, 5. Auflage, München 2014.

Ingold, *Albert*: Desinformationsrecht: Verfassungsrechtliche Vorgaben für staatliche Desinformationstätigkeit, Berlin 2011.

Internet & Gesellschaft Collaboratory (Hrsg.): Offene Staatskunst – Bessere Politik durch „Open Government"?, Abschlussbericht Oktober 2010, 1. Auflage, Berlin 2010.

Irion, *Kristina*: The Governance of Network and Information Security in the European Union: The European Public-Private Partnership for Resilience (EP3R), in: Gaycken, Sandro, Krüger, Jörg, Nickolay, Bertram, The Secure Information Society: Ethical, Legal and Political Challenges, Berlin 2013, S. 83–116.

Jaeger, *Wolfgang*/*Kokott*, *Juliane*/*Pohlmann*, *Petra*/*Schroeder*, *Dirk*: Frankfurter Kommentar zum Kartellrecht, 87. Lieferung, Köln 2016.

Jäger, *Thomas*/*Daun*, *Anna* (Hrsg.): Geheimdienste in Europa: Transformation, Kooperation und Kontrolle, Wiesbaden 2009.

Janda, *Timm*: Open Government – Transparenz, Partizipation und Kollaboration als Staatsleitbild, in: Schliesky, Utz, Schulz, Sönke (Hrsg.), Transparenz, Partizipation, Kollaboration – Web 2.0 für die öffentliche Verwaltung, Kiel 2012, S. 11–39.

Jandt, *Silke*/*Laue*, *Philip*: Voraussetzungen und Grenzen der Profilbildung bei Location Based Services, Kommunikation und Recht 2006, S. 316–322.

Jann, *Werner*: Kategorien der Policy-Forschung, Speyer 1981.

Jarass, *Hans*: Charta der Grundrechte der Europäischen Union, Kommentar, 2. Auflage, München 2013.

Ders.: Bundesimmissionsschutzgesetz, Kommentar, 11. Auflage, München 2015.

Ders./*Pieroth*, *Bodo* (Hrsg.): Grundgesetz für die Bundesrepublik Deutschland: Kommentar, 13. Auflage, München 2014.

Jastrow, *Serge-Daniel*/*Schlatmann*, *Arne*: Informationsfreiheitsgesetz – IFG, Kommentar, Heidelberg, München 2006.

Jestaedt, *Matthias*: Demokratieprinzip und Kondominialverwaltung: Entscheidungsteilhabe Privater an der öffentlichen Verwaltung auf dem Prüfstand des Verfassungsprinzips Demokratie, Berlin 1993.

Jolls, *Christine*/*Sunstein*, *Cass*/*Thaler*, *Richard*: A Behavioral Approach to Law and Economics, Stanford Law Review 50 (1998), S. 1471–1550.

Jung, *Volker*/*Warnecke*, *Hans-Jürgen*: Handbuch für die Telekommunikation, Berlin 2014.

Kahl, *Wolfgang*: Der Europäische Verwaltungsverbund: Strukturen – Typen – Phänomene, Der Staat 50 (2011), S. 353–387.

Ders.: Europäisches und nationales Verwaltungsorganisationsrecht. Von der Konfrontation zur Kooperation, Die Verwaltung 29 (1996), S. 341–384.

Kahnemann, *Daniel*/*Tversky*, *Amos*: Prospect Theory: An Analysis of Decision under Risk, Econometrica 47 (1979), S. 263–292.

Kahrl, *Frederic*: Das Kritische an den kritischen Infrastrukturen, Die Öffentliche Verwaltung 2009, S. 535–537.

Kaiser, *Anna-Bettina*: Die Kommunikation der Verwaltung. Diskurse zu den Kommunikationsbeziehungen zwischen staatlicher Verwaltung und Privaten in der Verwaltungsrechtswissenschaft der Bundesrepublik Deutschland, Baden-Baden 2009.

Dies.: Wissensmanagement im Mehrebenensystem, in: Schuppert, Gunnar Folke, Voßkuhle, Andreas (Hrsg.), Governance von und durch Wissen, Baden-Baden 2009, S. 217–239.

Karg, *Moritz*: Anmerkung zum Urteil des BGH vom 13.01.2011, III ZR 146/10 – Befugnisse nach § 100 Abs. 1 TKG, MultiMedia und Recht 2011, S. 345–346.

Kaufhold, *Ann-Katrin*: Gegenseitiges Vertrauen. Wirksamkeitsbedingungen und Rechtsprinzip der justiziellen Zusammenarbeit im Raum der Freiheit, Sicherheit und des Rechts, Europarecht 2012, S. 408–432.

Keppeler, *Lutz Martin*: Was bleibt vom TMG-Datenschutz nach der DS-GVO?, MultiMedia und Recht 2015, S. 779–783.

Kette, *Sven*: Bankenregulierung als Cognitive Governance: eine Studie zur gesellschaftlichen Verarbeitung von Komplexität und Nichtwissen, Wiesbaden 2008.

King, *Steven E.*: Science of Cyber-Security, The MITRE Corporation, Studie im Auftrag des United States Department of Defense, McLean (Virginia), 2010, online abrufbar: https://fas.org/irp/agency/dod/jason/cyber.pdf (zuletzt abgerufen am 30. April 2017).

Kingreen, *Thorsten*: Das Sozialstaatsprinzip im europäischen Verfassungsverbund: gemeinschaftsrechtliche Einflüsse auf das deutsche Recht der gesetzlichen Krankenversicherung, Tübingen 2003.

Ders./Kühling, *Jürgen*: Weniger Schutz durch mehr Recht: Der überspannte Parlamentsvorbehalt im Datenschutzrecht, JuristenZeitung 2015, S. 213–221.

Kircher, *Philipp*: Gesundheitswesen, in: Kingreen, Thorsten, Kühling, Jürgen (Hrsg.) Gesundheitsdatenschutzrecht, Baden-Baden 2015, S. 186–277.

Kirchhof, *Gregor*: Nudging – zu den rechtlichen Grenzen informalen Verwaltens, Zeitschrift für Rechtspolitik 2015, S. 136–137.

Klein, *Eckart*: Die verfassungsrechtliche Problematik des ministerialfreien Raumes: ein Beitrag zur Dogmatik der weisungsfreien Verwaltungsstellen, Berlin 1974.

Kleinwächter, *Wolfgang*: Internet Governance – die kontroverse des WSIS: Eine globale Ressource im Spannungsfeld nationaler Interessen, Medienheft 2005, Dossier 24, online abrufbar: http://www.medienheft.ch/dossier/bibliothek/d24_KleinwaechterWolfgang.pdf (zuletzt abgerufen am 30. April 2017).

Klindt, *Thomas* (Hrsg.): ProdSG: Produktsicherheitsgesetz, Kommentar, 2. Auflage, München 2015.

Kloepfer, *Michael*: Informationsrecht, München 2002.

Ders.: Datenschutz als Grundrecht: Verfassungsprobleme der Einführung eines Grundrechts auf Datenschutz, Königstein im Taunus 1980.

Ders.: Staatliche Informationen als Lenkungsmittel: dargestellt insbesondere am Problem behördlicher Warnungen und Empfehlungen im Umweltrecht, Berlin 1998.

Ders.: Informationsfreiheitsgesetz und Schutz von Betriebs- und Geschäftsgeheimnissen – Betriebs- und Geschäftsgeheimnisse in verschiedenen Rechtsgebieten und verschiedenen Kontexten, Rechtsgutachten im Auftrag des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Juni 2011, online abrufbar: http://www.bfdi.bund.de/SharedDocs/VortraegeUndArbeitspapiere/GutachtenIFGKloepfer.pdf?__blob=publicationFile (zuletzt abgerufen am 30. April 2017).

Ders./Schärdel, *Florian*: Grundrechte für die Informationsgesellschaft – Datenschutz und Informationszugangsfreiheit ins Grundgesetz?, JuristenZeitung 2009, S. 453–462.

Ders./Lewinski, *Kai von*: Das Informationsfreiheitsgesetz des Bundes (IFG), Deutsches Verwaltungsblatt 2005, S. 1277–1288.

Ders./Greve, *Holger*: Das Informationsfreiheitsgesetz und der Schutz von Betriebs- und Geschäftsgeheimnissen, Neue Zeitschrift für Verwaltungsrecht 2011, S. 577–584.

Klußmann, *Niels*: Lexikon der Kommunikations- und Informationstechnik, Neuausgabe, Heidelberg, München 2003.

Kluth, *Winfried*: Die Strukturierung von Wissensgenerierung durch das Verwaltungsorganisationsrecht, in: Spiecker gen. Döhmann, Indra, Collin, Peter (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, Tübingen 2008, S. 73–100.

Kment, *Martin*: Grenzüberschreitendes Verwaltungshandeln: transnationale Elemente deutschen Verwaltungsrechts, Tübingen 2010.

Koenig, *Christian*/*Loetz*, *Sascha*/*Neumann*, *Andreas*: Telekommunikationsrecht, Stuttgart 2004.

Ders./*Neumann*, *Andreas*: Telekommunikationsrechtliche Ansprüche auf Leistungen der Fakturierung und des Inkassos für Internet-by-Call-Dienstleistungen, Kommunikation & Recht 2004, Beilage 3, S. 1–31.

Ders./*Neumann*, *Andreas*: Die neue Top-Level-Domain „.eu" als Beitrag zum Auf- und Ausbau transeuropäischer Netze?, Europäische Zeitschrift für Wirtschaftsrecht 2002, S. 485–490.

Ders./*Braun*, *Jens-Daniel*: Defizite des deutschen Telekommunikationsrechts im Blick auf die Internet-Märkte und Abhilfemöglichkeiten, Kommunikation & Recht-Beilage 2/2002, S. 1–53.

Könen, *Andreas*: IT-Sicherheit gesetzlich geregelt, in: Datenschutz und Datensicherheit 2016, S. 12–16.

König, *Wolfgang*/*Popescu-Zeletin*, *Radu*/*Schliesky*, *Utz*: IT- und Internet als kritische Infrastruktur – Vernetzte Sicherheit zum Schutz kritischer Infrastrukturen, Kiel 2014.

Kommission der Europäischen Gemeinschaft (Hrsg.): Weißbuch Wachstum, Wettbewerbsfähigkeit und Beschäftigung – Herausforderungen der Gegenwart und Wege ins 21. Jahrhundert, Brüssel 1993.

Kopp, *Ferdinand*/*Ramsauer*, *Ulrich* (Hrsg.): Verwaltungsverfahrensgesetz: VwVfG, Kommentar, 16. Auflage, München 2015.

Koppensteiner, *Franz*: Die Transparenzverordnung im Wandel der Zeit, Europarecht 2014, S. 594–617.

KPGM: IT-Sicherheit in Deutschland, Handlungsempfehlungen für eine zielorientierte Umsetzung des IT-Sicherheitsgesetzes, Berlin 2014, online abrufbar: http://bdi.eu/media/presse/publikationen/KPMG_IT-Sicherheit_in_Deutschland.pdf (zuletzt abgerufen am 30. April 2017).

Krämer, *Sybille*: Medium, Bote, Übertragung: Kleine Metaphysik der Medialität, Frankfurt am Main 2008.

Kremer, *Sascha*: Datenschutz bei Entwicklung und Nutzung von Apps für Smart Devices, Computer und Recht 2012, S. 438–446.

Ders./*Völkel*, *Christian*: Cloud Storage und Cloud Collaboration als Telekommunikationsdienste, Computer und Recht 2015, S. 501–505.

Kropp, *Cordula*/*Wagner*, *Jost*: Wissensaustausch in Entscheidungsprozessen: Kommunikation an der Schnittstelle von Wissenschaft und Agrarpolitik, in: Mayntz, Renate, Neidhardt, Friedhelm, Weingart, Peter, Wengenroth, Ulrich (Hrsg.), Wissensproduktion und Wissenstransfer: Wissen im Spannungsfeld von Wissenschaft, Politik und Öffentlichkeit, Bielefeld 2008, S. 173–196.

Krüger, *Stefan*/*Maucher*, *Svenja-Ariane*: Ist die IP-Adresse wirklich ein personenbezogenes Datum? – Ein falscher Trend mit großen Auswirkungen auf die Praxis, MultiMedia und Recht 2011, S. 433–439.

Kühling, *Jürgen*: Europäisches Telekommunikationsverwaltungsrecht, in: Terhechte, Jörg Philipp (Hrsg.), Verwaltungsrecht der Europäischen Union, Baden-Baden 2011, § 24, S. 881–930.

Ders.: Das Ende der Privatheit, in: Müller-Heidelberg, Till, Finckh, Ulrich, Steven, Elke, Rogalla, Bela, Micksch, Jürgen, Kaleck, Wolfgang, Kutscha, Martin (Hrsg.), Grundrechte-Report 2003: Zur Lage der Bürger- und Grundrechte in Deutschland, Hamburg 2003, S. 15–23.

Ders.: Der Fall der Vorratsdatenspeicherungsrichtlinie und der Aufstieg des EuGH zum Grundrechtsgericht, Neue Zeitschrift für Verwaltungsrecht 2014, S. 681–685.

Ders./*Seidel*, *Christian*/*Sivridis*, *Anastasios*: Datenschutzrecht, 3. Auflage, Heidelberg 2015.

Ders./*Biendl*, *Michael*/*Schall*, *Tobias*: Telekommunikationsrecht, 2. Auflage, Heidelberg 2014.

Ders./*Schall*, *Tobias*: WhatsApp, Skype & Co. – OTT-Kommunikationsdienste im Spiegel des geltenden Telekommunikationsrechts, Computer und Recht 2015, S. 641–655.

Ders./*Sivridis*, *Anastasios*/*Schuchow*, *Mathis*/*Burghardt*, *Thorben*: Das datenschutzrechtliche Vollzugsdefizit im Bereich der Telemedien – ein Schreckensbericht, Datenschutz und Datensicherheit 2009, S. 335–342.

Kugelmann, *Dieter*: Polizei- und Ordnungsrecht, 2. Auflage, Berlin 2012.

Ders.: Wirkungen des EU-Rechts auf die Verwaltungsorganisation der Mitgliedstaaten, Verwaltungsarchiv 98 (2007), S. 78–100.

Ders.: Entwicklungstendenzen der Gewährleistung von Sicherheit in der Bundesrepublik Deutschland und der Europäischen Union, in: Würtenberger, Thomas, Gusy, Christoph, Lange, Hans-Jürgen (Hrsg.), Innere Sicherheit im europäischen Vergleich: Sicherheitsdenken, Sicherheitskonzepte und Sicherheitsarchitektur im Wandel, Berlin 2012, § 9, S. 169–173.

Ders.: Das Informationsfreiheitsgesetz des Bundes, Neue Juristische Wochenschrift 2005, S. 3609–3613.

Kujat, *Stefan*: Frühwarnsysteme zur Abwehr von Botnetzen, Passau 2010, online abrufbar: https://opus4.kobv.de/opus4-uni-passau/frontdoor/index/index/docId/205 (zuletzt abgerufen am 30. April 2017)

Kullik, *Jakob*: Vernetzte (Un-)Sicherheit: eine politisch-rechtliche Analyse der deutschen Cybersicherheitspolitik, Hamburg 2014.

Kuner, *Christopher*: Transborder Data Flows under Data Protection and Privacy Law, Oxford 2013.

Ders./*Hladjk*, *Jörg*: Rechtsprobleme der Kryptografie, in: Hoeren, Thomas, Sieber, Ulrich, Holznagel, Bernd (Hrsg.), Handbuch Multimedia-Recht, 42. Auflage, München 2015, Teil 17.

Kunkel, *Hanno*/*Rockstroh*, *Sebastian*: IT-Sicherheit in Produktionsumgebungen, in: Multimedia und Recht 2017, S. 77–82.

Kuran, *Timur*/*Sunstein*, *Cass*: Availability Cascades and Risk Regulation, Stanford Law Review 51 (1999), S. 683–768.

Kurose, *James*/*Ross*, *Keith*: Computer Networking: A Top-Down Approach, 6. Auflage, Upper Saddle River (NJ) 2013.

Kurth, *Matthias*: Eröffnungsbeitrag des Workshops: Bitstromzugang in Deutschland, Multimedia und Recht-Beilage 10/2003, S. 3–7.

Ders.: „Euro-Regulierer" durch die Hintertür?, MultiMedia und Recht 2009, S. 818–823.

Kurz, *Constanze*: Digitaler Schlachtplan: Agenda ohne Agenten, Frankfurter Allgemeine Zeitung, 22.8.2014, online abrufbar: http://www.faz.net/aktuell/feuilleton/aus-dem-maschinen raum/digitaler-schlachtplan-agenda-ohne-die-agenten-13110265.html (zuletzt abgerufen am 30. April 2017).

Kutscha, *Martin*: Innere Sicherheit und Verfassung, in: Roggan, Frederik, Kutscha, Martin (Hrsg.), Handbuch zum Recht der Inneren Sicherheit, 2. Auflage, Berlin 2006, S. 24–105.

Ladeur, *Karl-Heinz*: Postmoderne Rechtstheorie: Selbstreferenz – Selbstorganisation – Prozeduralisierung, 2. Auflage, Berlin 1995.

Ders.: Privatisierung öffentlicher Aufgaben und die Notwendigkeit der Entwicklung eines neuen Informationsverwaltungsrechts, in: Hoffmann-Riem, Wolfgang, Schmidt-Aßmann, Eberhard (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, Baden-Baden 2000, S. 225–256.

Ders.: Drittschutz des Entgeltregulierungsverfahrens nach §§ 23 ff. TKG?, Computer und Recht 2000, S. 433–441.

Ders.: Die Regulierung von Telekommunikation und Medien im Zeitalter ihrer Konvergenz: das Beispiel des Universal Mobile Telecommunications System (UMTS), Zeitschrift für das gesamte Recht der Telekommunikation 1999, S. 68–75.

Ders.: Der Staat der „Gesellschaft der Netzwerke". Zur Fortentwicklung des Paradigmas des „Gewährleistungsstaats", Der Staat 48 (2009), S. 163–192.

Ders.: Der Staat gegen die Gesellschaft: zur Verteidigung der Rationalität der „Privatrechtsgesellschaft", Tübingen 2006.

Ders.: Die Kommunikationsinfrastruktur der Verwaltung, in: Hoffmann-Riem, Wolfgang, Schmidt-Aßmann, Eberhard, Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts, Band II: Informationsordnung – Verwaltungsverfahren – Handlungsformen, 2. Auflage, München 2012, § 21, S. 35–106.

Ders.: Die Bedeutung des Allgemeinen Verwaltungsrechts für ein Europäisches Verwaltungsrecht, in: Trute, Hans-Heinrich, Groß, Thomas, Röhl, Hans Christian, Möllers, Christoph (Hrsg.), Allgemeines Verwaltungsrecht – Zur Tragfähigkeit eines Konzepts, Tübingen 2008, S. 795–820.

Ders.: Anmerkung zu einer Entscheidung des BVerfG, Beschluss vom 17.08.2010, 1 BvR 2585/06 – zur Reichweite des Persönlichkeitsschutzes gegen Äußerungen staatlicher Stellen, Zeitschrift für Urheber- und Medienrecht 2010, S. 960–961.

Ders.: Zur Kooperation von staatlicher Regulierung und Selbstregulierung des Internet, Zeitschrift für Urheber- und Medienrecht 1997, S. 372–384.

Lederer, *Beatrice*: Open Data: Informationsöffentlichkeit unter dem Grundgesetz, Berlin 2015.

Leendertz, *Ariane*: Das Komplexitätssyndrom, Gesellschaftliche „Komplexität" als intellektuelle und politische Herausforderung in den 1970er-Jahren, Max-Planck-Institut für Gesellschaftsforschung Discussion Paper 15/7, online abrufbar: http://www.mpifg.de/pu/mpifg_dp/dp15-7.pdf (zuletzt abgerufen am 30. April 2017).

Leible, *Stefan*/*Brzezinski*, *Katja*: Rechtsprechungsreport Lebensmittelrecht 2013, Wettbewerb in Recht und Praxis 2014, S. 276–285.

Leiner, *Barry*/*Cerf*, *Vinton*/*Clark*, *David*/*Kahn*, *Robert*/*Kleinrock*, *Leonard*/*Lynch*, *Daniel*, *Postel*, *Jon*/*Roberts*, *Larry*/*Wolff*, *Stephen*: Brief History of the Internet, 2012, online abrufbar: http://www.internetsociety.org/sites/default/files/Brief_History_of_the_Internet.pdf (zuletzt abgerufen am 20. April 2017).

Leisterer, *Hannfried*: Die neuen Pflichten zur Netz- und Informationssicherheit und die Verarbeitung personenbezogener Daten, Computer und Recht 2015, S. 665–670.

Ders./*Schneider*, Florian: Der überarbeitete Entwurf für ein IT-Sicherheitsgesetz, Überblick und Problemfelder, Computer und Recht 2014, S. 574–578.

Lem, *Stanislaw*: Summa technologiae, 6. Auflage, Frankfurt am Main 2003.

Lennartz, *Hans-Albert*: Probleme der Techniksteuerung durch Recht – am Beispiel des bundesdeutschen Datenschutzrechts (Teil 2), Recht der Datenverarbeitung 1990, S. 25–30.

Leopold, *Helmut*/*Bleier*, *Thomas*/*Skopik*, *Florian*: Vorwort der Herausgeber, in: Leopold, Helmut, Bleier, Thomas, Skopik, Florian (Hrsg.): Cyber Attack Information System: Erfahrungen und Erkenntnisse aus der IKT-Sicherheitsforschung, Berlin 2015, I–VIII.

Lepsius, *Oliver*: Steuerungsdiskussion, Systemtheorie und Parlamentarismuskritik, Tübingen 1999.

Ders.: Risikosteuerung durch Verwaltungsrecht: Ermöglichung oder Begrenzung von Innovationen?, Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer 63 (2004), S. 264–315.

Lessig, *Lawrence*: Code and Other Laws of Cyberspace, New York 1999.

Leupold, *Andreas*/*Glossner*, *Silke* (Hrsg.): Münchener Anwaltshandbuch IT-Recht, 3. Auflage, München 2013.

Leuschner, *Sebastian*: EuGH und Vorratsdatenspeicherung: Erfindet Europa ein Unionsgrundrecht auf Sicherheit?, Europarecht 2016, 431–452.

Levine, *David*: Professors' Letter in Opposition to the „Cybersecurity Information Sharing Act" (S. 754), 2015, online abrufbar: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2699761 (zuletzt abgerufen am 30. April 2017).

Lewinski, *Kai von*: Die Matrix des Datenschutzes: Besichtigung und Ordnung eines Begriffsfeldes, Tübingen 2014.

Ders.: Zur Geschichte von Privatsphäre und Datenschutz – eine rechtshistorische Perspektive, in: Schmidt, Jan-Hinrik, Weichert, Thilo (Hrsg.), Datenschutz: Grundlagen, Entwicklungen und Kontroversen, Bonn 2012, S. 23–33.

Ders.: Europäisierung des Datenschutzrechts, Datenschutz und Datensicherheit 2012, S. 564–570.

Ders.: Tätigkeitsberichte im Datenschutz, Recht der Datenverarbeitung 2004, S. 163–167.

Linke, *Tobias*: Rechtsfragen der Einrichtung und des Betriebs eines Nationalen Cyber-Abwehrzentrums als informelle institutionalisierte Sicherheitskooperation, Die Öffentliche Verwaltung 2015, S. 128–139.

Lisken, *Hans*/*Denninger*, *Erhard* (Hrsg.): Handbuch des Polizeirechts, 5. Auflage, München 2012.

Lodde, *Stephan*: Informationsrechte des Bürgers gegen den Staat, Köln, München 1996.

Loeser, *Roman*: Das Berichtswesen der öffentlichen Verwaltung: öffentliche Verwaltung im Rahmen unterschiedlicher Rechtsformen, Baden-Baden 1991.

Loewenstein, *George*/*Weber, Elke*/*Hsee*, *Christopher K.*/*Welch*, *Ned*: Risk as Feelings, Psychological Bulletin 127 (2001), S. 267–286.

Lombard, *Martine*: Warum bedient man sich im Bereich der Wirtschaft unabhängiger Behörden? Typologie ihrer Aufgaben, in: Masing, Johannes, Marcou, Gérard (Hrsg.), Unabhängige Regulierungsbehörden: Organisationsrechtliche Herausforderungen in Frankreich und Deutschland, Tübingen 2010, S. 143–170.

Lovet, *Guillaume*: Fighting cybercrime: Technical, juridical and ethical challenges, in: Virus Bulletin Conference Proceedings 2009, S. 63– 76.

Lowe, *Gavin*: An attack on the Needham-Schroeder public-key authentication protocol, Information Processing Letters 1995, Volume 56 Issue 3, S. 131–133, online abrufbar: http://web.cs.wpi.edu/~cs564/f12/papers/lowe95.pdf (zuletzt abgerufen am 30. April 2017).

Luch, *Anika*/*Schulz*, *Sönke*: Digitale Dimensionen der Grundrechte – Die Bedeutung der speziellen Grundrechte im Internet, MultiMedia und Recht 2013, S. 88–93.

Dies./*Schulz*, *Sönke*: Das Recht auf Internet als Grundlage der Online-Grundrechte, Kiel 2013.

Lucke, *Jörn von*/*Geiger*, *Christian*: Open Government Data: Frei verfügbare Daten des öffentlichen Sektors, Gutachten für die Deutsche Telekom AG zur T-City Friedrichshafen, Version vom 3.12.2010, online abrufbar: https://www.zu.de/institute/togi/assets/pdf/TICC-101203-OpenGovernmentData-V1.pdf (zuletzt abgerufen am 30. April 2017).

Ludwigs, *Markus*: Die Bundesnetzagentur auf dem Weg zur Independent Agency? Europarechtliche Anstöße und verfassungsrechtliche Grenzen, Die Verwaltung 44 (2011), S. 41–74.

Lüdemann, *Jörn*: Edukatorisches Staatshandeln: Steuerungstheorie und Verfassungsrecht am Beispiel der staatlichen Förderung von Abfallmoral, Baden-Baden 2004.

Luhmann, *Niklas*: Die Wissenschaft der Gesellschaft, Frankfurt am Main 2005.

Ders.: Soziologie des Risikos, unveränderter Nachdruck der Ausgabe von 1991, Berlin 2003.

Ders.: Organisation und Entscheidung, Opladen 2000.

Ders.: Vertrauen: ein Mechanismus der Reduktion sozialer Komplexität, 5. Auflage, Konstanz 2014.

Lurz, *Hanna*/*Scheben*, *Barbara*/*Dolle*, *Wilhelm*: Das IT-Sicherheitsgesetz: Herausforderungen und Chancen für Unternehmen – vor allem für KMU, Betriebs-Berater 2015, S. 2755–2762.

Maaßen, *Hans-Georg*: „Cyberwar – eine reale Gefahr aus der virtuellen Welt", Privacy in Germany 2015, S. 137–212.

Majone, *Giandomenico*: The New European Agencies: Regulation by Information, Journal of European Public Policy 1997, S. 262–275.

Ders.: Mutual Trust, Credible Commitments and the Evolution of Rules for a Single European Market, European University Institute Robert Schuman Centre for Advanced Studies Working Paper 1995.

Manssen, *Gerrit*: Telekommunikations- und Multimediarecht, 36. Auflage, Berlin 2015.

Mantz, *Reto*: Anmerkung zum Urteil des LG Berlin vom 31.01.2013, 57 S 87/08 – Zur Qualifizierung von IP-Adressen als personenbezogene Daten, Zeitschrift für Datenschutz 2013, S. 625–626.

Ders.: Anmerkung zu einer Entscheidung des LG München I, Urteil vom 12.01.2012, 17 HK O 1398/11 – Zur Frage der Zulässigkeit und der Verpflichtung des Anbieters von kostenlosen Hot Spot-Diensten zur Speicherung von Informationen zur Identifizierung von Nutzern, Computer und Recht 2012, S. 605–606.

Marly, *Anna-Lena*/*Wirz*, *Jochen*: Die Verbreitung digitaler Güter, in: Europäische Zeitschrift für Wirtschaftsrecht 2017, S. 16–19.

Martini, *Mario*/*Zimmermann*, *Georg von*: Voice over IP am regulatorischen Scheideweg, Computer und Recht 2007, S. 368–373.

Dies.: E-Mail und integrierte VoIP-Services: Telekommunikationsdienste i. S. des § 3 Nr. 24 TKG?, Computer und Recht 2007, S. 427–431.

Masing, *Johannes*: Transparente Verwaltung – Konturen eines Informationsverwaltungsrechts, Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer 63 (2004), S. 377–441.

Ders.: Unabhängige Behörden und ihr Aufgabenprofil, in: Masing, Johannes, Marcou, Gérard (Hrsg.), Unabhängige Regulierungsbehörden: Organisationsrechtliche Herausforderungen in Frankreich und Deutschland, Tübingen 2010, S. 181–219.

Maunz, *Theodor*/*Dürig*, *Günter* (Hrsg.): Grundgesetz, Band I: Art. 1–5, 75. Auflage, München 2015.

Ders./ders. (Hrsg.): Grundgesetz, Band II: Art. 6–15, 75. Auflage, München 2015.

Ders./ ders. (Hrsg.): Grundgesetz, Band IV: Art. 28–69, 75. Auflage, München 2015.

Mayer, *Franz Christian*: Europäisches Internetverwaltungsrecht, in: Terhechte, Jörg Philipp (Hrsg.), Verwaltungsrecht in der Europäischen Union, Baden-Baden 2011, § 25, S. 931–958.

Mayer-Schönberger, *Viktor*: The Authority of Law in Times of Cyberspace, Journal of Law, Technology and Policy, Vol. 1(1), S. 1–23.

Mehrbrey, *Kim Lars*/*Schreibauer*, *Marcus*: Haftungsverhältnisse bei Cyber-Angriffen – Ansprüche und Haftungsrisiken von Unternehmen und Organen, MultiMedia und Recht 2016, S. 75–82.

Meister, *Andre*: Geheime Kommunikation: BSI programmierte und arbeitete aktiv am Staatstrojaner, streitet aber Zusammenarbeit ab, netzpolitik.org, 16.03.2015, online abrufbar: https://netzpolitik.org/2015/geheime-kommunikation-bsi-programmierte-und-arbeite te-aktiv-am-staatstrojaner-streitet-aber-zusammenarbeit-ab/ (zuletzt abgerufen am 30. April 2017).

Meyer, *Jürgen* (Hrsg.): Charta der Grundrechte der Europäischen Union, 4. Auflage, Baden-Baden 2014.

Meyerdierks, *Per*/*Gendelev*, *Boris*: Anmerkung zum Urteil des LG Berlin vom 31.01.2013, 57 S 87/08 – Zur Frage, ob dynamische IP-Adressen personenbezogene Daten darstellen, Zeitschrift für Datenschutz 2013, S. 626–628.

Michalski, *Lutz* (Hrsg.): GmbHG, Band 1: Systematische Darstellungen §§ 1–34 GmbHG, 2. Auflage, München 2010.

Microsoft: Linux im Handel – Was jeder Händler wissen sollte, Whitepaper 2001.

Möllers, *Christoph*: Der vermisste Leviathan: Staatstheorie in der Bundesrepublik, Frankfurt am Main 2008.

Ders.: Materielles Recht – Verfahrensrecht – Organisationsrecht. Zu Theorie und Dogmatik dreier Dimensionen des Verwaltungsrechts, in: *Trute*, Hans-Heinrich, Gross, Thomas, Röhl, Christian, Möllers, Christoph (Hrsg.), Allgemeines Verwaltungsrecht – zur Tragfähigkeit eines Konzepts, Tübingen 2008, S. 525–550.

Ders.: Transnationale Behördenkooperation. Verfassungs- und völkerrechtliche Probleme transnationaler administrativer Standardsetzung, Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 65 (2005), S. 351–389.

Ders.: Gewaltengliederung – Legitimation und Dogmatik im nationalen und übernationalen Rechtsvergleich, Tübingen 2005.

Ders.: Theorie, Praxis und Interdisziplinarität in der Verwaltungsrechtswissenschaft, Verwaltungsarchiv 93 (2002), S. 22–60.

Ders./*Pflug*, *Ludger*: Verfassungsrechtliche Rahmenbedingungen des Schutzes kritischer IT-Infrastrukturen, in: Kloepfer, Michael (Hrsg.), Schutz kritischer Infrastrukturen, Baden-Baden 2010, S. 47–66.

Ders./*Terhechte*, *Jörg Phillip*: Europäisches Verwaltungsrecht und Internationales Verwaltungsrecht, in: Terhechte, Jörg Philipp (Hrsg.), Verwaltungsrecht der Europäischen Union, Baden-Baden 2011, § 40, S. 1437–1452.

Möstl, *Markus*: Hoheitliche Verbraucherinformation – Grundfragen und aktuelle Entwicklungen, Lebensmittel und Recht 2015, S. 185–192.

Ders.: Informationsinteresse und Geheimhaltungsbedürfnis als Antipoden im Verbraucherinformationsgesetz?, in: Leible, Stefan (Hrsg.), Verbraucherschutz durch Information im Lebensmittelrecht, Bayreuth 2010, S. 149–167.

Monopolkommission: Sondergutachten 68, Wettbewerbspolitik: Herausforderung digitaler Märkte, Bonn 2015.

Dies.: Sondergutachten 66, Telekommunikation 2013: Vielfalt auf den Märkten erhalten, Bonn 2013.

Montesquieu, *Charles de Secondat*: De l'esprit des lois, 1748.

Müller-Broich, *Jan Dominik*: Telemediengesetz, Baden-Baden 2012.

Needham, *Roger*/*Schroeder*, *Michael*: Using encryption for authentication in large networks of computers, Communication of the ACM 1978, S. 993–999.

Nehm, *Kay*: Das nachrichtendienstliche Trennungsgebot und die neue Sicherheitsarchitektur, Neue Juristische Wochenschrift 2004, S. 3289–3295.

Neumann, *Linus*: Chaos Computer Club – Stellungnahme zum Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), Ausschussdrucksache 18(4)284 F, 17. April 2015, online abrufbar: https://www.bundestag.de/blob/370474/011e1de4b10d93d5f9ae9d2e586cf6b3/18-4-284-f-data.pdf (zuletzt abgerufen am 30. April 2017).

Ders.: Chaos Computer Club – Effektive IT-Sicherheit fördern, Stellungnahme zur 7. Sitzung des Ausschusses Digitale Agenda des Deutschen Bundestages, Ausschussdrucksache 18(24)11, 7. Mai 2014, online abrufbar: http://www.bundestag.de/blob/278506/7bfa0b746372768036e3780f49b96ae0/stellungnahme_linus_neumann-pdf-data.pdf (zuletzt abgerufen am 30. April 2017).

Nolan, *Andrew*: Cybersecurity and Information Sharing: Legal Challenges and Solutions, Congressional Research Service, 2015, online abrufbar: https://www.fas.org/sgp/crs/intel/R43941.pdf (zuletzt abgerufen am 30. April 2017).

Nußberger, *Angelika*: Sachverständigenwissen als Determinante verwaltungsrechtlicher Einzelentscheidungen, Archiv des öffentlichen Rechts 129 (20049, S. 282–307.

Oerting, *Troels*: Das Europäische Cybercrime Centre (EC3) bei Europol, Kriminalistik 12 2012, S. 705–706.

Ohler, *Christoph*: Europäisches und nationales Verwaltungsrecht, in: Terhechte, Jörg Philipp (Hrsg.), Verwaltungsrecht der Europäischen Union, Baden-Baden 2011, § 9, S. 331–352.

Ders.: Anmerkung zu EuGH, Urteil vom 2.5.2006 – C-217/04, Vereinigtes Königreich Großbritannien und Nordirland/Europäisches Parlament u. a., Europäische Zeitschrift für Wirtschaftsrecht 2006, S. 372–374.

Ohly, *Ansgar*: Die Verantwortlichkeit von Intermediären, Zeitschrift für Urheber- und Medienrecht 2015, S. 308–318.

Ders./*Sosnitza*, *Ansgar*: UWG, Gesetz gegen den unlauteren Wettbewerb, Kommentar, 6. Auflage, München 2014.

Pahlen-Brandt, Ingrid: Zur Personenbezogenheit von IP-Adressen, Kommunikation und Recht 2008, S. 286–290.

Palandt, *Otto*: Bürgerliches Gesetzbuch, Kommentar, 75. Auflage, München 2016.

Palantir: Palantir Cyber – An End-to-End Cyber Intelligence Platform for Analysis & Knowledge Management, Palo Alto (CA) 2013, online abrufbar: http://docplayer.net/4555976-Palantir-cyber-an-end-to-end-cyber-intelligence-platform-for-analysis-knowledge-management.html (zuletzt abgerufen am 23.02.2016).

Palfrey, *John*/*Gasser*, *Urs*: Interop – The Promise and Perils of highly interconnected systems, New York 2012.

Pernice, *Ingolf*: Soll das Recht der Regulierungsverwaltung übergreifend geregelt werden? Europarechtliche Aspekte, in: Ständige Deputation des Deutschen Juristentages (Hrsg.), Verhandlungen des 66. Deutschen Juristentages Stuttgart 2006, Band II/1: Sitzungsberichte: Referate und Beschlüsse, München 2006, S. O 85-O 142.

Ders.: Das Ende der währungspolitischen Souveränität Deutschlands und das Maastricht-Urteil des BVerfG, in: Due, Ole, Lutter, Marcus, Schwarze, Jürgen (Hrsg.), Festschrift für Ulrich Everling, Band II, Baden-Baden 1995, S. 1057–1070.

Ders.: Verfassungs- und europarechtliche Aspekte der Transparenz staatlichen Handelns, 2. IFG-Tagung Berlin am 6./7. September 2012, in: Dix, Alexander, Franßen, Gregor, Kloepfer, Michael, Schaar, Peter, Schoch, Friedrich, Deutsche Gesellschaft für Informationsfreiheit e.V. (Hrsg.), Informationsfreiheit und Informationsrecht Jahrbuch 2013, Berlin 2014, S. 17–34.

Ders.: Die Verfassung der Internetgesellschaft, in: Blankenagel (Hrsg.), Den Verfassungsstaat nachdenken, Berlin 2014, S. 171–208.

Ders.; „Völkerrecht des Netzes" – Konstitutionelle Elemente eines globalen Rechtsrahmens für das Internet, in: Biaggini/Diggelmann/Kaufmann (Hrsg.), Polis und Kosmopolis, FS Thürer, 2015, S. 576–587.

Petermann, *Thomas*/*Bradke*, *Harald*/*Lüllmann*, *Arne*/*Poetzsch*, *Maik*/*Riehm*, *Ulrich*: Was bei einem Blackout geschieht: Folgen eines langandauernden und großflächigen Stromausfalls, Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag, Berlin 2011.

Petersen, *Stefanie*: Grenzen des Verrechtlichungsgebotes im Datenschutz, Münster, Hamburg 2000.

Petri, *Thomas*: Sicherheitsbehördliche Datenverarbeitung, in: Schmidt, Jan-Hinrik, Weichert, Thilo (Hrsg.), Datenschutz: Grundlagen, Entwicklungen und Kontroversen, Bonn 2012, S. 115–128.

Petri, *Thomas*/*Tinnefeld*, *Marie-Theres*: Völlige Unabhängigkeit der Datenschutzkontrolle, MultiMedia und Recht 2010, S. 157–161.

Peukert, *Alexander*: Das Urheberrecht und die zwei Kulturen der Online-Kommunikation, Gewerblicher Rechtsschutz und Urheberrecht 2014, Beilage 1/2014, S. 77–93.

Pfitzmann, *Andreas*: Stellungnahme zum „Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes" auf der Basis der Drucksachen 16/11967 und 16/12225, 7.5.2009, online abrufbar: http://dud.inf.tu-dresden.de/literatur/Innenausschuss APf20090507.pdf (zuletzt abgerufen am 30. April 2017).

Pflug, *Manuel*: Pandemievorsorge – informationelle und kognitive Regelungsstrukturen, Berlin 2013.

Picanso, *Kathryn*: Protecting Information Security Under a Uniform Data Breach Notification Law, Fordham Law Review 2006, S. 355–390.

Pieroth, *Bodo*/*Schlink*, *Bernhard*/*Kingreen*, *Thorsten*/*Poscher*, *Ralf*: Grundrechte, Staatsrecht II, 31. Auflage, Heidelberg 2015.

Pitschas, *Rainer*: Allgemeines Verwaltungsrecht als Teil der öffentlichen Informationsordnung, in: Hoffmann-Riem, Wolfgang, Schmidt-Aßmann, Eberhard, Schuppert, Gunnar Folke(Hrsg.), Reform des allgemeinen Verwaltungsrechts. Grundfragen, Baden-Baden 1993, 219–305.

Pitschas, *Rainer*: Das Informationsverwaltungsrecht im Spiegel der Rechtsprechung, Die Verwaltung 33 (2000), S. 111–137.

Pitschas, *Rainer*: „Sicherheitspartnerschaften" der Polizei und Datenschutz, Deutsches Verwaltungsblatt 2000, S. 1805–1815.

Pitschas, *Rainer*: Datenschutz in Sicherheitspartnerschaften der Polizei mit privaten Sicherheitsdienstleistern, in: Stober, Rolf (Hrsg.), Public-Private-Partnerships und Sicherheitspartnerschaften: Ergebnisse des Professorengesprächs vom 13. April 2000, Köln, München 2000, S. 91–115.

Pitschas, *Rainer*: Europäisches Verwaltungsverfahrensrecht und Handlungsformen der gemeinschaftlichen Verwaltungskooperation, Hill, Hermann, Pitschas, Rainer (Hrsg.), europäisches Verwaltungsverfahrensrecht, Berlin 2004, S. 301–336.

Pitschas, *Rainer*/*Aulehner*, *Josef*: Informationelle Sicherheit oder „Sicherheitsstaat"?, Neue Juristische Wochenschrift 1989, S. 2353–2359.

Plath, *Kai-Uwe* (Hrsg.): BDSG, Kommentar, Köln 2013.

Podlech, *Adalbert*: Individualdatenschutz – Sytemdatenschutz, in: Brückner, Klaus (Hrsg.), Beiträge zum Sozialrecht, Festgabe für Hans Grüner, Percha am Starnberger See 1982, S. 451–462.

Pöcker, *Markus*: Unabhängige Regulierungsbehörden und die Fortentwicklung des Demokratieprinzips, Verwaltungsarchiv 99 (2008), S. 380–400.

Pohl, *Helmut*: Zur Technik der heimlichen Online-Durchsuchung, Datenschutz und Datensicherheit 2007, S. 684–688.

Pohle, *Jan*/*Nink*, *Judith*: Die Bestimmbarkeit des Personenbezugs – Von der IP-Adresse zum Anwendungsbereich der Datenschutzgesetze, MultiMedia und Recht 2015, S. 563–567.

Pohlmann, *Norbert*: Zur Entwicklung einer IT-Sicherheitskultur – Wie das IT-Sicherheitsgesetz den gesellschaftlichen Umgang mit IT-Risiken fördern kann, in: Datenschutz und Datensicherheit 2016, S. 38–42.

Priebe, *Reinhard*: Sicherheitspolitik: EU-Cybersicherheitsstrategie, Europäische Zeitschrift für Wirtschaftsrecht 2013, S. 204.

Priebe, *Reinhard*: Die Aufgaben des Rechts in einer sich ausdifferenzierenden EG-Administration, in: Schmidt-Aßmann, Eberhard, Hoffmann-Riem, Wolfgang (Hrsg.). Strukturen des Europäischen Verwaltungsrechts, Baden-Baden 1999, S. 71–98.

Püschel, *Jan Ole*: Informationen des Staates als Wirtschaftsgut, Berlin 2006.

Quabeck, *Christian*: Dienende Funktion des Verwaltungsverfahrens und Prozeduralisierung, Tübingen 2010.

Queck, *Nadine*: Die Geltung des nemo-tenetur-Grundsatzes zugunsten von Unternehmen, Berlin 2005.

Raabe, *Oliver*: Abgrenzungsprobleme bei der rechtlichen Einordnung von Anonymisierungsdiensten im Internet, Computer und Recht 2003, S. 268–274.

Raabe, *Oliver*/*Dinger*, *Jochen*/*Hartenstein*, *Hannes*: Telekommunikationsdienste in Next-Generation-Networks am Beispiel von Peer-to-Peer-Overlay-Systemen, Kommunikation & Recht 2007, Beihefter 1, S. 1–12.

Rademacher, *Timo*: Realakte im Rechtsschutzsystem der Europäischen Union, Tübingen 2014.

Rath, *Michael*/*Kuss*, *Christian*/*Bach*, *Simone*: Das neue IT-Sicherheitsgesetz, Kommunikation und Recht 2015, S. 437–440.

Rathgeber, *Christian*: Terrorismusbekämpfung durch Organisationsrecht, Deutsches Verwaltungsblatt 2013, S. 1009–1016.

Raue, *Benjamin*: Informationsfreiheit und Urheberrecht, JuristenZeitung 2013, S. 280–288.

Raymond, *Eric*: The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary, Sebastopol (CA) 1999.

Rehberg, *Markus*: Der staatliche Umgang mit Informationen – Das europäische Informationsmodell im Lichte von Behavioral Economics, in: Eger, Thomas, Schäfer, Hans-Bernd (Hrsg.), Ökonomische Analyse der europäischen Zivilrechtsentwicklung, Tübingen 2007, S. 284–354.

Reichenbach, Gerold/Göbel, Ralf/Wolff, Hartfrid/Stokar von Neuforn, Silke (Hrsg.): Risiken und Herausforderungen für die öffentliche Sicherheit in Deutschland: Szenarien und Leitfaden; Grünbuch des Zukunftsforums Öffentliche Sicherheit, 2. Auflage, Berlin 2011.

Reindl-Krauskopf, *Susanne*: Cyber-Kriminalität, Zeitung für ausländisches öffentliches Recht und Völkerrecht 2014, S. 563–574.

Rittner, *Fritz*: Demokratie als Problem: Abschied vom Parlamentarismus?, JuristenZeitung 2003, S. 641–647.

Robinson, *Neil*/*Disley*, *Emma*/*Potoglou*, *Dimitris*/*Reding*, *Anais*/*Culley*, *Deidre*/*Penny*, *Maryse*/*Botterman*, *Maarten*/*Carpenter*, *Gwendolyn*/*Blackman*, *Colin*/*Millard*, *Jeremy*: Feasibilty study for a European Cybercrime Centre, Final Report, Studie für die Europäische Kommission, Brüssel 2012.

Röhl, *Hans Christian*: Ausgewählte Verwaltungsverfahren, in: Hoffmann-Riem, Wolfgang, Schmidt-Aßmann, Eberhard, Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts, Band II: Informationsordnung – Verwaltungsverfahren – Handlungsformen, 2. Auflage, München 2012, § 30, S. 731–798.

Roggan, *Fredrik*: G-10-Gesetz, Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, Baden-Baden 2012.

Ders.: Das neue BKA-Gesetz – Zur weiteren Zentralisierung der deutschen Sicherheitsarchitektur, Neue Juristische Wochenschrift 2009, S. 257–262.

Ronellenfitsch, *Michael*: Der Vorrang des Grundrechts auf informationelle Selbstbestimmung vor dem AEUV, Datenschutz und Datensicherheit 2009, S. 451–461

Roos, *Philipp*: Der neue Entwurf eines IT-Sicherheitsgesetzes – Bewegung oder Stillstand?, MultiMedia und Recht 2014, S. 723–730

Rosenberger, *Stefan*: Geheimnisschutz und Öffentlichkeit in Verwaltungsverfahren und -prozeß, Bayreuth 1998.

Rossi, *Matthias*: Informationszugangsfreiheit und Verfassungsrecht: Zu den Wechselwirkungen zwischen Informationsfreiheitsgrenzen und der Verfassungsordnung in Deutschland, Berlin 2004.

Ders.: Informationsfreiheitsgesetz, Handkommentar, Baden-Baden 2006.

Ders.: Möglichkeiten und Grenzen des Informationshandelns des Bundesrechnungshofes, Baden-Baden 2012.

Ders.: Informationsfreiheitsrecht in der gerichtlichen Praxis, Deutsches Verwaltungsblatt 2010, S. 554–563.

Ders.: Staatliche Daten als Informationsrohstoff, Neue Zeitschrift für Verwaltungsrecht 2013, S. 1263–1266.

Roßnagel, *Alexander*/*Wedde*, *Peter*/*Hammer*, *Volker*/*Pordesch*, *Ulrich*: Die Verletzlichkeit der ‚Informationsgesellschaft', 2. Auflage, Wiesbaden 1989.

Ders.: Das Telemediengesetz, Neue Zeitschrift für Verwaltungsrecht 2007, S. 743–748.

Ders.: Datenschutz in globalen Netzen, Datenschutz und Datensicherheit, 1999, S. 253–257.

Ders.: Datenschutzaudit: Konzeption, Durchführung, gesetzliche Regelung, Braunschweig, Wiesbaden 2000.*Roßnagel*, Alexander: Das Konzept des Datenschutzaudits, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht, München 2003, S. 437–484.

Ders.: Die „Überwachungs-Gesamtrechnung" – das BVerfG und die Vorratsdatenspeicherung, Neue Juristische Wochenschrift 2010, S. 1238–1242.

Ders.: Konflikte zwischen Informationsfreiheit und Datenschutz?, MultiMedia und Recht 2007, S. 16–21.

Ders.: Auf dem Weg zur elektronischen Verwaltung – Das E-Government-Gesetz, Neue Juristische Wochenschrift 2013, S. 2710- 2716.

Ders.: Schriftliche Stellungnahme zur Sachverständigenanhörung am 20. April 2015 zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), Ausschussdrucksache 18(4)284 B, 14. April 2015, online abrufbar: https://www.bundestag.de/blob/369962/584bab2bd8e0fd525f08ac0cd2c2d506/18-4-284-b-data.pdf (zuletzt abgerufen am 30. April 2017).

Ders./*Pfitzmann*, *Andreas*/*Garstka*, *Hansjürgen*: Modernisierung des Datenschutzrechts: Gutachten im Auftrag des Bundesministerium des Inneren, Berlin 2001.

Ders./*Scheuer*, *Alexander*: Das europäische Medienrecht, MultiMedia und Recht 2005, S. 271–278.

Ders./Schnabel, *Christoph*: Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht, Neue Juristische Wochenschrift 2008, S. 3534–3538.

Ders./ Hentschel, *Anja*: Verfassungsrechtliche Grenzen gesetzlicher Pflichten zur Offenlegung von Arbeits- und Beschäftigungsbedingungen, Düsseldorf 2016.

Ders.: Zusätzlicher Arbeitsaufwand für die Aufsichtsbehörden der Länder durch die Datenschutz-Grundverordnung, Kassel 2017, online abrufbar: http://suche.transparenz.hamburg.de/dataset/gutachten-zum-zusaetzlichen-arbeitsaufwand-fuer-die-aufsichtsbehoerden-der-laender-durch-d-2017 (zuletzt abgerufen am 22. April 2017).

Roth, *Hans-Peter*: Neuer Referentenentwurf zum IT-Sicherheitsgesetz, Zeitschrift für Datenschutz 2015, S. 17–22.

Ruffert, *Matthias*: Regulierung im System des Verwaltungsrechts, Archiv des öffentlichen Rechts 124 (1999), S. 237–281.

Rupp, *Hans Heinrich*: Grundfragen der heutigen Verwaltungsrechtslehre: Verwaltungsnorm und Verwaltungsrechtsverhältnis, 2. Auflage, Tübingen 1991.

Sachs, *Michael* (Hrsg.): Grundgesetz Kommentar, 7. Auflage, München 2014.

Säcker, *Franz Jürgen* (Hrsg.): TKG Telekommunikationsgesetz, 3. Auflage, Frankfurt am Main 2013.

Ders./Rixecker, *Roland*/*Oetker*, *Hartmut*/*Limperg*, *Bettina* (Hrsg.): Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 5: §§ 705–853, Partnerschaftsgesellschaftsgesetz, Produkthaftungsgesetz, 6. Auflage, München 2013.

Ders./Montag, *Frank* (Hrsg.): Münchener Kommentar zum Europäischen und Deutschen Wettbewerbsrecht (Kartellrecht), Band 2, 2. Auflage, München 2015.

Saeltzer, *Gerhard*: Sind diese Daten personenbezogen oder nicht?, Datenschutz und Datensicherheit 2004, S. 218–227.

Saloven, *Matjaz*/*Grant*, *Euan*/*Hanel*, *Peter*/*Makai*, *Viktor*/*Hansen*, *Kenneth*/*Belevicius*, *Linas*/*Pohnitzer*, *Angelika*: Study on the status of information exchange amongst law enforcement authorities in the context of existing EU instruments, Brüssel 2010., online abrufbar: http://ec.europa.eu/dgs/home-affairs/doc_centre/police/docs/icmpd_study_lea_infoex.pdf (zuletzt abgerufen am 30. April 2017).

Saurugg, *Herbert*: Die Netzwerkgesellschaft und Krisenmanagement 2.0: Durch aktive Systemgestaltung zu einer nachhaltigen Zukunft, Wien 2012.

Sassaman, *Len*/*Patterson*, *Meredith*/*Bratus*, *Sergey*/*Shubina*, *Anna*: The Halting Problems of Network Stack Insecurity, in: ;login: Volume 36 (2011), Nr. 6, S. 22–32.

Schaar, *Peter*: Datenschutz im Internet – Die Grundlagen, München 2002.

Ders.: Minimalprogramm in Sachen Datenschutz, MultiMedia und Recht 2014, S. 641–642.

Schadel, *Ruth*: Informationsrechte und -pflichten bei Sicherheitslücken im Internet – Zum Beitrag des Rechts zur Steuerung der IT-Sicherheit im Internet, Darmstadt 2007, online abrufbar: http://tuprints.ulb.tu-darmstadt.de/811/1/Schadel.pdf (zuletzt abgerufen am 30. April 2017).

Schallbruch, *Martin*: Die EU-Richtlinie über Netz- und Informationssicherheit: Anforderungen an digitale Dienste, Computer und Recht 2016, 663–670.

Schaumburg, *Harald*: Internationales Steuerrecht, Außensteuerrecht – Doppelbesteuerungsrecht, 3. Auflage, Köln 2011.

Schenke, *Wolf-Rüdiger*/*Graulich*, *Kurt*/*Ruthig*, *Josef* (Hrsg.): Sicherheitsrecht des Bundes, BPolG, BKAG, ATDG, BVerfSchG, BNDG, VereinsG, München 2014.

Scherschel, *Fabian*: BSI-Audit: OpenSSL ohne große Schwachstellen, aber mit Entropie-Problemen, Heise-Security, 10.02.2016, online abrufbar: http://www.heise.de/security/

meldung/BSI-Audit-OpenSSL-ohne-grosse-Schwachstellen-aber-mit-Entropie-Problemen-3097632.html (zuletzt abgerufen am 30. April 2017).

Scherzberg, *Arno*: Wissen, Nichtwissen und Ungewissheit im Recht, in: Engel, Christoph, Halfmann, Jost, Schulte, Martin (Hrsg.), Wissen – Nichtwissen – Unsicheres Wissen, Baden-Baden 2002, S. 113–144.

Scheurle, *Klaus-Dieter*/*Mayen*, *Thomas* (Hrsg.): Telekommunikationsgesetz: TKG Kommentar, 2. Auflage, München 2008.

Schießle, *Björn*: Free Software, Open Source, FOSS, FLOSS – same same but different, 11.5.2012, online abrufbar: https://blog.schiessle.org/2012/05/11/free-software-open-source-foss-floss-same-same-but-different/ (zuletzt abgerufen am 30. April 2017).

Schindler, *Gerhard*: Wirtschaftsschutz – Strategie und Herausforderungen für den Bundesnachrichtendienst, Rede des BND-Präsidenten Gerhard Schindler anlässlich des 11. Symposiums des Bundesamtes für Verfassungsschutz am 8. Mai 2014, online abrufbar: http://www.bnd.bund.de/DE/Organisation/Reden_der_Leitung/Redetexte/Rede_BfV-Symposium2014.html (zuletzt abgerufen am 30. April 2017).

Schleipfer, *Stefan*/*Eckhardt*, *Jens*: Anmerkungen zum Urteil des BGH vom 28.10.2014, VI ZR 135/13 – IP-Adresse ein personenbezogenes Datum bei Identifizierbarkeit durch Dritte?, Computer und Recht 2015, S. 113–116.

Schliesky, *Utz*/*Hoffmann*, *Christian*/*Luch*, *Anika*/*Schulz*, *Sönke*/*Borchers*, *Kim Corinna*: Schutzpflichten und Drittwirkung im Internet: Das Grundgesetz im digitalen Zeitalter, Baden-Baden 2014.

Ders./*Schulz*, *Sönke* (Hrsg.): Transparenz, Partizipation, Kollaboration – Web 2.0 für die öffentliche Verwaltung, Kiel 2012.

Schmidl, *Michael*: Aspekte des Rechts der IT-Sicherheit, Neue Juristische Wochenschrift 2010, S. 476–481.

Ders.: IT-Recht von A-Z, 2. Auflage, München 2014.

Schmidt, *Andreas*: At the Boundaries of Peer Production: The Organisation of Internet Security Production in the Cases of Estonia 2007 and Conficker, Telecommunications Policy 36 (2012), S. 451–461.

Schmidt, *Eric*/*Cohen*, *Jared*: The New Digital Age: Reshaping the Future of People, Nations and Business, New York 2013.

Schmidt-Aßmann, *Eberhard*: Verwaltungsorganisationsrecht als Steuerungsressource, Baden-Baden 1997.

Ders.: Das allgemeine Verwaltungsrecht als Ordnungsidee: Grundlagen und Aufgaben der verwaltungsrechtlichen Systembildung, 2. Auflage, Berlin 2006.

Ders.: Europäische Verwaltung zwischen Kooperation und Hierarchie, in: Cremer, Hans-Joachim, Giegerich, Thomas, Richter, Dagmar, Zimmermann, Andreas (Hrsg.), Tradition und Weltoffenheit des Rechts, Festschrift für Helmut Steinberger, Berlin 2002, S. 1375–1399.

Ders.: Verwaltungskooperation und Verwaltungskooperationsrecht in der Europäischen Gemeinschaft, Europarecht 1996, S. 270–301.

Ders.: Aufgaben und Perspektiven verwaltungsrechtlicher Forschung: Aufsätze 1975–2005, Tübingen 2006.

Ders.: Strukturen europäischer Verwaltung und die Rolle des Europäischen Verwaltungsrechts, in: Blankenagel, Alexander, Pernice, Ingolf, Schulze-Fielitz, Helmuth (Hrsg.), Verfassung im Diskurs der Welt, Liber Amicorum für Peter Häberle zum 70. Geburtstag, Tübingen 2004, S. 395–415.

Ders.: Verwaltungsrecht in der Informationsgesellschaft: Perspektiven der Systembildung, in: Hoffmann-Riem, Wolfgang, Schmidt-Aßmann, Eberhard (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, Baden-Baden 2000, S. 405–432.

Ders.: Verfassungsprinzipien für den Europäischen Verwaltungsverbund, in: Hoffmann-Riem, Wolfgang, Schmidt-Aßmann, Eberhard, Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts, Band I: Methoden – Maßstäbe – Aufgaben – Organisation, 2. Auflage, München 2012, § 5, S. 261–340.

Ders.: Der Verfahrensgedanke im deutschen und europäischen Verwaltungsrecht, in: Hoffmann-Riem, Wolfgang, Schmidt-Aßmann, Eberhard, Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts, Band II: Informationsordnung – Verwaltungsverfahren – Handlungsformen, 2. Auflage, München 2012, § 27, S. 495–556.

Ders.: Die Herausforderungen der Verwaltungsrechtswissenschaft durch die Internationalisierung der Verwaltungsbeziehungen, Der Staat 45 (2006), S. 315–338.

Ders.: Der Europäische Verwaltungsverbund und die Rolle des Europäischen Verwaltungsrechts, in: Schmidt-Aßmann, Eberhard, Schöndorf-Haubold, Bettina (Hrsg.), Der Europäische Verwaltungsbund. Formen und Verfahren der Verwaltungszusammenarbeit in der EU, Tübingen 2005, S. 1–23.

Ders.: Perspektiven der Europäisierung des Verwaltungsrechts, in: Axer, Peter, Grzeszick, Bernd, Kahl, Wolfgang, Mager, Ute, Reimer, Ekkehart (Hrsg.), Das Europäische Verwaltungsrecht in der Konsolidierungsphase. Systembildung – Disziplinierung – Internationalisierung, Die Verwaltung Beiheft 10, Berlin 2010, S. 263–283.

Schmidt-Holtmann, *Christina*: Der Schutz der IP-Adresse im deutschen und europäischen Datenschutzrecht: zur Auslegung des Begriffs des personenbezogenen Datums, Berlin 2014.

Schmidt-Kessel, *Martin*: Für ein digitales Produktsicherheitsgesetz – ein Plädoyer, Verbraucher und Recht 2015, S. 121–123.

Schneider, *Jens-Peter*: Stand und Perspektiven des Europäischen Datenverkehrs- und Datenschutzrechts, Die Verwaltung 44 (2011), S. 499–524.

Ders.: Informationssysteme als Bausteine des Europäischen Verwaltungsverbunds, Neue Zeitschrift für Verwaltungsrecht 2012, S. 65–70.

Ders.: Vorüberlegungen zum Informationsmanagement in europäischen Verwaltungsverfahren, in: Lipowicz, Irena, Schneider, Jens-Peter (Hrsg.), Perspektiven des deutschen, polnischen und europäischen Informationsrechts: Ergebnisse einer deutsch-polnischen Alexander von Humboldt-Institutspartnerschaft, Göttingen 2011, S. 159–186.

Ders./*Hofmann*, *Herwig*/*Ziller*, *Jaques*: ReNEUAL – Musterentwurf für ein EU-Verwaltungsverfahrensrecht, München 2015.

Schneider, *Jochen*: Datenschutz und neue Medien, Neue Juristische Wochenschrift 1984, S. 390–398.

Schneier, *Bruce*: Complexity the Worst Enemy of Security, Interview mit der Computerworld Hong Kong (CWHK), 17.12.2012, online abrufbar: https://www.schneier.com/news/archives/2012/12/complexity_the_worst.html (zuletzt abgerufen am 30. April 2017).

Ders.: Full Disclosure of Security Vulnerabilities a ‚Damned Good Idea', 2007, online abrufbar unter: https://www.schneier.com/essays/archives/2007/01/schneier_full_disclo.html (zuletzt abgerufen am 30. April 2017).

Schoch, *Friedrich*: Entformalisierung staatlichen Handeln, in: Isensee, Josef, Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts, Band III: Demokratie – Bundesorgane, 3. Auflage, Heidelberg 2005, S. 131–227.

Ders.: Der deutsche Professorenentwurf für ein Informationsgesetzbuch unter besonderer Beachtung des Ausgleichs zwischen Informationsfreiheit und Datenschutz, in: Lipowicz, Irena, Schneider, Jens-Peter (Hrsg.), Perspektiven des deutschen, polnischen und europäischen Informationsrechts: Ergebnisse einer deutsch-polnischen Alexander von Humboldt-Institutspartnerschaft, Göttingen 2011, S. 11–30.

Ders.: Amtliche Publikumsinformation zwischen staatlichem Schutzauftrag und Staatshaftung, Neue Juristische Wochenschrift 2012, S. 2844–2850.

Ders.: Amtliche Publikumsinformation im Spiegel der Rechtsprechung, Verwaltungsblätter für Baden-Württemberg 2014, S. 361–369.

Ders.: Informationszugangsfreiheit des Einzelnen und Informationsverhalten des Staates, Archiv für Presserecht 2010, S. 313–324.

Ders.: Informationsrecht in einem grenzüberschreitenden und europäischen Kontext, Europäische Zeitschrift für Wirtschaftsrecht 2011, S. 388–394.

Ders.: Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer 57 (1998), S. 158–215.

Ders.: Neue Entwicklungen im Verbraucherinformationsrecht, Neue Juristische Wochenschrift 2010, S. 2241–2247.

Ders.: Polizei- und Ordnungsrecht, in: Schoch, Friedrich (Hrsg.), Besonderes Verwaltungsrecht, 15. Auflage, Berlin 2013, Kapitel 2, S. 125–308.

Ders.: Diskussionsbemerkung, Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer 63 (2004), S. 442–468.

Ders. (Hrsg.): IFG: Informationsfreiheitsgesetz, Kommentar, 2. Auflage, München 2016.

Ders./Schneider, *Jens-Peter*/*Bier*, *Wolfgang* (Hrsg.): Verwaltungsgerichtsordnung: VwGO, Kommentar, 29. Auflage, München 2015.

Schönbohm, *Arne*: Deutschlands Sicherheit: Cybercrime und Cyberwar, Münster 2011.

Schöndorf-Haubold, *Bettina*: Europäisches Sicherheitsverwaltungsrecht, Baden-Baden 2010.

Dies.: Europäisches Sicherheitsverwaltungsrecht, in: Terhechte, Jörg Philipp (Hrsg.), Verwaltungsrecht der Europäischen Union, Baden-Baden 2011, § 35, S. 1211–1298.

Scholl, *Patrick*: Der private Sachverständige im Verwaltungsrecht: Elemente einer allgemeinen Sachverständigenlehre, Baden-Baden 2005.

Scholz, *Rupert*/*Pitschas*, *Rainer*: Informationelle Selbstbestimmung und staatliche Informationsverantwortung, Berlin 1984.

Scholz, *Susanne*: Informationsaustausch ohne Anonymisierung und unabhängig von der konkreten Besteuerung der Gesellschaften ist unzulässig – Anmerkung zum Beschluss des FG Köln vom 07.09.2015, Az.: 2 V 1375/15, Internationales Steuerrecht 2015, S. 835–844.

Schoppa, *Katrin*: Europol im Verbund der Europäischen Sicherheitsagenturen, Berlin 2013.

Schricker, *Gerhard*/*Loewenheim*, *Uwe* (Hrsg.): Urheberrecht, Kommentar, 4. Auflage, München 2010.

Schürmann, *Frank*: Öffentlichkeitsarbeit der Bundesregierung: Strukturen, Medien, Auftrag und Grenzen eines informalen Instruments der Staatsleitung, Berlin 1992.

Schuler, *Douglas*: Online Deliberation and Civic Intelligence, in: Lathrop, Daniel, Ruma, Laurel (Hrsg.), Open Government: Collaboration, Transparency, and Participation in Practice, Sebastopol (CA) 2010, S. 91–104.

Schulz, Sönke/*Tischer*, *Jakob*: Das Internet als kritische Infrastruktur, Zeitschrift für Gesetzgebung 2013, S. 339–357.

Schulz, *Wolfgang*: Beurteilungsspielräume als Wissensproblem – am Beispiel der Regulierungsverwaltung, Rechtswissenschaft 3 (2012), S. 330–350.

Schulski-Haddouti, *Christiane*: Crypto Wars 3.0: Neuorganisation des BSI gefordert, Heise online, 28.01.2015, online abrufbar: http://www.heise.de/newsticker/meldung/Crypto-Wars-3-0-Neuorganisation-des-BSI-gefordert-2530552.html (zuletzt abgerufen am 30. April 2017).

Schuppert, *Gunnar Folke*: Die Erfüllung öffentlicher Aufgaben durch verselbständigte Verwaltungseinheiten: eine verwaltungswissenschaftliche Untersuchung, Göttingen 1981.

Schuppert, *Gunnar Folke*: Governance durch Wissen, in: Schuppert, Gunnar Folke, Voßkuhle, Andreas (Hrsg.), Governance von und durch Wissen, Baden-Baden 2008, S. 259–304.

Schuppert, *Gunnar Folke*: Nudging: nicht wirklich neu und auch – ohne Kontextualisierung – nicht weiterführend, Verfassungsblog, 16.04.2015, online abrufbar: http://verfassungsblog.de/nudging-nicht-wirklich-neu-und-auch-ohne-kontextualisierung-nicht-weiterfuehrend/ (zuletzt abgerufen am 30. April 2017).

Schuster, *Fabian*/*Sassenbach*, *Thomas*: Monitoring und Fraud Detection durch Telekommunikationsanbieter, Computer und Recht 2011, S. 15–19.

Schwabenbauer, *Thomas*: Heimliche Grundrechtseingriffe: ein Beitrag zu den Möglichkeiten und Grenzen sicherheitsbehördlicher Ausforschung, Tübingen 2013.

Schwarze, *Jürgen*/*Becker*, *Ulrich*/*Hatje*, *Armin*/*Schoo*, *Johann* (Hrsg.): EU-Kommentar, 3. Auflage, Baden-Baden 2012.

Schwartz, *Paul*/*Solove*, *Danie*: Reconciling Personal Information in the United States and European Union, California Law Review 2014, Volume 102, S. 877–916.

Sellmann, *Christian*/*Augsberg*, *Steffen*: Chancen und Risiken des Bundesinformationsfreiheitsgesetzes – Eine Gebrauchsanleitung für (Private) Unternehmen, Wertpapier-Mitteilungen 2006, S. 2293–2301.

Sennekamp, *Irmela*: Der Diskurs um die Abgrenzung von Kartell- und Regulierungsrecht – Ein juristischer Streit zwischen gesetzgeberischem Steuerungsanspruch und rechtsdogmatischem Ordnungsdenken, Tübingen 2016.

Shapiro, *Martin*: Independent Agencies, in: Craig, Paul, Búrca, Gráinne de (Hrsg.), The Evolution of EU Law, 2. Auflage, Oxford 2011, Kapitel 5, S. 111–120.

Shirvani, *Foroud*: New Public Management und europäische Agenturen: Transparenzfragen bei der Modernisierung der Verwaltungsorganisation, Die Öffentliche Verwaltung 2008, S. 1–10.

Shostack, *Adam*/*Stewart*, *Andrew*: The New School of Information Security, Boston, MA, 2008

Siegel, *Thorsten*: Entscheidungsfindung im Verwaltungsverbund: horizontale Entscheidungsvernetzung und vertikale Entscheidungsstufung im nationalen und europäischen Verwaltungsverbund, Tübingen 2009.

Simitis, *Spiros*: Selbstbestimmung: Illusorisches Projekt oder reale Chance, Kritische Justiz 1988, S. 32–50.

Ders. (Hrsg.): Bundesdatenschutzgesetz, Kommentar, 8. Auflage, Baden-Baden 2014.

Simon, *Herbert*: Bounded Rationality and Organizational Learning, Organization Science 1991, S. 125–134.

Skierka, *Isabel*/*Morgus*, *Robert*/*Hohmann*, *Mirko*/*Maurer*, *Tim*: CSIRT Basics for Policy-Makers. The History, Types & Culture of Computer Security Incident Response Teams, Mai 2015.

Skopik, *Florian*/*Bleier*, *Thomas*/*Fiedler*, *Roman*: Cyber Attack Information System: Gesamtansatz, in: Leopold, Helmut, Bleier, Thomas, Skopik, Florian (Hrsg.): Cyber Attack Information System: Erfahrungen und Erkenntnisse aus der IKT-Sicherheitsforschung, Berlin 2015, S. 53–69.

Slaughter, *Anne-Marie*: A new world order, Princeton 2004.

Dies.: Global Government Networks, Global Information Agencies, and Disaggregated Democracy, Harvard Law School, Public Law Working Paper Nr. 18, September 2001, online abrufbar: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=283976 (zuletzt abgerufen am 30. April 2017).

Sloterdijk, *Peter*: Zorn und Zeit, 4. Auflage, Frankfurt am Main 2016.

Slovic, *Paul*/*Fischhoff*, *Baruch*/*Lichtenstein*, *Sarah*: Facts and Fears: Understanding Perceived Risk, in: Schwing, Richard C., Albers Jr., Walter A. (Hrsg.), Societal risk assessment: How safe is safe enough?, New York 1980, S. 181–214.

Smeddinck, *Ulrich*: Der Nudge-Ansatz – eine Möglichkeit, wirksam zu regieren?, Zeitschrift für Rechtspolitik 2014, S. 245–247.

Sobotta, *Christoph*: Transparenz in den Rechtsetzungsverfahren der Europäischen Union: Stand und Perspektiven des Gemeinschaftsrechts unter besonderer Berücksichtigung des Grundrechts auf Zugang zu Informationen, Baden-Baden 2001.

Sommer, *Julia*: Verwaltungskooperation am Beispiel administrativer Informationsverfahren im Europäischen Umweltrecht, Berlin 2003.

Dies.: Informationskooperation am Beispiel des europäischen Umweltrechts, in: Schmidt-Aßmann, Eberhard, Schöndorf-Haubold, Bettina (Hrsg.), Der Europäische Verwaltungsbund. Formen und Verfahren der Verwaltungszusammenarbeit in der EU, Tübingen 2005, S. 57–86.

Sommer, *Stephan*: Staatliche Gewährleistung im Verkehrs-, Post- und Telekommunikationsbereich: zur Interpretation der Gewährleistungsnormen der Art. 87e IV und 87f I GG im System verfassungsrechtlicher Leistungspflichten, Berlin 2000.

Sonntag, *Matthias*: IT-Sicherheit kritischer Infrastrukturen: von der Staatsaufgabe zur rechtlichen Ausgestaltung, München 2005.

Specht, *Louisa*/*Müller-Riemenschneider*, *Severin*: Dynamische IP-Adressen: Personenbezogene Daten für den Webseitenbetreiber? – Aktueller Stand der Diskussion um den Personenbezug, Zeitschrift für Datenschutz 2014, S. 71–75.

Spiecker gen. Döhmann, *Indra*/*Kurzenhäuser*, *Stephanie*: Das rechtliche Darstellungsgebot – Zum Umgang mit Risikoinformationen am Beispiel der Datenerhebung im Bundesinfektionsschutzgesetz (IfSG), in: Engel, Christoph, Englerth, Markus, Lüdemann, Jörn, Spiecker gen. Döhmann, Indra (Hrsg.), Recht und Verhalten – Beiträge zu Behavioral Law and Economics, Tübingen 2007, S. 133–164.

Dies.: Die informationelle Inanspruchnahme des Bürgers im Verwaltungsverfahren: Der Amtsermittlungsgrundsatz nach § 24 VwVfG, in: Spiecker gen. Döhmann, Indra, Collin, Peter (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, Tübingen 2008, S. 196–216.

Dies.: Wissensverarbeitung im Öffentlichen Recht, Rechtswissenschaft 2010, S. 247–282.

Dies.: Zum Datenschutz im Hinblick auf die Unabhängigkeit der nationalen Aufsichtsstellen über den Datenschutz, JuristenZeitung 2010, S. 787–791.

Spies, *Axel*: ITU-Konferenz in Dubai 2012 – Regulierung des Internet?, MultiMedia und Recht-Aktuell 2012, 339462.

Spindler, *Gerald*: Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, Studie im Auftrag des BSI, Bonn 2007, online abrufbar: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITSicherheitUndRecht/Gutachten_pdf.pdf?__blob=publicationFile&v=2 (zuletzt abgerufen am 30. April 2017).

Ders.: IT-Sicherheit – Rechtliche Defizite und rechtspolitische Alternativen, MultiMedia und Recht 2008, S. 7–13.

Ders.: IT-Sicherheit und kritische Infrastrukturen – Öffentlich-rechtliche und zivilrechtliche Regulierungsmodelle, in: Kloepfer, Michael (Hrsg.), Schutz kritischer Infrastrukturen, Baden-Baden 2010, S. 85–119.

Ders.: Produktverantwortung und Haftung im IT-Bereich, in: Kullmann/Pfister/Stöhr/ders. (Hrsg.), Produzentenhaftung, Loseblattsammlung mit Aktualisierung 07/16, Berlin 2016.

Ders./*Schuster*, *Fabian* (Hrsg.): Recht der elektronischen Medien, Kommentar, 3. Auflage, München 2015.

Ders.: IT-Sicherheitsgesetz und zivilrechtliche Haftung. Auswirkungen des IT-Sicherheitsgesetzes im Zusammenspiel mit der endgültigen EU-NIS-Richtlinie auf die zivilrechtliche Haftung, CR 2016, 297–312.

Stancke, *Fabian*: Grundlagen des Unternehmensdatenschutzrechts – gesetzlicher und vertraglicher Schutz unternehmensbezogener Daten im privaten Wirtschaftsverkehr, Betriebs-Berater 2013, S. 1418–1425.

Steinbeis, *Maximilian*: „Nudging" kommt nach Deutschland, Verfassungsblog, 27.08.2014, online abrufbar: http://verfassungsblog.de/nudging-kommt-nach-deutschland/ (zuletzt abgerufen am 30. April 2017).

Steiner, *Udo*: Öffentliche Verwaltung durch Private: allgemeine Lehren, Hamburg 1975.

Steinmüller, *Wilhelm*/*Lutterbeck*, *Bernd*/*Mallmann*, *Christoph*/*Harbort*, *Ulrich*/*Kolb*, *Gerhard*/*Schneider*, *Jochen*: Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministerium des Inneren, Bonn 1971, abgedruckt als Anlage 1 zur BT-Drs. VI/3826.

Ders./*Ermer*, *Leonhard*/*Schimmel*, *Wolfgang*: Das System des Datenschutzes, in: Steinmüller, Wilhelm, Ermer, Leonhard, Schimmel, Wolfgang (Hrsg.), Datenschutz bei riskanten Systemen, Berlin, New York 1978, S. 71–104.

Ders./*Ermer*, *Leonhard*/*Schimmel*, *Wolfgang*: Verallgemeinerung für riskante Systeme, in: Dies. (Hrsg.), Datenschutz bei riskanten Systemen, Berlin, New York 1978, S. 193–195.

Stelkens, *Ulrich*: Art. 291 AEUV, das Unionsverwaltungsrecht und die Verwaltungsautonomie der Mitgliedstaaten – zugleich zur Abgrenzung der Anwendungsbereiche von Art. 290 und Art. 291 AEUV, in: Europarecht 2012, S. 511–545.

Stelkens, *Paul*/*Bonk*, *Heinz Joachim*/*Sachs*, *Michael* (Hrsg.): VwVfG, Verwaltungsverfahrensgesetz, Kommentar, 8. Auflage, München 2014.

Stohrer, *Klaus*: Informationspflichten Privater gegenüber dem Staat in Zeiten von Privatisierung, Liberalisierung und Deregulierung: ein Beitrag zur Systematisierung und Vereinheitlichung des allgemeinen Informationsrechts, Berlin 2007.

Stolleis, *Michael*: Der lernfähige und der lernende Staat, in: Fried, Johannes, Stolleis, Michael (Hrsg.), Wissenskulturen: über die Erzeugung und Weitergabe von Wissen, Frankfurt am Main 2009, S. 58–78.

Streinz, *Rudolf* (Hrsg.): EUV/AEUV, Vertrag über die Europäische Union und Vertrag über die Arbeitsweise der Europäischen Union, 2. Auflage, München 2012.

Strulik, *Torsten*: Cognitive Governance. Gesellschaftliche Risikosteuerung im Spannungsfeld normativer und kognitiver Erwartungen, in: Governance von und durch Wissen, Schuppert, Gunnar Folke, Voßkuhle, Andreas (Hrsg.), Baden-Baden 2008, S. 87–109.

Stüer, *Bernhard*: ReNEUAL: Musterentwurf für ein EU-Verwaltungsverfahrensrecht, Deutsches Verwaltungsblatt 2016, S. 100–105.

Sunstein, *Cass Robert*: Informational Regulation and Informational Standing: Akins and Beyond, 147 University of Pennsylvania Law Review 147 (1999), S. 613–675.

Ders. (Hrsg.): Behavioral Law and Economics, Cambridge, MA 2000.

Ders.: Gesetze der Angst, Frankfurt am Main 2007.

Swedish Post and Telecom Agency: Which services and networks are subject to the electronic Communication Act? – Guidance, Stockholm 2009.

Sweren-Becker, *Eliza*: Congress Working in the Dark on Cybersecurity Bill, American Civil Liberties Union (ACLU) vom 17.11.2015, online abrufbar: https://www.aclu.org/blog/free-future/congress-working-dark-cybersecurity-bill (zuletzt abgerufen am 30. April 2017).

Sydow, *Gernot*: Verwaltungskooperation in der Europäischen Union: zur horizontalen und vertikalen Zusammenarbeit der europäischen Verwaltungen am Beispiel des Produktzulassungsrechts, Tübingen 2004.

Ders.: Staatliche Verantwortung für den Schutz nichtstaatlicher Geheimnisse. Eine Rekonstruktion des Geheimnisschutzrechts, Die Verwaltung 38 (2005), S. 35–64.

Ders.: Die Vereinheitlichung des mitgliedstaatlichen Vollzugs des Europarechts in mehrstufigen Verwaltungsverfahren, Die Verwaltung 34 (2001), S. 517–542.

Taeger, *Jürgen*: die Entwicklung des IT-Rechts im Jahr 2014, Neue Juristische Wochenschrift 2014, S. 3759–3765.

Ders./Gabel, *Detlev* (Hrsg.): BDSG und Datenschutzvorschriften des TKG und TMG, 2. Auflage, Frankfurt am Main 2013.

Terhaag, *Michael*: IT-Sicherheitsgesetz: Auswirkungen, Entwicklung und Materialien für die Praxis, Köln 2015.

Terhechte, *Jörg Philipp*: Europäisches Verwaltungsrecht und europäisches Verfassungsrecht, in: Terhechte, Jörg Philipp (Hrsg.), Verwaltungsrecht der Europäischen Union, Baden-Baden 2011, § 7, S. 273–306.

Ders.: Die föderalen Strukturen der Europäischen Union und das europäische Verwaltungsrecht, in: Härtel, Ines (Hrsg.), Handbuch Föderalismus – Föderalismus als demokratische Rechtsordnung und Rechtskultur in Deutschland, Europa und der Welt, Berlin 2012, § 89, S. 449–475.

Teufer, *Tobias*: „Too much Information"? – Aktuelles zur staatlichen Kommunikation im Lebensmittelrecht, Kommunikation und Recht 2013, S. 629–633.

Thomé, *Sarah*: Die Unabhängigkeit der Bundedatenschutzagentur, Verbraucher und Recht 2015, S. 130–133.

Tinnefeld, *Marie-Theres*/*Buchner*, *Benedikt*/*Petri*, *Thomas*: Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht, 5. Auflage, München 2012.

Tridimas, *Takis*: General Principles of EU Law, 2. Auflage, Oxford 2007.

Trute, *Hans-Heinrich*: Regulierung – am Beispiel des Telekommunikationsrechts, in: Eberle, Carl-Eugen, Ibler, Martin, Lorenz, Dieter (Hrsg.), Festschrift Winfried Brohm, Der Wandel des Staates von den Herausforderungen der Gegenwart, 2002, S. 169–189.

Ders.: Wissen – Einleitende Bemerkungen, in: Röhl, Hans Christian (Hrsg.), Wissen – Zur kognitiven Dimension des Rechts, Die Verwaltung, Beiheft 9, Berlin 2010, S. 11–38.

Ders.: Staatslehre als Sozialwissenschaft?, in Schulze-Fielitz, Helmuth (Hrsg.), Staatslehre als Wissenschaft, Die Verwaltung, Beiheft 7, Berlin 2007, S. 115–137.

Ders.: Die demokratische Legitimation der Verwaltung, in: Hoffmann-Riem, Wolfgang, Schmidt-Aßmann, Eberhard, Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts, Band I: Methoden – Maßstäbe – Aufgaben – Organisation, 2. Auflage, München 2012, § 6, S. 341–436.

Ders.: Wissenschaft und Technik, in: Isensee, Josef, Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts, Band IV: Aufgaben des Staates, 3. Auflage, Heidelberg 2006, § 88, S. 747–782.

Ders.: Katastrophenschutzrecht – Besichtigung eines verdrängten Rechtsgebiets, Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft 2005, S. 342–363.

Ders.: Der europäische Regulierungsverbund in der Telekommunikation: ein neues Modell europäisierter Verwaltung, in: Osterloh, Lerke, Schmidt, Karsten, Weber, Hermann, Staat, Wirtschaft, Finanzverfassung: Festschrift für Peter Selmer zum 70. Geburtstag, Berlin 2004, S. 565–586.

Ders.: Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer 57 (1998), S. 216–273.

Ders./Spoerr, *Wolfgang*/*Bosch*, *Wolfgang* (Hrsg.): Telekommunikationsgesetz mit FTEG, Reprint 2001, Berlin 2011.

Turner, *Fred*: From counterculture to cyberculture : Stewart Brand, the Whole Earth Network, and the rise of digital utopianism, Chicago 2008.

Tversky, *Amos*/*Kahnemann*, *Daniel*: Judgment under Uncertainty: Heuristics and Biases, Science 185 (1974), S. 1124–1131.

Tversky, *Amos*/*Kahnemann*, *Daniel*: Extensional Versus Intuitive Reasoning: The Conjunction Fallacy in Probability Judgment, Psychological Review 90 (1983), S. 293–315.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: Stellungnahme zum IT-Sicherheitsgesetz-Entwurf, 13.02.2015, online abrufbar: https://www.datenschutzzentrum.de/artikel/877-ULD-Stellungnahme-zum-IT-Sicherheitsgesetz-Entwurf.html (zuletzt abgerufen am 30. April 2017).

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: Stellungnahme zum Referentenentwurf des Bundesministerium des Inneren eines Gesetzes zur Erhöhung der Sicherheit informationstechnische Systeme (IT-Sicherheitsgesetz), 20.10.2014, online abrufbar: https://www.datenschutzzentrum.de/uploads/it/20141021-it-sicherheitsgesetz.pdf (zuletzt abgerufen am 30. April 2017).

University of California-Berkeley School of Law: Security Breach Notification Laws: Views from Chief Security Officers, Dezember 2007, online abrufbar: https://www.law.berkeley.edu/files/cso_study.pdf (zuletzt abgerufen am 30. April 2017).

Vedder, *Christoph*/*Heintschel von Heinegg*, *Wolff* (Hrsg.): Europäisches Unionsrecht. EUV, AEUV, Grundrechte-Charta, Handkommentar, Baden-Baden 2012.

Vesting, *Thomas*: Die Bedeutung von Information und Kommunikation für die verwaltungsrechtliche Systembildung, in: Hoffmann-Riem, Wolfgang, Schmidt-Aßmann, Eberhard, Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts, Band II: Informationsordnung – Verwaltungsverfahren – Handlungsformen, 2. Auflage, München 2012, § 20, S. 1–34.

Ders.: Die Medien des Rechts: Schrift, Weilerswist 2011.

Ders.: Zwischen Gewährleistungsstaat und Minimalstaat. Zu den veränderten Bedingungen der Bewältigung öffentlicher Aufgaben in der „Informations- oder Wissensgesellschaft", in: Hoffmann-Riem, Wolfgang, Schmidt-Aßmann, Eberhard (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, Baden-Baden 2000, S. 101–131.

Viellechner, *Lars*: Transnationalisierung des Rechts, Weilerswist 2013.

Vilain, *Yoan*: Demokratische Legitimität und Verfassungsmäßigkeit unabhängiger Regulierungsbehörden: Von den ursprünglichen Bedenken bis zur richterlichen Eingliederung in das französische Verwaltungssystem, in: Masing, Johannes, Marcou, Gérard (Hrsg.), Unabhängige Regulierungsbehörden: Organisationsrechtliche Herausforderungen in Frankreich und Deutschland, Tübingen 2010, S. 9–38.

Viscusi, *Kip*/*Vernon*, *John*/*Harrington*, *Joseph*: Economics of Regulation ans Antitrust, 4. Auflage, Cambridge, MA USA 2005.

Vogel, *Joachim*: Towards a Global Convention against Cybercrime, in: First World Conference of Penal Law. Penal Law in the XXIst Century, Guadalajara (Mexico) 2007, online abruf-

bar: http://www.penal.org/sites/default/files/files/Guadalajara-Vogel.pdf (zuletzt abgerufen am 30. April 2017).

Voßkuhle, *Andreas*: Beteiligung Privater an der Erfüllung öffentlicher Aufgaben und staatliche Verantwortung, Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer 62 (2003), S. 266–335.

Ders.: Sachverständige Beratung des Staates, in: Isensee, Josef, Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts, Band III: Demokratie – Bundesorgane, 3. Auflage, Heidelberg 2005, § 43, S. 425–475.

Ders.: Neue Verwaltungsrechtswissenschaft, in: Hoffmann-Riem, Wolfgang, Schmidt-Aßmann, Eberhard, Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts, Band I: Methoden – Maßstäbe – Aufgaben – Organisation, 2. Auflage, München 2012, § 1, S. 1–64.

Waechter, *Kay*: Geminderte demokratische Legitimation staatlicher Institutionen im parlamentarischen Regierungssystem: zur Wirkung von Verfassungsprinzipien und Grundrechten auf institutionelle und kompetenzielle Ausgestaltungen, Berlin 1994.

Wählisch, *Matthias*/*Schmidt*, *Thomas*/*Brün*, *Markus de*/*Häberlen*, *Thomas*: Exposing a Nation-Centric View on the German Internet – A Change in Perspective on AS-level, in: Taft, Nina, Ricciato, Fabio (Hrsg.), Proc. of the 13th Passive and Active Measurement Conference (PAM), Lecture Notes in Computer Science, Volume 7192, Berlin, Heidelberg 2012, S. 200–210.

Wahl, *Rainer*/*Masing*, *Johannes*: Schutz durch Eingriff, JuristenZeitung 1990, S. 553–563.

Weber, *Harald*: Historische und verfassungsrechtliche Grundlagen eines öffentlichen Informationszugangsrechts, Recht der Datenverarbeitung 2005, S. 243–251.

Weber, *Max*: Wirtschaft und Gesellschaft: Grundriss der verstehenden Soziologie, Nachdr. 5. Auflage hrsg. von Johannes Winckelmann, Tübingen 2013.

Weber, *Rolf*: Internet-Governance, in: Hoeren, Thomas, Sieber, Ulrich, Holznagel, Bernd (Hrsg.), Handbuch Multimedia-Recht, Teil 2, 42. Ergänzungslieferung, München 2015.

Wegener, *Bernhard*: Der geheime Staat: Arkantradition und Informationsfreiheitsrecht, Göttingen 2006.

Ders.: Aktuelle Fragen der Umweltinformationsfreiheit, Neue Zeitschrift für Verwaltungsrecht 2015, S. 609–616.

Wegener, *Christoph*/*Heidrich*, *Joerg*: Neuer Standard – Neue Herausforderungen: IPv6 und Datenschutz, Computer und Recht 2011, S. 479–484.

Weingart, *Peter*/*Carrier*, *Martin*/*Krohn*, *Wolfgang* (Hrsg.): Nachrichten aus der Wissensgesellschaft. Analysen zur Veränderung der Wissenschaft, Weilerswist 2007.

Weiß, *Wolfgang*: Dezentrale Agenturen in der EU-Rechtsetzung, in: Europarecht 2016, S. 631–665.

Weisser, *Niclas-Frederic*: Das Gemeinsame Terrorismusabwehrzentrum (GTAZ) – Rechtsprobleme, Rechtsform und Rechtsgrundlage, Neue Zeitschrift für Verwaltungsrecht 2011, S. 142–146.

Wentzel, *Joachim*: Agenturen im deutschen Verwaltungskontext: Nachzügler oder Vorreiter?, Die Öffentliche Verwaltung 2010, S. 763–771.

Werle, *Raymund*/*Schimank*, *Uwe* (Hrsg.): Gesellschaftliche Komplexität und kollektive Handlungsfähigkeit, Frankfurt am Main 2000.

Werner, *Jann*: Kategorien der Policy-Forschung, Speyer 1981.

Wettner, *Florian*: Die Amtshilfe im europäischen Verwaltungsrecht, Tübingen 2005.

Wewer, *Göttrik*: Kollaborative Verwaltung: Forschungsstand und Perspektiven, Die Verwaltung 46 (2013), S. 563–572.

Wiater, *Patricia*: Sicherheitspolitik zwischen Staat und Markt: Der Schutz kritischer Infrastrukturen, Baden-Baden 2013.

Wiebe, *Andreas*: Zugang zu und Verwertung von Informationen der öffentlichen Hand, in: Metzger, Axel, Wimmers, Jörg (Hrsg.), DGRI Jahrbuch 2014, Köln 2015, S. 123–134.

Ders./Ahnefeld, *Elisabeth*: Zugang zu und Verwertung von Informationen der öffentlichen Hand – Teil I – Zugang zu Informationen und IFG, in: Computer und Recht 2015, S. 127–136.

Ders./Ahnefeld, *Elisabeth*: Zugang zu und Verwertung von Informationen der öffentlichen Hand – Teil II – Weiterverwendung von Informationen – Open Government und Open Data, in: Computer und Recht 2015, S. 199–208.

Wiedemann, *Richard*: Unabhängige Verwaltungsbehörden und die Rechtsprechung des Bundesverfassungsgerichts zur demokratischen Legitimation, in: Masing, Johannes, Marcou, Gérard (Hrsg.), Unabhängige Regulierungsbehörden: Organisationsrechtliche Herausforderungen in Frankreich und Deutschland, Tübingen 2010, S. 39–52.

Wielsch, *Dan*: Zugangsregeln: die Rechtsverfassung der Wissensteilung, Tübingen 2008.

Ders.: Die epistemische Analyse des Rechts. Von der ökonomischen zur ökologischen Rationalität in der Rechtswissenschaft, JuristenZeitung 2009, S. 67–77.

Wille, *Angelo*: Die Pflicht der Organe der Europäischen Gemeinschaft zur loyalen Zusammenarbeit mit den Mitgliedstaaten, Baden-Baden 2003.

Willke, *Helmut*: Smart Governance: governing the Global Knowledge Society, Frankfurt am Main 2007.

Ders.: Dystopia: Studien zur Krisis des Wissens in der modernen Gesellschaft, Frankfurt am Main 2002.

Ders.: Einführung in das systemische Wissensmanagement, 3. Auflage, Heidelberg 2011.

Wirtz, *Sonja*/*Brink*, *Stefan*: Die verfassungsrechtliche Verankerung der Informationszugangsfreiheit, Neue Zeitschrift für Verwaltungsrecht 2015, S. 1166–1173.

Wolf, *Rainer*: „Herrschaft kraft Wissen" in der Risikogesellschaft, Soziale Welt 39 (1988), S. 164–187.

Wolff, *Hans*/*Bachof Otto*/*Stober Rolf*/*Kluth*, *Winfried*: Verwaltungsrecht Band II, 7. Auflage, München 2010.

Wolff, *Heinrich Amadeus*/*Brink*, *Stefan* (Hrsg.): Datenschutzrecht in Bund und Ländern, Kommentar, München 2013.

Wolff, *Heinrich Amadeus*/*Brink*, *Stefan* (Hrsg.): Beck'scher Online-Kommentar Datenschutzrecht, 19. Edition, München 2017.

Wolff, *Josephine*: Cybersecurity Legislation Is Too Short-Sighted, Slate, 29.04.2015, online abrufbar: http://www.slate.com/blogs/future_tense/2015/04/29/pcna_cisa_information_sharing_cybersecurity_legislation_is_too_short_sighted.html (zuletzt abgerufen am 30. April 2017).

Wollenschläger, *Burkard*: Wissensgenerierung im Verfahren, Tübingen 2009.

Wollenschläger, *Ferdinand*: Staatliche Verbraucherinformation als neues Instrument des Verbraucherschutzes. Möglichkeiten und Grenzen der Informationsbefugnis nach dem Verbraucherinformationsgesetz am Beispiel der Pankower Ekelliste und das Problem staatlicher Marktinformation, Verwaltungsarchiv 102 (2011), S. 20–50.

Würtenberger, *Thomas*: Polizei- und Ordnungsrecht, in: Ehlers, Dirk, Fehling, Michael, Pünder, Hermann (Hrsg.), Besonderes Verwaltungsrecht, Band 3, 3. Auflage, Heidelberg 2013, § 69, S. 398–556.

Würtenberger, *Thomas*: Legitimität, Legalität, in: Brunner, Otto, Conze, Werner, Koselleck, Reinhart (Hrsg.), Geschichtliche Grundbegriffe: Historisches Lexikon zur politisch-sozialen Sprache in Deutschland, Band 3, Stuttgart 1982, S. 677–740.

Zech, *Herbert*: Information als Schutzgegenstand, Tübingen 2012.

Zheng, *Denise*/*Lewis*, *James*: Cyber Threat Information Sharing – Recommendations for Congress and the Administration, Washington 2015, online abrufbar: http://csis.org/files/publication/150310_cyberthreatinfosharing.pdf (zuletzt abgerufen am 30. April 2017).

Zilioli, *Chiara*/*Selmayr*, *Martin*: The European Central Bank: An Independent Specialized Organization of Community Law, Common Market Law Review 2000, S. 591–643.

Ziller, *Jacques*: Introduction: les concepts d'administration directe, d'administration indirect et de co-administration et les fondements du droit administrative Européen, in: Auby, Jean-Bernard, Dutheil de la Rochère, Jacqueline (Hrsg.), Droit Administratif Européen, Brüssel 2007, S. 235–243.

Zöller, *Mark Alexander*: Der Rechtsrahmen der Nachrichtendienste bei der „Bekämpfung" des internationalen Terrorismus, JuristenZeitung 2007, S. 763–771.

Zöllner, *Wolfgang*: Informationsordnung und Recht, Berlin 1990.

Zuleeg, *Manfred*: Das Recht der europäischen Gemeinschaften im innerstaatlichen Bereich, Köln 1969.

Sachregister