Univ.-Prof. Dr. jur. Dirk Heckmann

Institut für IT-Sicherheit und Sicherheitsrecht
Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht
Forschungsstelle für IT-Recht und Netzpolitik

Gutachterliche Stellungnahme

auf Anfrage der Enquete-Kommission Internet und Digitale Gesellschaft
Projektgruppe Zugang, Struktur und Sicherheit im Netz
anlässlich des Expertengesprächs „Sicherheit im Internet“ am 28. November 2011

---

unter Mitarbeit der wissenschaftlichen Mitarbeiter

Florian Albrecht, Ermano Geuer, Axel Knabe, Beatrice Lederer
Marc Maisch und Alexander Seidl

Passau, den 25. November 2011

Gottfried-Schäffer-Str. 20 94032 Passau
www.mein-jura.de heckmann@uni-passau.de

Zusammenfassende Thesen

1. Die „Sicherheit im Netz“ herzustellen bzw. zu gewährleisten gehört zu den elementaren Herausforderungen eines Gemeinwesens im Informationszeitalter, das durch zunehmende Vernetzung, einen zunehmenden Einsatz smarter Technologien und den politischen Willen zum Aufbau einer medienbruchfreien Verwaltung geprägt ist.

2. „Sicherheit im Netz“ bezieht sich sowohl auf die Infrastrukturebene (insbesondere: Verfügbarkeit von Information und Kommunikation sowie Stabilität des Netzes) als auch auf die Anwendungsebene (insbesondere: Vertraulichkeit und Unversehrtheit von Information und Kommunikation). Hier soll verkürzt von IT-Sicherheitsgewährleistung gesprochen werden.

3. Die IT-Sicherheitsgewährleistung ist eine Aufgabe „zur gesamten Hand“, an der sowohl der Staat als auch die Wirtschaft und die Gesellschaft als Akteure und Profiteure des Internet mitzuwirken haben.

4. Dem Staat als Friedens- und Ordnungsmacht kommt aber eine besondere Infrastrukturverantwortung für das Netz zu, weil das Internet eine höchst bedeutungsvolle und zugleich erheblich gefährdete Infrastruktur darstellt.

5. Aus dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht) erwächst in seiner objektiven Dimension auch eine Schutzpflicht des Staates zur IT-Sicherheitsgewährleistung.

6. Diese verfassungsrechtliche Pflicht betrifft das „Ob“ der IT-Sicherheitsgewährleistung für das Internet. Für das „Wie“, insbesondere Umfang und Instrumente der Schutz- und Förderpflichten, hat der Staat einen Gestaltungsspielraum.

7. In einem abgestuften Schutzpflichtenkonzept ist auf der 1. Stufe zunächst die verfassungsrechtliche Pflicht des Staates zur Entwicklung, Ausbau und Weiterentwicklung einer IT-Sicherheitsstrategie zu nennen. Auf eine solche Strategie ganz zu verzichten wäre ein Verstoß gegen das Untermaßverbot.

8. Die Bundesregierung hat im Februar 2011 eine Cyber-Sicherheitsstrategie für Deutschland beschlossen und bereits zuvor im Juni 2009 die Nationale Strategie zum Schutz kritischer Infrastrukturen (KRITIS). Damit hat sie der 1. Stufe der Schutzpflicht zur IT-Sicherheitsgewährleistung Rechnung getragen.

9. Es wäre allerdings wünschenswert, dass im Rahmen diese „Cyberstrategie“ unter Berücksichtigung neuer Gefährdungslagen und Verantwortungsstrukturen u.a. Aspekte einer zunehmend offeneren Kommunikationskultur (z.B. soziale Medien), der Sicherheitsverantwortung der Internetnutzer (Selbstschutz und Fremdverantwortung) sowie

der zunehmenden Datenverknüpfung und automatisierten Programmabläufen in Plug-and-Play-Umgebungen einfließen. Hier besteht die Herausforderung einer koordinierten Gesamtstrategie in der Gemengelage punktueller Gefährdungsfaktoren.

10. Auf einer 2. Stufe beinhaltet die Schutzpflicht zur IT-Sicherheitsgewährleistung auch die Aufgabe, die strategischen Ziele und Instrumente in die Rechts-, Wirtschafts- und Sozialordnung zu implementieren. Dies ist auf verschiedene Art und Weise bereits realisiert worden. Zu nennen sind in institutioneller Hinsicht die Einrichtung eines Nationalen Cyberabwehrzentrums sowie die Aufgabenverteilung zwischen BSI und Bundesnetzagentur. In regulatorischer Hinsicht besteht allerdings eher eine Ansammlung einzelner Schutzvorschriften und Sicherheitsstandards, insbesondere im TKG, TMG, BDSG, StGB, und diverser sicherheitsrechtlicher und zivilrechtlicher Vorschriften. Angesichts des weiteren Gestaltungsspielraums des Gesetzgebers auf der operativen Ebene kann insoweit (noch) kein Verstoß gegen die Schutzpflicht auf IT-Sicherheitsgewährleistung festgestellt werden.

11. Es wäre allerdings erwägenswert (ohne dass dies hier abschließend beurteilt werden kann), Ideen für ein IT-Sicherheitsrecht zu entwickeln, die entweder in ein IT-Sicherheitsgesetz oder eine punktuelle Ergänzung vorhandener Gesetze einfließen könnten. Hierzu zählen etwa die Haftung für unsichere IT-Umgebungen, Kriterien zur Bestimmung des erforderlichen IT-Sicherheitsniveaus oder die Versicherbarkeit von IT-Risiken.

12. Auf einer 3. Stufe beinhaltet die Schutzpflicht zur IT-Sicherheitsgewährleistung schließlich die Obliegenheit einer „Hilfe zur Selbsthilfe“. Dahinter steht ein sicherheitsrechtlicher Subsidiaritätsgrundsatz: Soweit sich der Staat im Hinblick auf IT-Sicherheitsgefährdungen regulatorisch zurückhält (was ihm außerhalb der kritischen Infrastrukturen auch mit Blick auf seinen Gestaltungsspielraum erlaubt ist), muss er die Akteure befähigen, selbstbestimmt und eigenverantwortlich einen Beitrag zur Sicherheit der Informationstechnik zu leisten. Dies setzt einerseits eine erhöhte Sensibilität für IT-spezifische Gefährdungen und andererseits die Kenntnis und Verfügbarkeit entsprechender Abwehrmechanismen voraus. An dieser Stelle untätig zu bleiben, verletzt das Untermaßverbot.

13. Es wäre zum Beispiel wünschenswert, dass Medienkompetenz auf allen Ebenen über das bisher vorhandene Maß hinaus in die Bildungspolitik aufgenommen wird. Dies setzt die Erkenntnis voraus, dass Lehrer auf dem Gebiet der Medienkompetenz nicht nur lehren, sondern zunächst auch lernen müssen. Angesichts der Tatsache, dass Kinder und Jugendliche im Internet vielfach Opfer, aber auch (Mit-) Täter von IT-Sicherheitsgefährdungen sind, muss „Sicherheit im Netz“ auch und gerade über diese Altersgruppe initiiert werden.

Inhalt

A. Einleitung

Wir leben in einer vernetzten Welt. Die Informations-, Kommunikations- und Netzwerktechnologien (kurz: IT) sind gerade aus der Informationsgesellschaft nicht mehr wegzudenken. Dies gilt für den privaten und gesellschaftlichen Bereich ebenso wie für Wirtschaft und Staat. IT ist in allen Lebensbereichen zum zentralen Bestandteil nicht nur der Kommunikation, sondern auch der Steuerung jeglicher Geschäftsprozesse und technischen Anlagen sowie der Verwaltung des Gemeinwesens geworden.[1] Denn Vernetzung beschleunigt und erleichtert viele Prozesse und trägt so zur Wertschöpfung, Produktivitätssteigerung und kulturellen Vielfalt bei.

Zugleich erhöht Vernetzung jedoch die Abhängigkeit eines jeden Akteurs von der dahinter stehenden Infrastruktur. Die Informationstechnologie wird zusehends zum „Unsicherheitsfaktor". Die Infrastruktur an sich kann dabei ebenso zum Ziel von (willkürlichen) Angriffen und Gegenstand von (unwillkürlichen) Gefahren werden wie einzelne Anwendungen oder einzelne Informationen.

Ob und, wenn ja, was der Staat zur Sicherheit im Internet beitragen kann und beitragen muss, avanciert so zur entscheidenden Weichenstellung für die Zukunft der Informationsgesellschaft.

Eine derartige internetspezifische Sicherheitsinfrastruktur ist daher unerlässlich. Um sie entwerfen zu können, sind vorab die Dimensionen der *Sicherheit im Internet* zu benennen. Zwar sind sowohl die Forderung nach Sicherheit als auch der Begriff des Internet fest im allgemeinen Sprachgebrauch verankert.[2] Zur juristischen Analyse und Aufarbeitung genügt dieses Alltagsverständnis jedoch nicht.

I. IT-Sicherheit: Sicherheit im Internet

1. Sicherheit

Sicherheit ist kein originärer terminus technicus der Rechtswissenschaften, auch wenn er ihr nicht fremd ist.[3] Der Inhalt ist daher primär etymologisch zu erschließen. Demnach lässt sich Sicherheit als Zustand beschreiben,[4] in dem der Einzelne bzw. ein Kollektiv frei von schädlichen Einflüssen Dritter oder der Natur ist.[5] Damit wohnt dem Begriff Sicherheit eine wertende Komponente inne. Wann nämlich ein Einfluss „schädlich" ist, bedarf der Bestimmung, die regelmäßig aus der Sicht des (oder der) Betroffenen erfolgt

[1] BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07 u.a. – „Online-Durchsuchung" - ZUM 2008, 301, 310;*Gaycken/Karger*, MMR 2011, 3, 3.
[2] Vgl. nur die Ausführungen zum Begriff „Sicherheit" in Brockhaus Enzyklopädie Online, 2005-2011.
[3] So enthalten Rechtswörterbücher wie *Creifelds* Rechtswörterbuch oder das „Fachlexikon Recht" von *Alpmann/Brockhaus* keine Definition des Sicherheitsbegriffs.
[4] *Heckmann,* Sicherheitsarchitektur im bedrohten Rechtsstaat, in: *Blaschke/Förster/Lumpp/Schmidt*, Sicherheit statt Freiheit?, 2005, S. 9, 11.
[5] Vgl. *Heckmann,* Sicherheitsarchitektur im bedrohten Rechtsstaat, in: *Blaschke/Förster/Lumpp/Schmidt,* Sicherheit statt Freiheit?, 2005, S. 9, 11.

und schon deshalb subjektive Elemente enthält (die allerdings in einem übergeordneten Normierungsprozess auch objektiviert werden können). In diesem Verständnis ist Sicherheit über die Zustandsbeschreibung hinaus eine Zielbestimmung, die es allen voran durch politisches Handeln zu konkretisieren gilt.[6]

Den etymologischen Gehalt zugrunde gelegt kann Unsicherheit, verstanden als Gefahr für den Zustand der Sicherheit, sowohl von der Natur (was in einem weiteren Sinne auch Friktionen innerhalb von komplexen technischen Systemen einschließt) als auch von Dritten ausgehen. Um Sicherheit im Internet zu gewährleisten, müssen beide Unsicherheitsfaktoren bedacht werden. Gerade angesichts der eingangs skizzierten Abhängigkeit der Informationsgesellschaft von der IT soll vorliegend die Unsicherheit, die von intentionalem Handeln Dritter ausgeht, in den Mittelpunkt gestellt werden.

2. Internet

Die Konkretisierung des Sicherheitsbegriffs wäre jedoch unvollständig, wenn sie nicht einem Objekt zugeordnet würde. Diese Spezifikation wird grundsätzlich durch die Bezugnahme auf das Internet erreicht. Um der Komplexität der Sicherheit im Netz gerecht zu werden, ist allerdings eine weitere Aufschlüsselung erforderlich: Zum einen ist „das Internet" funktional-technisch auszudifferenzieren (a). Zum anderen sind die Dimensionen der „Sicherheit im Netz" näher zu betrachten (b).

a) Funktional-technische Betrachtung des Internet

Um Sicherheit effektiv gewährleisten zu können, ist eine funktional-technische Betrachtung des Internet unerlässlich. Dabei ist entsprechend den Kommunikationsaufgaben, die im Internet erfüllt werden, zwischen einzelnen funktionalen Ebenen zu differenzieren.

Das auf das World Wide Web zugeschnittene *TCP/IP-Referenzmodell* (Transmission Control Protocol/Internet Protocol) unterscheidet zwischen 1) Netzzugangsschicht (z.B. LAN, WLAN); 2) Internetschicht (insb. IP); 3) Transportschicht (z.B. TCP) und 4) Anwendungsschicht (z.B. http, DNS, FTP).

Differenzierter ist das *OSI-Referenzmodell,* das auch die Netzwerkkommunikation einbezieht. Es unterscheidet sieben Schichten: 1) Bitübertragungsschicht; 2) Sicherungsschicht; 3) Vermittlungsschicht; 4) Transportschicht; 5) Sitzungsschicht; 6) Darstellungsschicht und 7) Anwendungsschicht.

Beide Referenzmodelle lassen erkennen, dass das Internet zu komplex und vielschichtig ist, um nach einheitlichen Instrumenten zur Gewährleistung von Sicherheit im Internet

[6] Ausführungen zum Begriff „Sicherheit" in Brockhaus Enzyklopädie Online, 2005-2011. Vgl. *Thiel*, Die „Entgrenzung" der Gefahrenabwehr, 2010, S. 179 ff.

zu suchen. „Die“ Sicherheit im Internet gibt es nicht. Es gibt nur die Sicherheit einer jeden Schicht.

b) Dimensionen der Sicherheit im Internet

Die Gewährleistung von „Sicherheit im Internet“ lässt sich nicht allein durch eine rechtliche Betrachtung erreichen. IT-Sicherheit steht vielmehr im Spannungsfeld von Organisation, Technik und Recht.[7] Sicherheit im Internet verlangt technische und organisatorische Maßnahmen. Dazu zählen grundlegende Vorkehrungen wie die Kontrolle von Zutritt, Zugang und Zugriff auf Datenverarbeitungsanlagen.

Diese technischen und organisatorischen Maßnahmen stellen sich (unabhängig von der Begründung bestimmter Pflichten und ihrer Durchsetzbarkeit) als Obliegenheit dar. Ihnen nachzukommen liegt im ureigensten Interesse des jeweiligen Verwenders – sei es der Staat, sei es die Wirtschaft oder sei es die Gesellschaft bzw. der einzelne Bürger.

Derartige Obliegenheiten können durch den Staat zu rechtlichen Pflichten transformiert werden, die rechtsförmig durchsetzbar und erzwingbar sind. So sieht das Gesetz zum Beispiel die Kontrolle von Zutritt, Zugang und Zugriff auf Datenverarbeitungsanlagen als verpflichtend an, wenn personenbezogene Daten automatisiert verarbeitet oder genutzt werden, Anlage zu § 9 Satz 1 BDSG.

Demnach ist Sicherheit im Internet einerseits die *Sicherheit des Internet (an sich)*, also die Sicherheit der Verfügbarkeit der Infrastruktur und der grundlegenden Kommunikationsmöglichkeiten. Andererseits erfasst sie auch die *Sicherheit im Internet (also bei den Internetanwendungen)*, womit auch und besonders Anforderungen an die Vertraulichkeit und Integrität elektronischer Kommunikation erfasst werden.

Daneben existieren webbasierte Kriminalitätsformen, die das *Internet als Tatort oder als Tatmittel* missbrauchen.[8] Hierunter fallen vielfältige Verletzungsformen, die von Persönlichkeitsrechtsverletzungen bis hin zur organisierten Industrie- und Wirtschaftsspionage reichen. Die Rechtsgutverletzung kann dabei außerhalb des Internet eintreten. Entscheidend ist, dass das Internet Tatort oder Tatmittel ist. Denn es ermöglicht die Rechtsverletzung erst oder erleichtert sie unter Umständen durch die Möglichkeit zum anonymen Handeln. Auch diese Dimension, die *Sicherheit vor Internetkriminalität* ist in die Architektur eines Sicherheitsrechts einzubeziehen, zumal nicht selten organisatorische und/oder technische Maßnahmen maßgeblich zur Sicherheitsgewährleistung beitragen können (z.B. die technische Ausgestaltung von Bewertungsplattformen)[9].

---

[7] *Heckmann,* MMR 2006, 280.
[8] Vgl. *Heckmann,* jurisPK-Internetrecht, 3. Aufl. 2011, Kap. 8 Rn. 14 ff.
[9] Vgl. die Anforderungen, die der BGH im „spickmich“-Urteil aufstellt, BGH v. 23.06.2009 – VI ZR 196/08 – NJW 2009, 2888.

Das Internet kann aber nicht nur Gegenstand der (Un-)Sicherheit, nicht nur Ort oder Mittel zur Generierung von Unsicherheit sein. Es kann auch zur Gewährleistung der Sicherheit beitragen. *Sicherheit durch das Internet*, der Instrumente wie Online-Streifengänge, Ermittlungen in sozialen Netzwerken oder weiter reichende Eingriffe wie Online-Durchsuchungen dienen, ist als „Sicherheitsfaktor" bei der Bestimmung der Eckpunkte des IT-Sicherheitsrechts zu beachten. Dass die Anwendung solcher webbasierter „Sicherheitsinstrumente" ihrerseits Risiken birgt, zeigt die aktuelle Diskussion um den sog. Staatstrojaner[10].

3. Sicherheit im Internet

Die Vielschichtigkeit des Begriffs der Sicherheit sowie seines Objekts, des Internet, macht deutlich, dass Sicherheit im Internet mehr ist als IT-Sicherheit verstanden als Datensicherheit[11]. *Sicherheit im Internet* ist Sicherheit des Internet an sich, Sicherheit auf Anwendungsebene und Sicherheit vor Internetkriminalität.

Bei der Bestimmung des Ziels der Modellierung der Sicherheit im Internet bietet sich eine Orientierung an § 2 Abs. 2 BSIG an. Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität sind zu gewährleisten.[12] Dies gilt auf allen Ebenen des Internet – wenn auch mit jeweils unterschiedlicher Gewichtung.

II. Architektur der Sicherheit im Internet

Innerhalb der Sicherheitsarchitektur des Netzes ist weiterhin nach Gefahrenquellen zu unterscheiden. „Quelle der Unsicherheit" können einerseits (natürliche oder juristische) Personen sein. Unsicherheit kann intentional erzeugt werden. Aber der Mensch ist auch vor sich selbst und damit vor einfachem „menschlichen Versagen" zu schützen. Auch unwillkürlich können Personen zum Unsicherheitsfaktor werden. Die Unsicherheit kann andererseits durch äußere Umstände generiert werden.[13]

Unabhängig davon, welches (normativ zu konkretisierende) Sicherheitsniveau bei der Sicherheitsarchitektur zugrunde gelegt wird (2.), sind beide Unsicherheitsfaktoren in den Blick zu nehmen. Dies gilt für alle Akteure der Sicherheitsgewährleistung (1.).

1. Akteure der Sicherheitsgewährleistung

Ein wesentlicher Akteur der Gewährleistung der Sicherheit im Internet ist der *Staat*. Dies lässt sich nicht nur auf die etymologische, sondern vor allem auf eine rechtliche Betrachtung stützen: Zum einen ist die öffentliche Gewalt grundrechtsverpflichtet, Art. 1 Abs. 3 GG. Sie hat nicht nur die abwehrrechtliche Komponente der Grundrechte zu be-

[10] Hierzu *Braun/Roggenkamp*, K&R 2011, 681 ff.
[11] Zum Verständnis als Datensicherheit *Kramer/Meints,* in: Hoeren/Sieber, Handbuch Multimedia-Recht, 28. EL 2011, Teil 16.5 Rn. 3.
[12] Vgl. *Kramer/Meints,* in: Hoeren/Sieber, Handbuch Multimedia-Recht, 28. EL 2011, Teil 16.5 Rn. 3.
[13] Vgl. die grundlegende Unterscheidung zwischen Beeinträchtigungen durch Dritte und Beeinträchtigungen durch die Natur.

achten, sondern auch die objektive Wertordnung zu wahren, die sich aus einer Gesamtschau des Grundgesetzes ergibt. Zum anderen ist der Rechtsstaat seinen objektiven, ebenfalls verfassungsrechtlich verankerten Prinzipien verpflichtet: Er hat Rechtssicherheit zu gewährleisten.

In welchem Umfang der Staat in diesem Rahmen zum Sicherheitsfaktor werden kann und/oder werden muss, ist im Einzelfall anhand Untermaßverbot und Verhältnismäßigkeitserwägungen zu bestimmen (vgl. im Folgenden B I und II).

Dies gilt ebenso für die Frage, ob und wenn ja in welchem Umfang die „Sicherheitsakteure" *Gesellschaft* und *Wirtschaft* zur Verantwortung gezogen werden. Das Verhältnis von informationeller Selbstverantwortung eines jeden Akteurs zum Konzept der „Hilfe zur Selbsthilfe" und zu konkreten staatlichen, den Einzelnen entlastenden Handlungspflichten ist im Rahmen der IT-sicherheitsrechtlichen Pflichtenfolge zu klären (B III).

2. Relativität des Sicherheitsbegriffs

Bei der Ausgestaltung der IT-sicherheitsrechtlichen Pflichten ist aus rechtlicher Sicht zweierlei zu beachten: zum einen die Einschätzungsprärogative des Gesetzgebers, die dazu führt, dass nur in Ausnahmefällen konkret verpflichtende Vorgaben zur Ausgestaltung der Architektur der Sicherheit im Internet gemacht werden können.

Zum anderen ist der Begriff der Sicherheit relativ.[14] Absolute Sicherheit gibt es angesichts umfassender Bedrohungslagen nicht. Auch das Gesetz fordert sie nicht – weder das Grundgesetz noch das einfache Recht. Dies ist vor dem Hintergrund des Grundsatzes *impossibilium nulla est obligatio* folgerichtig. Das grundrechtliche Spannungsfeld, in dem sich die Sicherheit im Internet bewegt, verstärkt diese Relativität des Sicherheitsbegriffs.

Sicherheit im Internet ist daher vor dem Hintergrund des Grundsatzes der Verhältnismäßigkeit normativ zu definieren und bestmöglich zu gewährleisten. Es gilt, Freiheit und Sicherheit mit Blick auf die Zukunft der Informationsgesellschaft auszutarieren.[15]

Daraus folgt auch, dass Maßnahmen und Maßgaben zur IT- und Internetsicherheit kaum wirksam werden können, wenn nicht geklärt ist, von welchem Sicherheitsniveau hierbei ausgegangen werden kann bzw. soll.

---

[14] Zur Relativität der IT-Sicherheit im Besonderen *Gaycken/Karger,* MMR 2011, 3, 4.
[15] Umfassend hierzu *Heckmann,* Sicherheitsarchitektur im bedrohten Rechtsstaat, in: *Blaschke/Förster/Lumpp/Schmidt*, Sicherheit statt Freiheit?, 2005, S. 9 ff.

B. Der staatliche Schutz- und Gewährleistungsauftrag im Bereich der IT-Sicherheit

I. Die normative Durchdringung der IT durch die informationelle Selbstbestimmung und das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme

Das Bundesverfassungsgericht hat in den letzten Jahren in mehreren wegweisenden Entscheidungen das Verhältnis von Staat und IT unter verschiedenen Gesichtspunkten in den Blick genommen und verfassungsrechtlich gewürdigt. Insbesondere das Jahr 2008 markierte hierbei einen „Wendepunkt" mit Blick auf eine normative Durchdringung des Lebensbereichs der IT. Neben mehreren anderen wegweisenden Entscheidungen dieses Jahres[16] hat insbesondere die verfassungsrechtliche Würdigung der Online-Durchsuchung[17] die Entstehung einer IT-bezogenen Dimension des Verfassungsrechts eingeleitet. In der Ableitung des neuen Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[18] hat das Bundesverfassungsgericht den Schutz des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i.V.m. Art 1 Abs.1 GG insbesondere um die zusätzliche Schutzrichtung der Integritätserwartung mit Blick auf die durch die Bürger in ihrem Alltag genutzten informationstechnischen Systeme erweitert. Während die erste Schutzrichtung der Vertraulichkeit der im informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten im Zweifel schon durch den Gewährleistungsgehalt des informationellen Selbstbestimmungsrechts Schutz erfährt,[19] wird durch die zweite Schutzrichtung der grundrechtliche Schutzumfang ergänzt und in Inhalt und Reichweite vorverlagert. Denn in die Integrität des informationstechnischen Systems wird nach der Entscheidung des Bundesverfassungsgerichts grundsätzlich schon dann eingegriffen, wenn durch Systeminfiltration durch Dritte für diese die Möglichkeit besteht, Leistungen, Funktionen und Speicherinhalte des Systems zu nutzen bzw. fremdzusteuern. Dafür ist es weder nötig, dass eine durch die Systeminfiltration ermöglichte Maßnahme tatsächlich ausgeführt noch dass eine so durchgeführte Maßnahme erfolgreich ist.[20] Ebenso wenig ist der Integritätsschutz auf solche Maßnahmen beschränkt, welche die Erhebung, Speicherung oder Verarbeitung personenbezogener Daten zu Ziel haben. Auch solche durch Systeminfiltration ermöglichten Maßnahmen, deren Ziel beispielsweise die Nutzung von Systemleistungen und -funktionen erstreben, sind vom Schutzbereich umfasst. Aufgrund der Tatsache, dass das Bundesverfassungsgerichts in seinem Urteil zudem den Schutz informationstechnischer

[16] BVerfG, Urt. v. 11.03.2008 – 1BvR 2074/05 u.a. – „Kfz-Kennzeichenerfassung" - NJW 2008, 1505; BVerfG, v. 11.03.2008 – 1BvR 256/08 – „Vorratsdatenspeicherung" – MMR 2009, 29.
[17] BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07 u.a. – „Online Durchsuchung" - ZUM 2008, 301, 310.
[18] Kurz auch Online-Grundrecht oder IT-Grundrecht.
[19] Vgl. zur Abgrenzung zu anderen Grundrechten, *Hornung*, CR 2008, 301 ff.

Systeme nicht notwendig nur auf heimliche Maßnahmen erstreckt[21] ist es grundsätzlich zudem möglich, die mit Blick auf die Online-Durchsuchung ausformulierte Schrankensystematik in manchen Fällen auch auf nicht-heimliche Infiltrationsszenarien zu übertragen. Bei der Frage, welche Art informationstechnischer Systeme dem Schutzbereich des IT-Grundrechts unterfallen, hat das Bundesverfassungsrecht das Grundrecht mit Weitblick für neue technische Entwicklungen offengehalten und daher nicht durch einen zu technikzentrierten Definitionsansatz künstlich verkürzt. Daher ist zunächst jedes System erfasst, das eine Kapazität zur Erhebung personenbezogener Daten besitzt. Für die Zuordnung eines Systems zum Schutzbereich kommt es weiter auf die konkreten Speicher- und Verarbeitungskapazitäten des informationstechnischen Systems an. Die Systemkapazitäten zur Datenverarbeitung müssen es grundsätzlich gestatten, entweder alleine oder in technischer Vernetzung mit anderen informationstechnischen Systemen eine Verarbeitungs- und Erhebungskapazität zu realisieren, durch die ein Systemzugriff weite Bereiche der persönlichen Lebensgestaltung oder sogar ein umfassendes Persönlichkeitsprofil offenlegen könnte. Dabei kommt es allein auf die Kapazität des einzelnen Systems an, nicht ob derlei Dateninhalte im Einzelfall tatsächlich vorliegen.

II. Grundrechtliche Schutzpflicht zur Gewährleistung von IT-Sicherheit

Das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art 1 Abs. 1 GG hat in seiner Ausprägung als Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme die aus der informationellen Selbstbestimmung durch das Bundesverfassungsgericht deduzierten Schutzpflichten um eine IT-spezifische Schutzpflichtendimension erweitert.[22] Damit hat das Gericht das Verhältnis von IT und Staat in letzter Konsequenz in die umfassende Wertordnung des Grundgesetzes eingepflegt und damit der objektiven Wertordnung des Grundgesetzes in seiner vollen Breite geöffnet.

1. Begründung der Schutzpflichtendimension

Grundrechte verkörpern eine „objektive Wertordnung" des Grundgesetzes, „die als verfassungsrechtliche Grundentscheidung für alle Bereiche des Rechts gilt."[23] Sie bilden insoweit einen übergreifenden verfassungsrechtlichen Maßstab und Gewährleistungsanspruch für alle Teile der Rechtsordnung und der staatlichen Handlungsträger. Auf der Grundlage dieser objektiven Wertentscheidung hat das Bundesverfassungsgericht in seiner Rechtsprechung grundsätzlich anerkannt, dass Grundrechte nicht nur einen Abwehranspruch gegen staatlich-hoheitliches Handeln beinhalten, sondern auch unmittel-

[21] Vgl. die Formulierung „insbesondere", BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07 u.a. – „Online Durchsuchung" - ZUM 2008, 301, 310, 313..
[22] Die folgenden Ausführungen sind angelehnt an *Heckmann*, Staatliche Schutz- und Förderpflichten zur Gewährleistung von IT-Sicherheit – Erste Folgerungen aus dem Urteil des Bundesverfassungsgerichts zur „Online-Durchsuchung", in: Rüßmann (Hrsg.), Festschrift für Gerhard Käfer 2009, S. 129 ff.
[23] Ständige Rspr. des Bundesverfassungsgerichts; vgl. nur BVerfG, Beschl. v. 22.03.2004 – 1 BvR 2248/01; BVerfGE 7, 198, 205; BVerfGE 6, 55, 72.

bare grundgesetzlich verankerte Schutzpflichten begründen können. Diese haben das Ziel, die grundrechtlichen Schutz- und Rechtsgüter durch staatliches Handeln vor Beeinträchtigungen nichtstaatlichen Ursprungs zu sichern.[24] Danach sind gerade die staatlichen Handlungsträger verpflichtet, sich schützend und fördernd vor die Rechts- und Schutzgüter der grundrechtlichen Freiheitsgewährleistungen zu stellen. Es entsteht auf diese Weise eine Mehrheit an Grundrechtsfunktionen, nämlich einerseits die Verpflichtung des Staates, nicht gerechtfertigte Eingriffe zu unterlassen (abwehrrechtliche Dimension der Grundrechte) und andererseits seine Pflicht, nicht gerechtfertigte Beeinträchtigungen von dritter Seite präventiv und repressiv zu bekämpfen (Schutzpflichtdimension der Grundrechte). Die einem Grundrecht innewohnenden „zwei Pflichtenaspekte“[25] der Abwehr und des Schutzes ergänzen sich so zu einem umfassenden Gewährleistungsanspruch grundrechtlich garantierter Rechts- und Schutzgüter gegenüber staatlichen und nichtstaatlichen Eingriffen bzw. Beeinträchtigungen. Dabei lassen sich die originären Ursprünge staatlicher Schutzpflichten auf die staatstheoretisch begründete Verpflichtung des Staates als übergeordnete Friedens- und Ordnungsmacht zurückführen, die Bürger vor Beeinträchtigungen ihrer Freiheit und Sicherheit zu schützen. Verfassungsrechtlich legitimiert und konkretisiert wird dieses zunächst staatstheoretische Prinzip sodann durch die grundrechtlich verankerten und gewährleisteten Rechts- und Schutzgüter. Aus dem zuvor Gesagten lassen sich grundrechtliche Schutzpflichten dann begründen, wenn grundrechtliche Rechtsgüter in ihrem Bestand gefährdet werden oder wenn die mit einem Grundrecht verbundene Freiheitsausübung (wesentlich) erschwert oder vereitelt wird und sich diese Gefährdung – in Abgrenzung bzw. in Erweiterung zu der abwehrrechtlichen Dimension der Grundrechte – auch und gerade auf nichtstaatliche Gefahrenquellen zurückführen lässt.

Auch das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 in seiner Ausprägung als Recht auf Vertraulichkeit und Integrität von informationstechnischen Systemen nimmt grundsätzlich an beiden Pflichtenaspekten des Grundrechtsschutzes gleichermaßen teil. Denn es verkörpert als Ausfluss des allgemeinen Persönlichkeitsrechts konsequenterweise einen Teil der objektiven Wertordnung des Grundgesetzes und nimmt damit auch an dessen Wirkungen teil. Insoweit stellen sich im Lichte der Ausführungen des Bundesverfassungsgerichts die Vertraulichkeit und Integrität informationstechnischer Systeme und damit wichtige Aspekte der IT-Sicherheit als Grundbedingung und Wesensmerkmal der heutigen Gesellschaft mit stetig wachsendem Verbrei-

[24] BVerfGE 49, 89, 142; BVerfGE 46, 160 ff. Darüber hinaus besteht eine Vielzahl anderer durchaus unterschiedlicher Handlungsansätze. Diese reichen von dem Rückgriff auf das Sozialstaatsprinzip, über den Menschenwürdegehalt des Art. 1 Abs.1 GG bis hin zur erweiternden Auslegung der abwehrrechtlichen Dimension der Grundrechte (sog. Kongruenztheorie). Ausführlich zu diesen unterschiedlichen Begründungsansätzen *Szczekalla*, Die sogenannten grundrechtlichen Schutzpflichten, 2002, S. 143 ff. jeweils m.w.N.

[25] So *Isensee*, Das Grundrecht auf Sicherheit, 1983, S. 33.

tungsgrad und Bedeutungsgehalt zugleich als elementare Voraussetzung bzw. notwendige Umweltbedingung dar. Ohne deren Existenz kann die Nutzung der Informationstechnologie durch den Bürger grundrechtskonform nicht mehr gewährleistet werden.[26] Gerade aufgrund dieses Verständnisses der (sicheren) Informationstechnologie als einer der Wesensmerkmale der modernen Gesellschaft, muss diese zugleich als eine Grundvoraussetzung für die Wahrnehmung einer Vielzahl grundrechtlicher Freiheiten verstanden werden. Die Vertraulichkeit und Integrität informationstechnischer Systeme wird somit zu einer Art „Querschnittsbedingung" für die Grundrechtsausübung des Einzelnen, die einen prägenden und bestimmenden Einfluss auf die Effektuierung der grundrechtlichen Gewährleistungsbereiche haben kann. Zugleich hat das Bundesverfassungsgericht im „Online-Durchsuchungsurteil" ein allgemeines Bedrohungspotential an Persönlichkeitsgefährdungen beschrieben, welches nicht nur auf staatliche Eingriffe rekurriert, sondern vielmehr an die Risiken und Gefahren für die Persönlichkeitsentfaltung anknüpft, die durch eine Verletzung der Vertraulichkeit und Integrität informationstechnischer Systeme entstehen können, gerade wenn und weil der Bürger auf deren Nutzung angewiesen ist.[27] Dabei differenziert das Urteil bei der Darstellung der IT-spezifischen Bedrohungssituationen grundsätzlich nicht zwischen privaten und staatlichen Gefahrenquellen, sondern spricht von einer Gefährdung durch den Zugriff „Dritter". Der insoweit betonte Schutz vor staatlichem Zugriff wird in einem direkten Bezug zum Recht auf informationelle Selbstbestimmung gesetzt, welches gerade nicht allein in seiner abwehrrechtlichen Dimension anerkannt ist, sondern vielmehr auch an der Schutzpflichtendimension teilnimmt. Da es insoweit bei der Ableitung des neuen Grundrechts gerade um die Beseitigung von Schutzlücken ging, ist es nicht ersichtlich, warum diese Schutzlücken auf der abwehrrechtlichen Seite beseitigt, dann aber auf der schutzpflichtbezogenen Seite hinsichtlich der nicht-staatlichen Bedrohungslagen offen gelassen werden sollen. Die Gewährleistung grundrechtlicher Rechts- und Schutzgüter ist in diesem Sinne vollständig und eben nicht nur partiell auszugestalten.

2. Umfang der grundrechtlichen Schutzpflicht

Der inhaltliche Umfang und die Reichweite der grundrechtlichen Schutzpflicht zur Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme entsprechen dem komplementären Schutzbereich des korrespondierenden Freiheitsrechts, d.h. der Reichweite und dem Regelungsgehalt der abwehrrechtlichen Dimension. Es begründet in diesem Sinne einen Schutz- und Gewährleistungsauftrag des Staates mit dem

[26] So schreibt das Bundesverfassungsgericht in seinem Urteil zur Online-Durchsuchung: „Aus der Bedeutung der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung und aus den Persönlichkeitsgefährdungen, die mit dieser Nutzung verbunden sind, folgt ein grundrechtlich erhebliches Schutzbedürfnis. Der Einzelnen ist darauf angewiesen, dass der Staat die mit Blick auf die ungehinderte Persönlichkeitsentfaltung berechtigten Erwartungen an die Integrität und Vertraulichkeit derartiger Systeme achtet." BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, jurisRdnr. 163.
[27] BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, jurisRdnr. 182.

Ziel der Vermeidung und Bekämpfung nicht-staatlicher Eingriffe, die darauf abzielen, durch Infiltration, Manipulation und Ausforschung informationstechnischer Systeme einen (unbefugten) Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erlangen. Die beiden durch das Bundesverfassungsgericht ins Spiel gebrachten Merkmale der Vertraulichkeit und Integrität knüpfen dabei an den Definitionsmerkmalen eines übergreifenden IT-Sicherheitsbegriffs (wenn auch nicht deckungsgleich so doch aber weitgehend) an. Denn IT-Sicherheit ist regelmäßig dann gewährleistet, wenn die in einem informationstechnischen System hinterlegten Informationen für jeden Nutzer, der hierzu berechtigt ist (Vertraulichkeit) mit genau dem Inhalt, den ihr Urheber geschaffen hat (Integrität), immer dann, wenn dies erforderlich (und vereinbart) ist (Zugänglichkeit), verfügbar sind, wobei die Informationen jedem Urheber in dem Maße zurechenbar sein müssen, in dem der Zweck der Informationsverarbeitung diese Zurechnung erfordert (Verbindlichkeit).[28] Geht man insoweit davon aus, dass die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gerade Ausdruck und Grundbedingung einer umfassenden Gewährleistung der grundrechtsbezogenen IT-Sicherheit ist, kann – zumindest in diesem Kontext – der Begriff der IT-Sicherheit für die Umschreibung des Schutzbereichs des neuen Grundrechts verwendet werden. Darüber hinaus ließe sich auch darüber nachdenken, den Anwendungsbereich des neuen Grundrechts nicht nur auf die Begriffe Vertraulichkeit und Integrität im engeren Sinne zu beschränken, sondern vielmehr über die direkt genannten Begriffe hinaus in einem umfassenden Sinne an dem Begriff und dem Verständnis der IT-Sicherheit anzuknüpfen und auch andere Aspekte der IT-Sicherheit in den Schutzbereich des neuen Grundrechts einzubeziehen.

Dies begründet allerdings keinen umfassenden IT-Sicherheitsgewährleistungsanspruch des Bürgers in dem Sinne, dass der Staat jegliche Maßnahme wahrzunehmen hätte, die tatsächlich oder aus Sicht des Bürgers vermeintlich zur Erhöhung des (abstrakten oder konkreten) IT-Sicherheitsniveaus führt. Das notwendige und mögliche Maß an Schutz ist insoweit von den betroffenen Schutz- und Rechtsgütern, deren Rang, den vorhandenen Schutzmaßnahmen, den kollidierenden Schutz- und Rechtsgütern sowie den rechtlichen und tatsächlichen Rahmenbedingungen abhängig, in deren Kontext die grundrechtliche Schutzpflicht steht.[29] Dies bezieht insbesondere die Grundrechte Dritter mit ein. Dabei muss auch der Vorbehalt des Möglichen, insbesondere unter dem Aspekt der staatlichen Leistungsfähigkeit, berücksichtigt werden.[30] Die grundrechtlichen Schutzpflichten sind

[28] So die Definition der IT-Sicherheit bei *Heckmann*, in: Hill/Schliesky, Herausforderung e-Government, 2009, S. 131. Vgl. zu den Schutzzielen des IT-Sicherheitsrechts *Heckmann*, MMR 2006, 280 ff.
[29] BVerfGE 49, 89, 142; *Steinberg*, NJW 1996, 1985, 1987 f.
[30] BVerfGE 49, 89, 142 – „Kalkar I": „OB, wann und in mit welchem Inhalt sich eine solche Ausgestaltung [rechtlicher Regelungen] von Verfassungs wegen gebietet, hängt von der Art und dem Rang des verfassungsrechtlich geschützten Rechtsguts sowie von den schon vorhandenen Regelungen ab."

demnach *dynamische und final-programmierte Optimierungsgebote*,[31] auf deren Basis es zu einer Reduktion des staatlichen Gestaltungsspielraums und damit zur Entstehung abgestufter Handlungs- und Unterlassungspflichten im Anwendungsbereich des IT-Grundrechts bzw. im Bereich der IT-Sicherheit kommen kann, die gemeinsam auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ausgerichtet sind. Im Sinne eines unabdingbaren Minimalstandards sind in diesem Sinne zunächst die Grundentscheidung und Grundverantwortung des Staates für eine aktive und effektive Gewährleistung der IT-Sicherheit („Ob"), aber auch die Verpflichtung zur Vornahme grundlegender und elementarer Maßnahmen und Strukturentscheidungen („Wie") zu nennen, deren Fehlen einer evidenten Verletzung der grundrechtlich geschützten Rechts- und Schutzgüter gleichkäme. Eine Verdichtung zu einer Handlungspflicht im Sinne einer konkreten Einzelmaßnahme[32] kann es nur dort geben, wo eine bestimmte Maßnahme zum elementaren Schutz der Rechtsgüter des IT-Grundrechts unbedingt erforderlich ist und die damit verfolgten Schutzinteressen andere durch diese Maßnahme betroffene und insoweit beeinträchtigte oder vernachlässigte Interessen wesentlich überwiegen. Das kann insbesondere dort der Fall sein, wo es um solche Bestandteile der IT-Infrastruktur geht, „bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden." (so die Definition des BSI für Kritische Infrastrukturen[33]). Hier trifft den Staat eine besondere Infrastrukturverantwortung.

3. Infrastrukturverantwortung des Staates

a) Vernetzung und kritische Infrastrukturen

Aus der Tatsache, dass die Informationstechnik „die zentrale Infrastruktur des 21. Jahrhunderts"[34] ist, können sich unter Umständen auch in diesem Zusammenhang Schutzpflichten des Staates ergeben. Konkret können diese etwa aus dem Gedanken folgen, dass der Staat in den Bereichen, in denen er den Ausbau und die Entwicklung der Informationstechnologie tatsächlich an sich zieht, mithin die Aufgabe der IT-Gestaltung rechtlich oder tatsächlich in einer bestimmten Weise determiniert, auch die Verantwortung für die grundrechtskonforme Ausgestaltung der Informationstechnologie übernehmen muss. In Anbetracht des Umstandes, dass der Staat die Entwicklung der IT allerdings grundsätzlich (zu Recht) der gesellschaftlichen Entwicklung überlässt, findet sich insoweit in der Regel nur dort ein Ansatzpunkt, wo der Staat selbst in die Verantwortung für IT tritt, d.h. im Bereich der staatlichen (IT)Selbstversorgung. Dies betrifft insbesondere die Bereiche der staatlichen informationstechnischen Systeme und Netze. Dabei darf

[31] Hierzu BVerfGE 49, 89, 90.
[32] Vgl. hierzu *Brüning*, Jus 2000, 955, 959.
[33] https://www.bsi.bund.de/ContentBSI/Themen/Kritis/Einfuehrung/KritisDefinitionen/definitionen.html
[34] So der damalige Bundesinnenminister *Wolfgang Schäuble*, zitiert nach Behördenspiegel 5/2008, S. 43.

aber nicht übersehen werden, dass neuen, insbesondere extraterritorialen bzw. entgrenzten Gefahrenszenarien ausreichend Rechnung getragen werden muss. Gerade in den Bereichen des Cyberterrorismus und des Cyberwar führen die durch zunehmende Vernetzung herbeigeführten „technosozialen Abhängigkeiten“[35] zu neuen Verwundbarkeiten im Bereich kritischer Infrastrukturen, die nichtstaatliche (Terrorismus) und staatliche Angreifer mit unter Umständen verheerenden Folgen ausnutzen können. Kritische Infrastrukturen[36] lassen sich insoweit als jedenfalls solche Einrichtungen, Anlagen, Dienste und Systeme bezeichnen, auf die Staat und Gesellschaft existenziell angewiesen sind und deren Ausfall bzw. Störung zu gravierenden Schäden für das Gemeinwesen, Wirtschaft und Bevölkerung sowie den Einzelnen führen würde.[37] Gerade deren Vernetzungsgrad und die Folgen eines Ausfalls bzw. einer nachhaltigen Störung lassen IT-Infrastrukturen daher grundsätzlich als kritische Infrastrukturen erscheinen.[38] Dabei kann und darf es grundsätzlich keinen Unterschied machen, ob sich derlei kritische Infrastrukturen in öffentlicher oder privater Hand befinden. Die herausragende Bedeutung der informationstechnologischen Vernetzung für das Gemeinwohl und in letzter Konsequenz für den Fortbestand des Staates geben diesem aus dem Schutz- und Gewährleistungsgehalt des IT-Grundrechts jedenfalls die Aufgabe an die Hand, durch ausreichende gesetzliche Regelungen auch die Verantwortung der Privatwirtschaft für diese „wesentlichen Lebensadern“ des modernen Staatswesens sicherzustellen. Die seitens der Bundesregierung im nationalen Plan zum Schutz der Informationsstrukturen (NPSI)[39] vorgegebenen strategischen Ziele der Prävention, Reaktion und Nachhaltigkeit zusammen mit den institutionellen Koordinierungsstellen Bundesamt für Sicherheit in der Informationstechnologie (BSI) und Nationales Cyberabwehrzentrum geben in diesem Bereich grundsätzlich ein ausreichendes Instrumentarium im Rahmen des weiten gesetzgeberischen Ermessens- und Umsetzungsspielraums an die Hand.

b) Verhältnismäßigkeit der IT-Sicherheitsanforderungen

Dabei darf allerdings mit Blick auf die besondere Bedeutung der Informationsstrukturen für die „Überlebensfähigkeit“ des Staates das auch in den öffentlich-rechtlichen Anforderungen zur IT-Sicherheit kodifizierte Verhältnismäßigkeitsprinzip[40] mit Blick auf die

---

[35] Zum Begriff vgl. *Gaycken/Karger*, MMR 2011, 3, 4.

[36] Nach der Definition des BSI sind **Kritische Infrastrukturen** „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“ Als Kritische Infrastrukturen werden vom BSI aufgeführt: Transport und Verkehr, Energie, Gesundheit, Informationstechnik und Telekommunikation, Finanz- und Versicherungswesen, Wasser, Ernährung, Staat und Verwaltung sowie Medien und Kultur.

[37] Vgl. hierzu die Definition in Art. 2a) der Richtlinie 2008/114/EG des Rates über die Ermittlung und Ausweisung kritischer Infrastrukturen v. 8.12.2008, ABl. EG Nr. L 345, S. 75;

[38] So auch *Gaycken/Karger*, MMR 2011, 3, 4. Vgl. auch die Aufzählung des BSI

[39] Abrufbar unter http://www.eco.de/dokumente/Nationaler_Plan_Schutz_Informationsinfrastrukturen_%282%29.pdf.

[40] Vgl. z.B. die §§ 9 BDSG, 25a KWG, 109 TKG.

weitreichenden Folgen auch systemischer Störungen nicht überstrapaziert werden. Auch mit Blick auf kritische IT-Infrastrukturen ist insoweit eine absolute – also lückenlose, alle erdenklichen Schadensfälle im Bereich der Prävention und Abwehr bzw. Folgenminderung berücksichtigende – IT-Sicherheit nicht erzielbar. Dieser Grundsatz muss aber bei der Prüfung der Erforderlichkeit zugleich neue, dynamische Schadenszenarien und deren unmittelbare und mittelbare Folgen für das Staatsganze ausreichend berücksichtigen. Insbesondere betrifft dies auch die erhebliche Gefährdung durch staatliche und nicht-staatliche (terroristische) Informationsoperationen und dagegen in Frage kommende Abwehrmaßnahmen. Es ist in diesem Bereich dem grundrechtlichen Schutz- und Gewährleistungsauftrag des Staates jedenfalls auch zuzurechnen, mögliche völkerrechtliche und kriegsvölkerrechtliche Unsicherheiten im Rahmen nationaler, europäischer und internationaler Kooperationen so weitgehend als möglich zu reduzieren. Das betrifft in wesentlichem Maße die Frage, ob und inwieweit staatliche aktive Netzverteidigung im Rahmen des Selbstverteidigungsrechts nach Art. 51 der UN-Charta oder völkergewohnheitsrechtlich unterhalb dieser Schwelle mit wesensgleichen Mitteln zulässig sein kann. Zugleich stellt sich in beiden Zusammenhängen das Problem, inwieweit etwaige Verteidigungsmaßnahmen gegen das territoriale Hoheitsgebiet eines unbeteiligten Staates (z.B. im Rahmen terroristischer Angriffe) völkerrechtlich zulässig sein können. Dabei können die durch den Internationalen Gerichtshof aufgestellten Grundsätze zur Staatenverantwortlichkeit[41] allenfalls einen Ausgangspunkt für eine völkerrechtliche Beurteilung bilden, ob derartige Abwehrmaßnahmen zulässigerweise in die Souveränität des Drittstaates eingreifen.[42] Es ist daher den staatlichen Handlungsträgern jedenfalls auch aufgetragen, auf internationaler Ebene auf die Herstellung entsprechender Rechtssicherheiten hinzuwirken, sei es durch bi- oder multilaterale Kooperationen oder neue völkerrechtliche Verträge, welche die kriegsvölkerrechtlichen Aspekte staatlicher Informationsoperationen konkretisieren. Soweit die Nichtidentifizierbarkeit von Angreifern eine Gegenwehr aufgrund fehlender Attributionsmöglichkeit ausscheiden lässt, müssen insoweit die fehlenden Reaktionsmöglichkeiten durch weiterführende Maßnahmen der Prävention, Nachhaltigkeit oder Folgenminderung ausgeglichen werden.

c) Entnetzung

Dies kann letztlich als ultima ratio in gewissen Bereichen auch eine abgestufte Entnetzung besonders kritischer Bereiche zur Folge haben.[43] Damit ist gemeint, dass einzelne kritische IT-Infrastrukturen vom Netz gehen. Dieser Aspekt, der bei der Privatwirtschaft

[41] Vgl. den Corfu Channel Case des Internationalen Gerichtshofes aus dem Jahre 1949 in dem er verschiedene Grade der staatlichen Beteiligung und damit der Zurechenbarkeit von Handlungen Privater auf dessen Hoheitsgeiet herausgebildet hat. Diese sind: „toleration", sponsorship/support, „inability to act". Vgl. ICJ Rep 1949, 4 (22) (Corfu Channel Case [United Kingdom of Great Britain and Northern Ireland v. Albania])

[42] Vgl. zu alledem auch *Plate*, ZRP 2011, 200 ff.

[43] Vgl. hierzu *Gaycken/Karger*, MMR 2011, 3, 4.

schon teilweise auf der Agenda steht[44], wird auch im öffentlichen Bereich zunehmend diskussionswürdig sein. Das Problem an heutigen IT-Infrastrukturen ist deren vollständige Vernetzung, die auch zugleich das Einfallstor für alle Attacken bietet.[45] Um dem entgegenzuwirken, wird der Trend auf die Dauer mehr in Richtung Intranet für kritische Strukturen gehen, da entsprechende Sicherungsmaßnahmen im Rahmen des Internet nicht in hinreichender Form getroffen werden können. Die Abschottung eines Staates im Internet nach außen wäre nur dann effektiv möglich, wenn sich dieser vom Internet komplett abkoppelt und eine Art nationales Intranet schafft, was wiederum ein Szenario wäre, dass für die Wirtschaft inakzeptabel ist.[46] Es bedarf bei den IT-Infrastrukturen wohl in Zukunft vermehrt der Analyse, inwiefern diese als kritische Infrastruktur (Transport, Energie, Versorgung, etc.) einzustufen sind und bei Bejahung dessen eine Hinterfragung, ob deren Vernetzung mit Drittsystemen, wie dem Internet, tatsächlich geboten ist oder inwiefern nicht aus Gründen der Sicherheit darauf verzichtet werden kann;[47] dabei sind jedoch auch abgestufte Formen der Entnetzung denkbar.[48]

III. Abgestufte Sicherheitsgewährleistungspflicht des Staates aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG in seiner Ausprägung als IT-Grundrecht

Vorliegend wird vorgeschlagen, im Sinne einer (nicht notwendig abschließenden) IT-sicherheitsrechtlichen Pflichtenfolge drei größere Untergruppen zu bilden, innerhalb derer diejenigen Maßnahmen notwendig sind, die jenseits des unabdingbaren Minimalstandards (Untermaßverbot) anhand des zuvor angedeuteten Abwägungsmodells zu konkretisieren sind. Dabei hat das Bundesverfassungsgericht in anderem Kontext bereits festgestellt, dass eine staatliche Verantwortung zur Gewährleistung der Voraussetzungen selbst bestimmter Kommunikationsteilhabe gerade dann begründet ist, wenn es dem Einzelnen nicht mehr möglich und zumutbar ist, wirksamen Selbstschutz zu verwirklichen.[49] Dies weist auf den grundsätzlichen Vorrang des informationellen Selbstschutzes durch den Bürger hin, dem Vorrang gegenüber anderen, insbesondere grundrechtlich eingriffsintensiveren, Schutzmaßnahmen einzuräumen ist. Im Rahmen der für die IT-Sicherheitsgewährleistungspflicht des Staates anzunehmenden, abgestuften Pflichtenfolge trifft auf einer ersten Ebene zunächst den Bürger eine Obliegenheit zum informationellen Selbstschutz. Ist es dem Bürger aus tatsächlichen oder rechtlichen Gründen nicht oder nicht ausreichend möglich, einen solchen Selbstschutz zu verwirkli-

---

[44] *Müller*, VW 2011, 1680.
[45] *Gaycken/Karger*, MMR 2011, 3, 5.
[46] *Gaycken,* Zeit Online, 16. Juni 2011 - http://www.zeit.de/2011/25/USA-Internet-Kontrolle.
[47] *Gaycken/Karger*, MMR 2011, 3, 8.
[48] Erwähnenswert scheinen hier „Air Gap"-Systeme, die Kommunikation nur in eine Richtung erlauben, so dass z.B. Malware ins System zwar gelangen kann, aber keine Daten an Dritte versenden kann. Dazu *Gaycken/Karger*, MMR 2011, 3, 8 m.w.N.
[49] BVerfG, Urt. v. 23.10.2006 – 1 BvR 2027/02, jurisRdnr. 29 und Orientierungssatz 2c.

chen, ist der Staat aufgefordert, Mechanismen und Instrumente zur nachhaltigen Beseitigung des Schutzdefizits bereitzustellen.[50] Der Ermöglichung von „Hilfe zur Selbsthilfe“ (z.B. durch die Vermittlung von Medienkompetenz) ist als Mittel möglichst „souveränitätsschonender“ und freiheitssichernder Einflussnahme unmittelbaren staatlichen Eingriffshandlungen der Vorzug zu geben. Erst auf einer dritten und letzten Stufe kommen staatliche Handlungspflichten zu Eingriffen in andere grundrechtlich geschützte Freiheitsbereiche dann zum Zuge, wenn sie nicht durch Maßnahmen der ersten und zweiten Stufe substituierbar sind.

1. Pflicht zur Entwicklung, Ausbau und Weiterentwicklung einer IT-Sicherheitsstrategie

Kern der grundrechtlichen Schutzpflicht ist die Entwicklung und der Ausbau der rechtlichen Grundlagen zum Aufbau einer IT-Sicherheitsstrategie. Sie begründet insoweit eine Pflicht des Staates, die Kompetenzen und Befugnisgrundlagen im Bereich der IT-Sicherheit im Geiste der verfassungsrechtlichen Garantien aufzubauen bzw. weiterzuentwickeln und in diesem Sinne zur effektiven Verwirklichung und Gewährleistung der IT-Sicherheit in der Bundesrepublik Deutschland beizutragen. Vor dem Hintergrund des weiten gesetzgeberischen Ermessensspielraums wird sich im Einzelfall wohl nur in den seltensten Fällen eine konkrete Pflicht zur Ausgestaltung der Rechtsordnung oder konkreter zur Ausrichtung der IT-Sicherheitsstrategie in der einen oder andere Weise ableiten lassen. Gleichwohl ergibt sich eine allgemeine (Grund)Pflicht zur Beachtung und Berücksichtigung des – mit der vorliegenden grundrechtlichen Schutzpflicht verbundenen – Auftrags zur widerspruchsfreien und kohärenten Gewährleistung von IT-Sicherheit bis in die unterste Ebene der staatlichen Sicherheitsarchitektur. Dazu bedarf es einer expliziten IT-Sicherheitsstrategie. Gleichzeitig darf nicht übersehen werden, dass das Feld der Informationstechnologie überaus dynamisch und einem ständigen Wandel unterworfen ist. Daraus folgt die Notwendigkeit der permanenten Anpassung der Rahmenbedingungen und Grundlagen im Sinne einer effektiven Sicherheitsgewährleistung. In diesem Zusammenhang ist es dem Staat auch aufgetragen, durch gesetzgebereiches Handeln und Kooperation mit Privaten die tatsächlichen Rahmenbedingungen der IT-Sicherheit auf allen gesellschaftlichen Ebenen zu begleiten.

a) IT-Sicherheitsstrategie des Bundes

Am 17. Juni 2009 hat die Bundesregierung die „**Nationale Strategie zum Schutz Kritischer Infrastrukturen**“ (KRITIS) beschlossen. Im Dreiklang von Prävention, Reaktion und Nachhaltigkeit soll unter Einbindung von Bund, Ländern, Kommunen und der Privatwirtschaft das Schutzniveau für kritische Infrastrukturen erhöht werden. Der Umset-

[50] Vgl. zu diesem Umstand auch *Luch*, MMR 2011, 75, 77.

zungsplan (UP KRITIS)[51] bildet die Grundlage für eine langfristige Zusammenarbeit zwischen Wirtschaft und Staat. Dem UP KRITIS können zu diesem Zwecke umfangreiche Hinweise und Empfehlungen zum Aufbau bzw. der Verbesserung von bestehenden Risiko- und Krisenmanagementstrukturen entnommen werden.

Die teilnehmenden Unternehmen haben die im UP KRITIS beschriebenen Sicherheitsmaßnahmen freiwillig zu ihrem eigenen Standard erklärt und arbeiten nunmehr gemeinsam mit den eingebundenen staatlichen Stellen an der Realisierung übergreifender Maßnahmen. Ein Ergebnis dieser Zusammenarbeit ist der Leitfaden "Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement"[52], der Betreiber kritischer Infrastrukturen bei der strukturierten Ermittlung von Risiken, der darauf basierenden Umsetzung vorbeugender Maßnahmen sowie dem effektiven und effizienten Umgang mit Krisen unterstützt.

Am 23.02.2011 hat das Bundeskabinett zudem die neue **Cyber-Sicherheitsstrategie für Deutschland**[53] beschlossen und die mit dem UP KRITIS geschaffene Struktur an die Gefährdungslage angepasst. Ziel der Strategie ist, Cyber-Sicherheit in Deutschland auf einem hohen Niveau zu gewährleisten - ohne dabei die Chancen und den Nutzen des Cyber-Raums zu beeinträchtigen.[54]

Die Strategie beruht u.a. auf der Annahme, dass eine Cyber-Sicherheitsstrategie angesichts der verteilten Verantwortung von Staat, Wirtschaft und Gesellschaft nur dann erfolgreich sein kann, wenn alle Akteure gemeinsam und partnerschaftlich ihre jeweilige Aufgabe wahrnehmen.[55] Im Vordergrund des Maßnahmenpakets stehen zivile Ansätze. Diese werden ergänzt durch die Maßnahmen der Bundeswehr zum Schutz ihrer eigenen Handlungsfähigkeit und im Rahmen zugrunde liegender Mandate, um auf diese Weise Cyber-Sicherheit als Teil gesamtstaatlicher Sicherheitsvorsorge zu verankern.[56] Zielsetzung ist

- der verstärkte Schutz Kritischer Infrastrukturen vor IT-Angriffen und

---

[51] Aufrufbar über http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2007/Kritis.pdf;jsessionid=B42B88CFCAD3D9FE23B8D0A233FE2C79.2_cid231?__blob=publicationFile.
[52] Aufrufbar über http://www.bmi.bund.de/cae/servlet/contentblob/131080/publicationFile/14972/Leitfaden_Schutz_kritischer_Infrastrukturen.pdf.
[53] Aufrufbar über http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_download.pdf?__blob=publicationFile.
[54] BT-Drs. 17/5694 S. 1; http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2011/02/cyber_abwehr.html.
[55] http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_download.pdf?__blob=publicationFile, S. 4.
[56] http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_download.pdf?__blob=publicationFile, S. 5.

- der Schutz der IT-Systeme in Deutschland einschließlich einer Sensibilisierung der Bürgerinnen und Bürger.[57]

Zudem wird unter der Federführung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ein Nationales Cyber-Abwehrzentrum errichtet. Siehe hierzu sogleich unter b)

b) Institutionen für die Entwicklung und Umsetzung der IT-Sicherheitsstrategie

Zur Prävention, Information und Frühwarnung wurde auf Bundesebene das **sog. „Nationale Cyber-Abwehrzentrum"** geschaffen, um insbesondere im Bereich der organisierten Kriminalität und des Terrorismus Cyber-Angriffen effektiv begegnen zu können.

Das Cyber-Abwehrzentrum ist eine gemeinsame Informations- und Kooperations-Plattform zum schnellen Informationsaustausch und zur besseren Koordinierung von Schutz- und Abwehrmaßnahmen gegen IT-Sicherheitsvorfälle. Das Zentrum arbeitet unter Federführung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und direkter Beteiligung des Bundesamtes für Verfassungsschutz (BfV) und des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK) auch mit Bundeskriminalamt (BKA), Bundespolizei (BPol), Zollkriminalamt (ZKA), Bundesnachrichtendienst (BND) sowie der Bundeswehr als assoziierten Behörden sowie den aufsichtführenden Stellen über die Betreiber Kritischer Infrastrukturen zusammen. Auch die Länder sollen in Zukunft durch Einschaltung des IT-Planungsrates an das Abwehrzentrum angeschlossen werden. Eine Einbindung der Wirtschaft in das Cyber-Abwehrzentrum erfolgt mittelbar. Bereits bestehende Strukturen der beteiligten Behörden zur Wirtschaft wie z.B. im UP KRITIS sollen genutzt und konsequent ausgebaut werden.[58]

Das Abwehrzentrum ist Bestandteil der vom Bundesministerium des Innern erarbeiteten Cyber-Sicherheitsstrategie für Deutschland. Seine Aufgabe besteht darin, IT-Sicherheitsvorfälle schnell und umfassend zu bewerten und abgestimmte Handlungsempfehlungen zu erarbeiten. Dazu werden unter anderem Informationen über Schwachstellen in IT-Produkten ausgetauscht sowie IT-Vorfälle, Verwundbarkeiten und Angriffsformen analysiert. Das Abwehrzentrum beschäftigt sich mit Schwachstellen und deren Auswirkungen auf die Verfügbarkeit der Informations- und Kommunikationstechnik sowie die Integrität, Authentizität und Vertraulichkeit der sich darin befindenden Daten.[59] Die vom Abwehrzentrum erstellen Lagebilder werden insbesondere für den Cyber-Sicherheitsrat bzw. die Bundesregierung und die beteiligten Behörden er-

[57] http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2011/02/cyber_abwehr.html.
[58] BT-Drs. 17/5694, S. 4.
[59] BT-Drs. 17/5694, S. 4.

stellt.[60] Eine dauerhaft analytische oder operative Zusammenarbeit findet im Cyber-Abwehrzentrum hingegen nicht statt.[61]

Alle beteiligten Behörden arbeiten dabei unter Beibehaltung ihrer bisherigen gesetzlichen Befugnisse. Das Cyberabwehrzentrum ist keine eigenständige Behörde, weswegen eine gesetzliche Grundlage (Errichtungsgesetz) entbehrlich ist; die Rechtsgrundlage der Zusammenarbeit sind Kooperationsvereinbarungen.[62]

Rechte der Internetnutzer sollen durch die Arbeit des Cyber-Abwehrzentrums nicht berührt werden. Personenbezogene Daten werden durch das Abwehrzentrum in der Regel nicht verarbeitet. Sollte ausnahmsweise ein Austausch personenbezogener Daten erforderlich sein, erfolgt dieser ausschließlich zwischen den jeweils beteiligten Behörden und Stellen auf der Grundlage der für die jeweilige Behörde geltenden Gesetze und Vorschriften.[63]

Mit der Schaffung eines **Bundesamts für Sicherheit in der Informationstechnik (BSI)** im Jahr 1991 wandte sich der Staat sowohl an Nutzer als auch Hersteller von IT. Beim BSI handelt es sich um eine selbständige, dem Bundesministerium des Inneren unterstehende Bundesoberbehörde, § 1 BSIG. Durch das Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes[64] wurde der Aufgaben- und Befugnisbereich des BSI umfassend modernisiert und erweitert.

Das Bundesamt soll die Sicherheit in der Informationstechnik fördern, § 3 Abs. 1 Satz 1 BSIG. Hierzu nimmt es unter anderem folgende Aufgaben wahr: die Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes (§ 3 Satz 2 Nr. 1 BSIG), die Sammlung und Auswertung von Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen und die Zurverfügungstellung der gewonnenen Erkenntnisse für andere Stellen, soweit dies zur Erfüllung ihrer Aufgaben oder zur Wahrung ihrer Sicherheitsinteressen erforderlich ist (§ 3 Satz 2 Nr. 2 BSIG), die Untersuchung von Sicherheitsrisiken bei Anwendung der Informationstechnik sowie Entwicklung von Sicherheitsvorkehrungen, insbesondere von informationstechnischen Verfahren und Geräten für die Sicherheit in der Informationstechnik (IT-Sicherheitsprodukte), soweit dies zur Erfüllung von Aufgaben des Bundes erforderlich ist, einschließlich der Forschung im Rahmen seiner gesetzlichen Aufgaben (§ 3 Satz 2 Nr. 3 BSIG) und die Entwicklung von Kriterien, Verfahren und Werkzeugen für die Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen oder Komponenten und für die Prüfung und Bewertung der Kon-

[60] BT-Drs. 17/5694, S. 4.
[61] BT-Drs. 17/5694, S. 2.
[62] BT-Drs. 17/5694, S. 3.
[63] BT-Drs. 17/5694, S. 3.
[64] Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes v. 14.08.2009, BGBl I 2009 S. 2821 ff.

formität im Bereich der IT-Sicherheit (§ 3 Satz 2 Nr. 4 BSIG). Das BSI unterstützt des Weiteren die Polizeien und Strafverfolgungsbehörden bei der Wahrnehmung ihrer gesetzlichen Aufgaben (§ 3 Satz 2 Nr. 13 a BSIG). Diese Unterstützung darf nur gewährt werden, soweit sie erforderlich ist, um Tätigkeiten zu verhindern oder zu erforschen, die gegen die Sicherheit in der Informationstechnik gerichtet sind oder unter Nutzung der Informationstechnik erfolgen (§ 3 Satz 2 Nr. 13 Satz 2 BSIG).

Ein Hauptbetätigungsfeld ist das angesichts von Hacker-Angriffen eingerichtete Computer Emergency Response Team für Bundesbehörden (CERT-Bund). Es ist die zentrale Anlaufstelle für präventive und reaktive Maßnahmen bei sicherheitsrelevanten Vorfällen in Computersystemen. Hauptaufgaben des CERT-Bund sind unter anderem die Erstellung und Veröffentlichung präventiver Handlungsempfehlungen zur Schadensvermeidung sowie die Unterstützung bei der Reaktion auf IT-Sicherheitsvorfälle. Ferner ist es für die aktive Alarmierung der Bundesverwaltung bei akuten Gefährdungen zuständig und informiert darüber hinaus interessierte Privatpersonen über den Warn- und Informationsdienst Bürger-CERT.

Als zentrale Meldestelle für IT-Sicherheit sammelt das BSI Informationen über Sicherheitslücken und neue Angriffsmuster, wertet diese aus und gibt Informationen und Warnungen an die betroffenen Stellen oder die Öffentlichkeit weiter (vgl. § 4 BSIG sowie § 7 BSIG).[65]

Auch die **Bundesnetzagentur**[66] gewährleistet – jedenfalls mittelbar – die Verfügbarkeit von Informationen. Die Bundesnetzagentur hat unter anderem die zentrale Aufgabe, für die Einhaltung des Telekommunikationsgesetzes (TKG) zu sorgen. Damit stellt sie die Liberalisierung und Deregulierung des Telekommunikationsmarktes durch einen diskriminierungsfreien Netzzugang und effiziente Netznutzungsentgelte sicher. In diesem Bereich sorgt sie unter anderem für die Sicherstellung einer flächendeckenden Grundversorgung mit Telekommunikationsdienstleistungen (Universaldienstleistungen), für die Sicherstellung einer effizienten und störungsfreien Nutzung von Frequenzen sowie für die Wahrung der Interessen der öffentlichen Sicherheit.

c) Stiftung Datenschutz

Der aus staatlichen Schutzpflichten folgenden Pflicht zur Entwicklung, Ausbau und Weiterentwicklung einer IT-Sicherheitsstrategie kann der Staat angesichts der schnell vo-

[65] BT-Drs. 16/11967.

[66] Die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen ist eine selbständige Bundesoberbehörde im Geschäftsbereich des Bundesministeriums für Wirtschaft und Technologie.

ranschreitenden Entwicklung informationstechnologische Entwicklungen auch im Rahmen der Gründung und Finanzierung einer Stiftung Datenschutz gerecht werden.[67]

Die Errichtung einer solchen Stiftung ist gegenwärtig Gegenstand eines Abstimmungsprozesses innerhalb der Bundesregierung. Sie wird voraussichtlich in 2012 gegründet.[68] Die geplanten Aufgaben der Stiftung ergeben sich aus dem Koalitionsvertrag zwischen CDU, CSU und FDP.[69] Ein Schwerpunkt ihrer Tätigkeit wird auf den Bereichen Entwicklung eines Datenschutzzertifikats sowie Bildung und Aufklärung liegen.[70] Unabhängigkeit und Neutralität werden zentrale Eigenschaften der Stiftung sein.[71]

Mit der Einrichtung der Stiftung Datenschutz wird angesichts der zunehmenden Bedrohungen der informationellen Selbstbestimmung und der beschränkten Steuerungsfähigkeit des Rechts[72] ein neuer Ansatz zum Schutz personenbezogener Daten verfolgt.[73] *Bräutigam/Sonnleitner* stellen in diesem Zusammenhang zutreffend fest, dass das Datenschutzrecht in Zukunft vermehrt auf ein Zusammenspiel mit der Technik, dem Individuum und der Wirtschaft setzen muss.[74]

Einen Schwerpunkt der Tätigkeit der Stiftung Datenschutz könnte die Prüfung interner Datenverarbeitungsvorgänge von Unternehmen auf ihre Vereinbarkeit mit datenschutzrechtlichen Bestimmungen sein.[75] Es scheint daher sinnvoll, die Tätigkeit der Stiftung über den Verbraucherschutz hinausgehend im B2B-Bereich anzusiedeln.[76] Zudem könnte der Tätigkeitsbereich der Stiftung auch auf weitere Felder der IT-Sicherheit ausgeweitet werden.

Mit der Stiftung Datenschutz könnte dann ein wesentlicher Beitrag auf einem seitens des Gesetzgebers nur schwer erschließbaren Gebiet zur regulierten Selbstregulierung geleistet werden.[77]

---

[67] Hierbei könnte es sich sowohl um eine Stiftung bürgerlichen als auch um eine Stiftung öffentlichen Rechts handeln. So http://www.bfdi.bund.de/SharedDocs/Publikationen/KonzeptionStiftungDatenschutz.pdf?__blob=publicationFile.
[68] http://www.heise.de/newsticker/meldung/Datenschutz-Stiftung-kommt-erst-2012-1375810.html.
[69] BT-Drs. 17/6699, S. 1.
[70] BT-Drs. 17/6699, S. 2.
[71] Dies wird im Rahmen der Gestaltung der Stiftungsorgane und durch die Art der Finanzierung sichergestellt werden; BT-Drs. 17/6699, S. 2.
[72] Vgl. *Heckmann*, K&R 2010, 1, 5 ff.; zur Entwicklung hin zu einem „Smart Life" siehe *Heckmann*, K&R 2011, 1 und zur „fortschreitenden Virtualisierung" *Pilz/Schulz*, RDV 2011, 117, 118.
[73] *Bräutigam/Sonnleitner*, AnwBl 2011, 240.
[74] *Bräutigam/Sonnleitner*, AnwBl 2011, 240.
[75] *Bräutigam/Sonnleitner*, AnwBl 2011, 240, 241.
[76] „Dies scheint zumindest da sinnvoll, wo Unternehmen datenschutzrelevante Dienstleistungen im Rahmen von Outsourcing-Projekten oder Datenverarbeitungen im Auftrag in Anspruch nehmen." So zutreffend *Bräutigam/Sonnleitner*, AnwBl 2011, 240, 241.
[77] Vgl. *Pilz/Schulz*, RDV 2011, 117, 119.

2. Pflicht zur Implementierung einer IT-Sicherheitsstrategie

a) Umfang des Gewährleistungsauftrages bei der Implementierungspflicht

Der Gewährleistungsauftrag des neuen Grundrechts macht es zudem erforderlich, die insoweit (weiter)entwickelte IT-Sicherheitsstrategie in einem weiteren Schritt in die sicherheitsrelevanten Organisationsstrukturen und Handlungsfelder zu implementieren. Die staatlichen Handlungsträger werden vor diesem Hintergrund zu einem an den Notwendigkeiten und Grundparametern der IT-Sicherheitsstrategie ausgerichteten Verhalten verpflichtet. Daraus folgt zunächst eine Pflicht aller staatlichen Handlungsträger, die vorhandenen Kompetenzen und Befugnisgrundlagen effektiv und im Sinne der IT-Sicherheitsstrategie wahrzunehmen und ihnen im Rahmen ihrer Möglichkeiten und in Ansehung kollidierender verfassungsrechtlicher Zielsetzungen und Rahmenbedingungen zur praktischen und nachhaltigen Umsetzung zu verhelfen. Die Implementierungspflicht erfasst nicht allein den unmittelbaren Kern- und Aufgabenbereich des neuen Grundrechts. Vielmehr übt die grundrechtliche Schutzpflicht als allgemeiner verfassungsrechtlicher Maßstab ihren Einfluss übergreifend auf das gesamte staatliche Handeln aus. Sie begründet damit die grundsätzliche Notwendigkeit, die materiellen Belange der IT-Sicherheit auch bei der Wahrnehmung anderer Aufgabenfelder mit zu berücksichtigen. Sie muss mithin also im Wege praktischer Konkordanz zu einem angemessenen Ausgleich mit den anderen, ggf. konfligierenden Sachinteressen gebracht werden. Das schließt die übergreifende Wahrnehmung der gesetzgeberischen Handlungsspielräume bei der Ausgestaltung öffentlich-rechtlicher Regelungen für verschiedene Bereiche des gesellschaftlichen und wirtschaftlichen Gemeinwesens mit ein.

b) Implementierung im Rahmen öffentlich-rechtlicher Vorschriften

Eine Implementierung der IT-Sicherheitsstrategie kann insbesondere durch Schaffung eines rechtlichen Rahmens für den präventiven Schutz von (kritischen) IT-Infrastrukturen realisiert werden. Ein einheitliches Gesetz, das sich mit allen Aspekten der IT-Sicherheit befasst, existiert bisher allerdings nicht. Vielmehr finden sich rechtliche Ansätze zur Regelung der IT-Sicherheit über die gesamte Rechtsordnung verstreut.

Öffentlich-rechtliche Regelungen sind etwa im Recht der Telekommunikation (§ 109 TKG), im Datenschutzrecht (§ 9 BDSG) und im Wirtschaftsaufsichtsrecht (§ 25a KWG) zu finden.

Gem. § 109 TKG hat der Dienstanbieter angemessene technische Vorkehrungen oder sonstige Maßnahmen zu treffen, um die im Gesetz genannten Schutzgüter zu schützen. Technische Vorkehrungen in diesem Sinne sind alle Maßnahmen, die sich auf die Funk-

tionsweise der technischen Einrichtung beziehen. Dabei sind bei der Planung alle in Betracht kommenden Risiken einzubeziehen.[78]

Die Verpflichtung zur Sicherung der eigenen IT-Systeme wird durch die Haftungsprivilegierung des § 44a TKG jedoch erheblich abgeschwächt. § 109 TKG ist darüber hinaus schwerpunktmäßig auf die Sicherung des Netzes gegen Kommunikationsstörungen ausgerichtet, nicht aber hinsichtlich des Schutzes auch Dritter gegenüber Angriffen über das Netz. Für die Dienstanbieter bestehen insoweit nur geringe Anreize, die IT-Sicherheit auch tatsächlich zu verbessern.[79]

Gem. § 9 BDSG haben die verantwortlichen Stellen technische und organisatorische Maßnahmen zu treffen und Sicherheitsmaßnahmen zu ergreifen. Konkretisiert werden diese Maßnahmen in der Anlage zu § 9 BDSG: Dazu gehört neben der Verhinderung unbefugter Nutzung (Zugangskontrolle) und unbefugter Veränderung oder Entfernung von Daten (Zugriffskontrolle) insbesondere die Verfügbarkeitskontrolle.

Über § 9 BDSG ist ein Schutz allerdings nur für personenbezogene Daten natürlicher Personen realisiert. Daten von juristischen Personen oder nicht-personenbezogene Daten werden dem Schutz der Vorschrift nicht unterstellt. Darüber hinaus werden von § 9 BDSG nicht alle Fragen des IT-Risikomanagements erfasst.[80] Das wesentliche Defizit der Regelung liegt zudem darin, dass der Vollzug der Vorschrift keineswegs gesichert ist. Die dort genannten IT-Sicherheitsmaßnahmen sind insbesondere zivilrechtlich nicht durchsetzbar.[81]

§ 25a KWG sieht für Kreditinstitute die Verpflichtung zu angemessenen und wirksamem Risikomanagement vor. Dazu gehört gem. § 25a Abs. 1 Satz 2 Nr. 2 KWG zum einen eine angemessene technisch-organisatorische Ausstattung, zum anderen die Festlegung eines angemessenen Notfallkonzepts für IT-Systeme. Mit einem Rundschreiben zu den Mindestanforderungen an das Risikomanagement (MaRisk) hat die Bundesanstalt für Finanzdienstleistungsaufsicht die Anforderungen des § 25a KWG konkretisiert.[82]

Die oben genannten Regelungen offenbaren, dass das Recht der IT-Sicherheit bisher eher lückenhaft und stark zersplittert ist. Einer nachhaltigen Implementierung der IT-Sicherheitsstrategie wird damit jedenfalls nur unzureichend Rechnung getragen. Es

[78] *Bock*, in: Beck'scher TKG-Kommentar, 3. Aufl. 2006, § 109 TKG Rn. 19.
[79] *Spindler*, MMR 2008, 7, 10.
[80] *Spindler*, MMR 2008, 7, 10.
[81] *Spindler*, MMR 2008, 7, 10; allerdings können ggf. Geschäftsführer oder Vorstände im Rahmen ihrer persönlichen Haftung belangt werden, wenn durch Verstöße gegen § 9 BDSG ein Schaden für ihr Unternehmen verursacht wird, vgl. *Schultze-Melling*, in: Taeger/Gabel, BDSG, 2010, § 9 Rn. 34.
[82] Rundschreiben 15/2009 (BA) – Mindestanforderungen an das Risikomanagement – MaRisk, Geschäftszeichen BA54-FR 2210-2208/0001 v. 14.08.2009.

scheint daher erwägenswert, die Schaffung eines einheitlichen und übergreifenden IT-Sicherheitsgesetzes ins Auge zu fassen.[83]

c) Implementierung im Rahmen zivilrechtlicher Vorschriften

Ein Bestreben der Wirtschaft, mehr Verantwortung und Sicherheit im Internet zu gewährleisten, stellt die Unternehmensleitung, gleichsam aber auch alle Mitarbeiter im Spannungsfeld von Technik, Organisation und Recht, vor komplexe Herausforderungen.[84] Die zunehmende Durchdringung des menschlichen Umfeldes mit Informationstechnologien und die Verlagerung des Lebens in virtuelle Räume[85] führt dazu, dass ein verantwortlicher Umgang und eine sichere Ausgestaltung des Internets nicht auf singuläre Anwendungsbereiche, wie etwa die Virenbekämpfung oder Hackerangriffe, beschränken lässt.[86] Die Gewährleistung von Verantwortung und Sicherheit im Internet ist vielmehr ganzheitlich in allen Bereichen relevant, in denen mit dem Internet verfochtene Informationstechnologien zur Anwendung kommen.[87]

Ein adäquates Niveau der Sicherheitsgewährleistung muss gewährleisten können, dass unternehmensbezogene Informationserhebungs- und -verarbeitungsprozesse so ausgestaltet sind, dass sie zum einen den Anforderungen der Informationsintegrität, -authentizität, -vertraulichkeit und -verfügbarkeit entsprechen, zum anderen aber auch den zahlreichen rechtlichen Erfordernissen des Wirtschaftsverwaltungsrechts, der allgemeinen und bereichsspezifischen Datenschutzgesetze sowie einschlägiger vertraglicher Verpflichtungen genügen.[88] Die IT-Sicherheit wird damit zu einem integralen Bestandteil jedes unternehmerischen Planungs- und Steuerungsprozesses.[89]

Hersteller von Hardware und Applikationen haben grundsätzlich die gleichen rechtlichen Vorgaben wie andere Hersteller auch zu beachten. Primär handelt es sich hierbei um die Regelung der verschuldensabhängigen Produzentenhaftung (§§ 823 ff. BGB) und des verschuldensunabhängigen Produkthaftungsgesetzes (ProdHaftG)[90]. Die zivilrechtlichen Anforderungen sind dabei eng mit der öffentlich-rechtlichen Regulierung der Produktsicherheit verzahnt.[91]

---

[83] *Spindler*, MMR 2008, 7; *Gaycken/Karger*, MMR 2011, 3.
[84] *Heckmann*, MMR 2006, 280, 282.
[85] Zur rechtssicheren Internetnutzung und insbesondere dem „Vertrauen in virtuellen Räumen“ *Heckmann*, K&R 2010, 1.
[86] *Heckmann*, MMR 2006, 280, 282.
[87] *Heckmann*, MMR 2006, 280, 282.
[88] *Heckmann*, MMR 2006, 280, 282.
[89] *Heckmann*, MMR 2006, 280, 282.
[90] Inzwischen dürfte mit der herrschenden Auffassung Software als Produkt i.S.d. ProdHaftG zu qualifizieren sein. Vgl. *Spindler*, NJW 2004. 3145, 3149; *Oechsler*, in: Staudinger, BGB, 2009, § 2 ProdHaftG Rn. 64 m.w.N.
[91] *Spindler*, Verantwortung von IT-Hersteller, Nutzern und Intermediären, 2007, S. 43, aufrufbar über https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Recht/Gutachten_pdf.pdf?__blob=publicationFile.

Grundlegende Regelungen über die Produktsicherheit finden sich im Gesetz über technische Arbeitsmittel und Verbraucherprodukte (Geräte- und Produktsicherheitsgesetz - GPSG).[92] In materieller Hinsicht sind die Hauptinstrumente der Gewährleistung von Sicherheit bestimmte Grundpflichten der Hersteller.[93] In verfahrensrechtlicher Hinsicht wird mittels Zertifizierungs- und Genehmigungsverfahren ein erhöhtes Maß an Sicherheit gewährleistet.[94] Die öffentlich-rechtlichen Produktsicherheitsgesetze sind als Schutzgesetze gem. § 823 Abs. 2 BGB zu qualifizieren und können folglich eine zivilrechtliche Haftung der IT-Hersteller nach sich ziehen.[95]

Weitgehend anerkannt ist, dass Hardware-Produkte als körperliche Gegenstände als Produkte i.S.d. GPSG einzuordnen sind.[96] Die Einordnung von Software ist angesichts der insoweit im Vordergrund stehenden geistigen Leistung problematisch.[97] *Spindler* stellt insoweit auf die Zielsetzung des GPSG ab und lässt auch Applikationen den Produktbegriff unterfallen, soweit diese „gefährlich" sein können und ein nicht völlig belangloses Gefährdungspotential schaffen.[98] Erfasst werden vom Schutz des GPSG allerdings nur Gefährdungen der Sicherheit und Gesundheit von Verwendern und Dritten (vgl. § 4 Abs. 1 GPSG).[99] Solche Gefahrenlagen werden in der Praxis regelmäßig im Rahmen des Einsatzes von „embedded Software" anzutreffen sein.[100]

Weitere Vorgaben hinsichtlich der Gewährleistung von IT-Sicherheit folgen aus § 91 Abs. 2 AktG. Hiernach ist der Vorstand einer AG verpflichtet, geeignete Maßnahmen zu treffen, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden. Diese Verpflichtung erfasst neben der bloßen Früherkennung von Risiken insbesondere die Einführung und Aufrechterhaltung von Risiko-Vermeidungsstrategien. Demzufolge hat das Unternehmen nicht nur die Pflicht, eine angemessene IT-Ausstattung zu unterhalten, sondern auch den zuverlässigen und sicheren Betrieb dieser IT-Systeme zu gewährleisten.[101]Das Risikomanagement gehört allerdings nicht nur in der AG, sondern auch in Gesellschaften anderer Rechtsform, wie etwa der GmbH (vgl. §

---

[92] Ein Anspruch des Produktbenutzers besteht aber nur bei Gefahren für die Gesundheit und die Sicherheit für Personen. So *Spindler*, NJW 2004, 3145, 3149.
[93] *Spindler*, Verantwortung von IT-Hersteller, Nutzern und Intermediären, 2007, Rn. 95.
[94] *Spindler*, Verantwortung von IT-Hersteller, Nutzern und Intermediären, 2007, Rn. 96, 104 ff.
[95] Vgl. BGH, Urt. v. 28.03.2006 – VI ZR 46/05 – NJW 2006, 1589; *Potinecke*, DB 2004, 55, 50; *Spindler*, NJW 2004. 3145; *Wagner*, BB 1997, 2541, 2541 f.
[96] *Zscherpe/Lutz*, K&R 2005, 499, 500; *Hoeren/Ernstschneider*, MMR 2004, 507; *Runte/Potinecke*, CR 2004, 725.
[97] Vertiefend *Spindler*, Verantwortung von IT-Hersteller, Nutzern und Intermediären, 2007, Rn. 215 ff.
[98] *Spindler*, Verantwortung von IT-Hersteller, Nutzern und Intermediären, 2007, Rn. 218; *Zscherpe/Lutz*, K&R 2005, 499, 500; *Runte/Potinecke*, CR 2004, 725, 727.
[99] Eigentums- und Vermögensschäden liegen Außerhalb des Schutzumfanges des GPSG; *Spindler*, Verantwortung von IT-Hersteller, Nutzern und Intermediären, 2007, Rn. 222; a.A. *Runte/Potinecke*, CR 2004, 725, 728.
[100] *Spindler*, Verantwortung von IT-Hersteller, Nutzern und Intermediären, 2007, Rn. 223.
[101] *Nolte/Becker,* IT Compliance, BB Special 5 zu BB 2008, 24.

43 GmbHG) zu den Geschäftsführerpflichten.[102] Gem. §§ 76, 93 AktG hat der Vorstand auf erkannte Risiken angemessen zu reagieren. Zwar ist insoweit den §§ 91, 93 AktG kein konkretes Pflichtenprogramm zu entnehmen. Von der „üblichen Sorgfalt" der Unternehmensführung ist aber in jedem Fall auch die Erkennung und Bekämpfung von IT-Risiken erfasst.[103]

Die gesellschaftsrechtlichen Regelungen weisen einen hohen Abstraktionsgrad auf und erfordern somit eine Konkretisierung. Ihre Wirkung beschränkt sich zudem allein auf das Innenverhältnis. Die Vorgaben laufen bei fehlender Durchsetzung also leer.[104]

d) Implementierung im Rahmen strafrechtlicher Vorschriften

Im Strafrecht hat der deutsche Gesetzgeber seine Handlungsspielräume durch eine technik- und praxisnahe Gesetzgebung ausgeschöpft. Bereits 1986 wurden bestehende, gravierende Strafbarkeitslücken im Bereich der Computerkriminalität geschlossen, indem zahlreiche neue Straftatbestände in das Strafgesetzbuch durch das 2. WiKG8 inkorporiert wurden: Computerspionage (§ 202a StGB), Computerbetrug (§ 263a StGB), Datenveränderung sowie Computersabotage (§§ 303a, 303b StGB). Doch schon bald kam es bedingt durch den technischen Fortschritt zu weiteren Strafbarkeitslücken, die es erneut zu beheben galt. Am 11.08.2007 trat daher das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität in Kraft, welches dem gewachsenen Missbrauchspotential im Bereich der Informationstechnologie sowie den diesbezüglichen europarechtlichen Vorgaben (Übereinkommen des Europarates über Computerkriminalität vom 23.11.2001 und Rahmenbeschluss des Rates der Europäischen Union vom 24.05.2005 über Angriffe auf Informationssysteme) Rechnung tragen soll.

Zu diesem Zweck wurde der Tatbestand des Ausspähens von Daten (§ 202a StGB) weiter gefasst. Von § 202a StGB wird das reine Hacking, d.h. das einfache Überwinden von Sicherheitseinrichtungen ohne Ausspähen von Daten, erfasst. Da die Vorschrift allein auf „Daten" abstellt, macht sich der Täter auch dann strafbar, wenn zwar das Computersystem als Ganzes ungesichert ist, die konkreten Daten aber gegen unberechtigten Zugang geschützt sind.

Ergänzt wurden zudem die Straftatbestände des „Abfangens von Daten" (§ 202b StGB) sowie das Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c StGB). § 202c StGB wurde zur Sanktionierung „besonders gefährlicher Vorbereitungshandlungen" ins StGB aufgenommen und stellt in Abs. 1 Nr. 2 den Verkauf, die Herstellung, das Überlassen, Verbreiten und sonstige Zugänglichmachen von sog. „Hackertools" unter Strafe.

---

[102] *Gaycken/Karger*, MMR 2011, 3, 8.
[103] *Trappehl/Schmidl*, NZA 2009, 985, 986.
[104] *Spindler*, MMR 2008, 7, 10.

Darüber hinaus wurde § 303a StGB (Datenveränderung) mit einem dritten Absatz versehen, sodass die Vorbereitungshandlungen des § 202c StGB nun entsprechend auch hier gelten. Nach § 303a StGB macht sich strafbar, wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert. Eine Unterdrückung von Daten kann bspw. durch einen (D)DoS-Angriff begangen werden.

Schließlich kam es auch zu einer Erweiterung des Anwendungsbereichs der strafbaren Computersabotage (§ 303b StGB). Nach § 303b Abs. 1 Nr. 2 StGB macht sich strafbar, wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er Daten (§ 202a Abs. 2 StGB) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt. Diese Tatvariante soll Störungen erfassen, die durch „an sich neutrale" Handlungen des Eingebens oder Übermittelns von Daten in ein Computersystem bei missbräuchlicher oder unbefugter Begehungsweise entstehen. Das subjektive Korrektiv „in der Absicht, einem anderen Nachteil zuzufügen" stellt dabei sicher, dass bspw. in der Netzwerkgestaltung begründete gängige Aktivitäten oder andere zulässige Maßnahmen der Betreiber oder Unternehmen nur dann unter Strafe gestellt werden, wenn diese missbräuchlich, d.h. in Schädigungsabsicht erfolgen.

Zudem soll mit der Einführung einer neuen EU-Richtlinie über Angriffe auf Informationssysteme der zunehmenden Gefährdung durch Botnetzkriminalität Rechnung getragen werden.[105] Die neue Richtlinie schließt bestehende Strafbarkeitslücken, indem die Strafbarkeit für das Abfangen von Daten (Art. 6) und Tathandlungen im Zusammenhang mit Tatwerkzeugen (Art. 7) unter Strafe gestellt werden.[106] Die Höhe der Strafen wird heraufgesetzt, die erschwerenden Umstände (Art. 10) erweitert und eine Verpflichtung zur Einführung eines Systems zur Erfassung von Straftaten aufgenommen (Art. 15).[107] In der Bundesrepublik Deutschland besteht im Bereich des materiellen Strafrechts nur teilweise Umsetzungsbedarf. Art. 6 und 7 der Richtlinie basieren auf Vorgaben der Cybercrime-Konvention des Europarates, die Deutschland in § 202b StGB und § 202c StGB geregelt hat.[108]

Am 04.08.2009 trat das Gesetz zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten (GVVG) in Kraft, mit dem drei neue Straftatbestände in das StGB eingeführt wurden. Einer davon war § 91 StGB, der die „Anleitung zur Begehung einer schweren staatsgefährdenden Gewalttat" unter Strafe stellt. Nach der Gesetzesbegründung soll die Norm unter anderem die vielfach ohne konkreten Tatbezug erfolgende

[105] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI des Rates, KOM(2010) KOM Jahr 2010 Seite 517; dazu *Gercke*, ZUM 2011, 609, 613.
[106] *Gercke*, ZUM 2011, 609, 613.
[107] *Gercke*, ZUM 2011, 609, 613.
[108] *Gercke*, ZUM 2011, 609, 613.

Verbreitung von Bombenbauanleitungen und sog. „Kochbüchern“ zur Planung terroristischer Anschläge über das Internet und das Sichverschaffen derselben (z.B. mittels Download), wenn es zur Vorbereitung einer solchen Gewalttat erfolgt, erfassen.

d) Schaffung eines einheitlichen IT-Sicherheitsrechts

Vor dem Hintergrund der skizzierten „Rechtszersplitterung“ stellt sich aus Sicht des Staates die rechtspolitische Frage, inwiefern er gehalten ist, ein einheitliches IT-Sicherheitsrecht zu schaffen. Um sich diesem Begriff anzunähern, kann eine Anleihe bei § 2 Abs. 2 BSIG genommen werden und somit IT-Sicherheit als Sicherheit in der Informationstechnik definiert werden, deren Einhaltung von bestimmten Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, entweder durch Sicherheitsvorkehrungen in informationstechnischen Systemen oder Komponenten oder bei der Anwendung von informationstechnischen Systemen oder Komponenten. IT-Sicherheit ist damit in verschiedene Schutzrichtungen zu interpretieren: die Schutzrichtung der Verfügbarkeit, der Unversehrtheit, der Vertraulichkeit, sowie der Verbindlichkeit, Zurechenbarkeit und Verantwortlichkeit.[109] Daraus ergeben sich sowohl auf privatwirtschaftlicher, als auch auf öffentlich-rechtlicher Seite Verpflichtungen, IT-Sicherheitsstandards einzuhalten. Alle technischen Maßnahmen, bedürfen dabei stets einer praktikablen rechtlichen Flankierung.[110] Eine Vereinheitlichung des IT-Sicherheitsrechts bedeutet dabei schwerpunktmäßig nicht zuletzt, dass Verantwortungen klar zugewiesen sind und Haftungsfragen an die Besonderheiten des IT-Sicherheitsrechts angepasst werden.[111] Hier ist zu überdenken, ob bestehende Sicherheits- und Haftungsnormen einer Anpassung und Abstimmung aufeinander bedürfen, die zu einer Erhöhung der Sicherheit im Internet führen kann. Ob dies aus rechtsökonomischer Sicht in naher Zukunft der Fall sein wird ist offen, da entsprechende Anreize wohl nicht in genügender Form vorhanden sind.[112]

3. Subsidiarität staatlicher IT-Sicherheitsgewährleistung: Gewährung von Hilfe zur Selbsthilfe

Gerade unter dem Aspekt der Grundrechtsausübungsvoraussetzung kommt der Befähigung des Einzelnen, aus eigener Kraft in tatsächlicher Hinsicht von seinen Grundrechten Gebrauch zu machen bzw. seine grundrechtlichen Rechts- und Schutzgüter vor Zugriffen Dritter zu schützen, eine besondere Bedeutung zu. Dabei besteht das Problem, dass der

---

[109] Einzelheiten hierzu vgl. Heckmann, MMR 2006, 280, 281.
[110] Vgl. nur die Thesen von *Heckmann*, Die elektronische Verwaltung zwischen IT-Sicherheit und Rechtssicherheit, in: Hill/Schliesky (Hrsg.), Herausforderung e-Government, 2009, S. 131, 141.
[111] *Spindler*. MMR 2008, 7, 11 f. Vgl. auch *Spindler*, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, S. 296 (Publikation des BSI)-
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Recht/Gutachten_pdf.pdf?__blob=publicationFile
[112] Zu dieser Einschätzung gelangt auch *Spindler*, der dabei auch den Aspekt einer möglichen Überregulierung im Blick hat; *Spindler*. MMR 2008, 7, 13 f.

Einzelne Zugriffe auf seine informationstechnischen Systeme wegen des hohen (technischen) Komplexitätsgrads und der Geschwindigkeit der informationstechnischen Entwicklung zum Teil nur begrenzt abwehren kann. Ein wirkungsvoller technischer Selbstschutz wird insoweit kaum möglich sein oder den durchschnittlichen Nutzer zumindest regelmäßig überfordern.[113] Insoweit besteht dann aber eine staatliche Verantwortung, einen adäquaten Schutz im Rahmen und nach Maßgabe des grundrechtlichen Schutzbereichs zu gewährleisten. Schon aus Gründen der generellen Leistungsfähigkeit des Staates kann sich hieraus freilich keine „Pflicht zur individuellen Betreuung" des einzelnen Bürgers ergeben. Vielmehr beschränkt sich die grundrechtliche Minimalpflicht des Staates jenseits der Verpflichtung zu Aufbau und Weiterentwicklung eines staatlichen IT-Sicherheitskonzepts und dem Ausgleich von Infrastrukturdefiziten durch eine beobachtende Begleitung der globalen IT-Sicherheitsbemühungen aller staatlichen, unternehmerischen und gesellschaftlichen Akteure auf die ausreichende Verfügbarkeit von Mitteln der Selbsthilfe durch den einzelnen Internetnutzer. Das betrifft insbesondere die gesetzgeberische Ausrichtung der tatsächlichen rechtlichen Rahmenbedingungen, um die dem Endnutzer im Rahmen der informationellen Selbstbestimmung und des IT-Grundrechts zur Verfügung gestellten Gewährleistungsgehalte nicht ins Leere laufen zu lassen. Hilfe zur Selbsthilfe stellt sich soweit allerdings als ein zwischen Selbstschutz und Verantwortung des Nutzers korrespondierendes Konzept dar. Der Staat schützt den Bürger im Zweifel nicht immer nur dann, wenn er ihm ausreichende Möglichkeiten des Selbstschutzes an die Hand gibt, sondern vielmehr auch, wenn er die Nutzer im Rahmen eigener informationeller Handlung in die Verantwortung nimmt.

a) Informationelle Selbstbestimmung durch „Selbstverantwortung" des Nutzers

Sofern eine Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten nicht von einem gesetzlichen Tatbestand erlaubt wird, steht und fällt die Datenverarbeitung mit der Einwilligung des Nutzers. Die Abgabe einer Einwilligung bzw. deren Widerruf gehören zu den präventiven Schutzinstrumenten der informationellen Selbstbestimmung.

Die repressive Wahrnehmung der informationellen Selbstbestimmung ist problembehaftet: Datenschutzverletzungen weisen die Besonderheit auf, dass sie nicht vollständig rückgängig gemacht werden können. Personenbezogene Daten in Form von Dateien, Portraitaufnahmen oder anderen Medieninhalten werden von Dritten weiterverarbeitet und genutzt. Eine Rückholung oder Sperrung der Daten ist technisch unmöglich und rechtlich außerhalb des Geltungsbereichs des Bundesdatenschutzgesetzes praktisch aussichtslos. Dies gilt auch für soziale Netzwerke, bspw. Facebook. Im Zuge der Nutzung eines Mitgliedskontos wird eine unüberschaubare Bandbreite an personenbezogenen

[113] So auch BVerfG, Urt. v. 27.02.2008 – 1BvR 370/07, 1 BvR 595/07, jurisRdnr. 159 ff.

Daten, vorwiegend Medieninhalte und Informationen zur Selbstdarstellung der Person, erhoben, verarbeitet und vom Portalbetreiber zu Werbezwecken genutzt. Prävention zum Schutz der informationellen Selbstbestimmung ist daher besonders wichtig. Repressiver Rechtsschutz allein genügt nicht, unabhängig davon, wie streng die gesetzlichen Vorgaben im Bereich des Datenschutzes sind. Staatliche Vorgaben allein sind nicht hinreichend, wie bereits die Praxiserfahrung des § 3a BDSG zeigt. Die darin normierte Pflicht, Datenverarbeitungssysteme an den Grundsätzen der Datenvermeidung und Datensparsamkeit auszurichten, findet in der Wirtschaft kaum Beachtung. Neben der Regulierung der datenverarbeitenden Stellen muss vielmehr der Bürger zu einem verantwortungsvollen Umgang mit seinen Daten „erzogen" werden.

„Informationelle Selbstverantwortung" ist daher ein Ziel, das es von staatlicher Seite zu forcieren gilt. Dies kann etwa durch entsprechende Kampagnen geschehen. Mit der Forderung nach „informationeller Selbstverantwortung" geht jedoch kein Recht des Staates zum Rückzug aus seiner Verantwortung einher. Gesetzliche Rahmenbedingungen müssen bereit gestellt, ihre Wirksamkeit und Durchsetzbarkeit gewährleistet werden. Vor diesem Hintegrund bietet sich in der Praxis ein besonders Identitätsmanagement an. Neutrale Institutionen könnten Datensätze mit Nutzerprofilen (vergleichbar mit der DENIC) speichern. Die personenbezogenen Daten des Nutzers lägen nicht mehr beim Portalanbieter, bspw. Facebook, sondern auf der Identitätsplattform. Der Nutzer könnte bestimmen, welche Netzwerke auf welche Daten zugreifen können. Widerruft er seine Zustimmung, können die Plattformbetreiber nicht mehr darauf zugreifen. Eine solche technisch-organisatorische Maßnahme könnte den Nutzer in seiner „informationellen Selbstverantwortung" unterstützen.

b) Umgang des Nutzers mit fremden Informationen

Die Nutzung sozialer Netzwerke ist dadurch geprägt, dass zunehmend Informationen, die in früheren Zeiten noch in einer abgetrennten Sphäre des „Für-sich-Behaltens" oder „Mit-Freunden-Teilens" verblieben wären, einer so großen Menge an anderen Menschen mitgeteilt oder zur Verfügung gestellt werden, dass dies einer Veröffentlichung dieser Informationen gleichkommt.[114] Die Veröffentlichung der Informationen ist dabei keineswegs unentgeltlich. Die Gegenleistung besteht in der Preisgabe von persönlichen Daten – der „Währung" des Web 2.0.

Aus datenschutzrechtlicher Sicht problematisch ist dabei nicht nur die Preisgabe von Daten mit Bezug zur eigenen Person, sondern dass Nutzern sozialer Netzwerke zunehmend Informationen über Dritte aus einem ebenso sensiblen sozialen Kontext preisgegeben werden.[115] Dies kann bspw. im Wege der Veröffentlichung privater Fotos, Videos,

[114] Vertiefend *Heckmann*, K&R 2010, 770 ff.
[115] *Heckmann* in: jurisPK-Internetrecht, 3. Aufl. 2011, Kap. 9, Rn. 484 ff.

Tonmitschnitte, der Zuweisung von Medieninhalten oder der Preisgabe von Informationen über eine Person sowie wörtlichen Zitaten der Person erfolgen.[116] Sofern die Betroffenen nicht ausdrücklich und vollumfänglich in diese Datenverarbeitung eingewilligt haben, stellt sich die Frage, ob der Nutzer datenschutzrechtlich auch für entsprechende Rechtsfolgen in die Verantwortung genommen werden kann. Datenverarbeitung, ausschließlich für persönliche oder familiäre Tätigkeiten, wird vom Anwendungsbereich des Bundesdatenschutzgesetzes ausdrücklich ausgenommen. Vor dem Hintergrund der gleichlautenden Vorschrift der EU-Datenschutzrichtlinie hat der EuGH hingegen die Ansicht vertreten, dass dieser Ausnahmetatbestand bei Veröffentlichungen im Internet keine Anwendung findet.[117]

Die in der Wissenschaft bereits aufkommende Forderung, technische Anforderungen und rechtliche Voraussetzungen auch auf private Datenverarbeiter auszuweiten, scheint somit zunehmend an Berechtigung zu gewinnen. Während der Nutzer bisher lediglich die Rolle des Betroffenen datenschutzrechtlich relevanter Vorgänge einnimmt, könnte er künftig auch die Rolle des (verantwortlichen) Datenverarbeiters einnehmen. Mit Blick auf die sozialen Netzwerke, die nicht nur eine Selbstgefährdung der informationellen Selbstbestimmung des Nutzers herbeiführen, sondern in besonderem Maße auch zur Fremdgefährdung verleiten, ist dies nur konsequent.

c) Eigenverantwortlicher Basisschutz für private Rechner

Nicht nur IT-Hersteller und Dienstleister, sondern auch Nutzer von Informationstechnologie können Pflichten gegenüber Dritten treffen, die unmittelbar mit dem Einsatz von IT zusammenhängen. Im Unterschied zu Arbeitnehmern treffen private Nutzer im Bereich der IT-Sicherheit regelmäßig keine vertraglichen Pflichten. Für den Bereich der Verkehrssicherungspflichten und des Strafrechts sind davon Ausnahmen zu machen. In Ermangelung spezialgesetzlicher Pflichten im privaten Bereich kann eine Haftung privater Nutzer darüber hinaus nur auf deliktische Ansprüche gestützt werden.[118]

Mangels eines entsprechenden Vorsatzes wird eine Haftung privater Nutzer oftmals nur auf die Verletzung deliktischer Verkehrspflichten gem. § 823 Abs. 1 BGB gestützt werden können. Bei diesen kommt insbesondere eine Eigentumsverletzung wegen Störung der Integrität von Daten Dritter in Betracht. Der private Nutzer muss die Rechtsgutsverletzung durch zurechenbares und pflichtwidriges Handeln oder Unterlassen verursacht haben. Denkbar ist, dass der Nutzer durch Weiterverbreitung von Viren oder Malware zur Schädigung eines Dritten beiträgt. Eine Haftung für Unterlassen kommt in Betracht, wenn es der Nutzer versäumt, seinen privaten Rechner im Rahmen des Zumutbaren ge-

[116] Dazu *Kläner*, Telemedicus, Beitrag v. 20.07.2010, http://www.telemedicus.info/article/1806-Datenschutz-und-Datensicherheit-in-sozialen-Netzwerken.html.
[117] EuGH, Urt. v. 06.11.2003 – C-101/1 - „Lindquist" - EuZW 2004, 245; vgl. *Albrecht/Maisch*, Datenschutz in sozialen Netzwerken: Wenn das Leben der Anderen tabu ist, Legal Tribune Online, 05.07.2011.
[118] *Spindler*, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, 2007, S. 117 ff.

gen Attacken zu schützen und somit Angreifer die Sicherheitslücken zum Schaden Dritter ausnutzen, indem sie seinen Rechner instrumentalisieren.[119]

Grundsätzlich haftet derjenige aus Verletzung von Verkehrssicherungspflichten, der eine Gefahrenquelle schafft und nicht die zumutbaren Schutzvorkehrungen trifft. Da die Rechtsordnung keine allgemeine Rechtspflicht kennt, andere vor Schäden zu bewahren, sind Verkehrspflichten besonderes zu begründen. Bei der Zumutbarkeit ist auf die berechtigte Sicherheitserwartung der betroffenen Verkehrskreise abzustellen. Der Bekanntheitsgrad von Gefahren für die IT-Sicherheit kann im privaten Bereich nicht ohne weiteres festgestellt werden. Sind Schutzvorkehrungen unbekannt oder technisch aufwändig, so trifft den Nutzer keine Pflicht zur Überwachung seiner Computer, solange kein konkreter Hinweis auf einen Missbrauch besteht.[120] Angesichts der rasanten technischen Entwicklung ist gegenwärtig zwar auch vom durchschnittlichen IT-Nutzer zumindest die Kenntnis grundlegender Sorgfaltsmaßnahmen zu erwarten.[121] Schutzmaßnahmen müssen allerdings technisch und wirtschaftlich zumutbar sein. Dies gilt beispielsweise nicht für Maßnahmen, die eine Konfiguration einer Firewall oder die Befolgung von Entfernungsanleitungen voraussetzen. Als zumutbar wird jedoch die Installation eines Programms, bspw. eines Virenschutzprogramms, bewertet, dass einfach gestaltet ist und ggf. selbsttätig Schutzmaßnahmen umsetzt.[122]

Mit zunehmender Verbreitung von Breitband-Internetanschlüssen und der Kommerzialisierung des Internets sind Betreiber sog. Botnetze verstärkt kriminell motiviert. Die Geschäftsmodelle der Angreifer belaufen sich auf Klickbetrug, Passwort-Spionage und DDoS-Angriffe, um bspw. durch einen Ansturm an Serveranfragen E-Commerce-Plattformen temporär abzuschalten.[123] Botnetze bestehen aus hunderten Rechnern und Servern, die durch die Botnetz-Betreiber kontrolliert und ferngesteuert werden. Botnetze setzen dabei Ansammlungen von Rechnern voraus, die durch Schadsoftware der Kontrolle ihrer Nutzer entzogen worden sind. Ein entsprechend befallener Rechner kann von außen über eine bestehende Internetverbindung gesteuert und ohne Wissen des Besitzers zur Begehung von Straftaten genutzt werden. Die Durchführung von DDoS-Angriffen auf fremde Server durch ein Botnetz erfüllt den Tatbestand der Computersabotage gem. § 303b StGB.[124]

Botnetze stellen dabei nicht nur eine Gefährdung für ihre Zielobjekte dar. Auch der Besitzer eines infizierten Rechners kann sich als Teilnehmer der Tat strafbar machen. Hat der Nutzer bspw. von der Infizierung seines Rechners Kenntnis erlangt und unternimmt

---

[119] *Spindler*, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, 2007, S. 119.
[120] BGH NJW 2004, 1590 = JZ 2004, 1124 m. Anm. *Spindler*.
[121] *Spindler*, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, 2007, S. 123.
[122] *Spindler*, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, 2007, S. 123.
[123] *Heckmann* in: jurisPK-Internetrecht, 3. Aufl. 2011, Kap. 8, Rn. 17 ff.
[124] LG Düsseldorf, Urt. v. 22.03.2011 - 3 KLs 1/11.

nichts, um diese zu beseitigen oder den Rechner vom Netz zu nehmen, so ist eine Strafbarkeit aus pflichtwidrigem Unterlassen gem. § 13 StGB wegen Beteiligung an den Delikten des Botnetzbetreibers nicht ausgeschlossen.

Die dazu erforderliche Garantenstellung ergibt sich daraus, dass ein Eigentümer oder Besitzer von Sachen, Anlagen oder Maschinen, von denen Gefahren ausgehen, diese zu kontrollieren und zu verhindern hat, dass aus ihnen Schäden für fremde Rechtsgüter erwachsen. Solche Gefahrenquellen mit gewaltigem Schadenspotential können von Rechnern mit Internetanbindung ausgehen. Der Halter eines solchen Rechners ist daher zur Abwehr von Gefahren, bspw. durch Beseitigung des Schadprogramms oder Abschaltung der Internetverbindung, verpflichtet, soweit dies möglich und zumutbar ist. Da es dem Nutzer in der Regel an der Tatherrschaft fehlt, kommt eine Strafbarkeit wegen Beihilfe in Betracht, wenn ein entsprechender Vorsatz, bspw. Eventualvorsatz, bezüglich der Haupttat gegeben ist.

Botnetzkriminalität ist ein weiteres Beispiel für Gefährdungslagen, die aus dem sorgfaltswidrigen Umgang mit Informationstechnologie bzw. mangelhaften Präventionsmaßnahmen für die Sicherheit von IT in der privaten Sphäre erwachsen und für die der Nutzer unmittelbar (straf- und zivilrechtlich) zur Verantwortung gezogen werden kann.

d) Erleichterung der Wirtschaftsspionage mittels Social Engineering

Die „klassische Industrie- bzw. Wirtschaftsspionage“ wird mit Hilfe des Internets deutlich erleichtert. Die Bereitschaft der Unternehmen zu kundenfreundlicher Transparenz bietet ideale Ansatzpunkte für diese Form der Informationsbeschaffung. So gibt beispielsweise die Website eines Unternehmens - oft ungewollt - wichtige Informationen preis. Über Stellenausschreibungen und Online-Jobbörsen lässt sich z.B. in Erfahrung bringen, welche Mitarbeiter ein Unternehmen sucht und ob man auf diesem Weg ggf. einen Spion einschleusen kann. Interessant ist auch, auf welchen anderen Websites das künftige Opfer auftaucht, ob es Mitglied in einem Verband ist und ob seine Mitarbeiter Beiträge für Newsgroups verfassen. Sobald das „Gebilde“ Unternehmen verstanden worden ist, können Zielpersonen ausfindig gemacht und kontaktiert werden, um ihr Vertrauen zu gewinnen. Auch hier hilft entscheidend das Internet mit Personensuchmaschinen wie YASNI und mit den Sozialen Netzwerken wie Facebook oder Xing. Die vorgebliche Intimität der Social Networks wie Facebook, Xing oder Linkedin, die dem Knüpfen persönlicher Kontakte dienen sollen, verführt manche ihrer Mitglieder dazu, bereitwillig auch vertrauliche dienstliche beziehungsweise unternehmensinterne Informationen preiszugeben.[125] Immer wieder nutzen Kriminelle den Umstand, dass die Kommunikation in derartigen Netzwerken auf der persönlichen Verbindung der User basiert und ein hoher Grad an Vertrauen im Spiel ist. Bei den meisten Netzwerken kann man

[125] *Schnitzer/Hochenrieder*, DuD 2007, 927, 929.

sich jedoch leicht registrieren und die Angaben zur Person werden dabei in der Regel nicht verifiziert.[126] Dadurch lassen sich mit Fake-Profilen leicht Daten ausspähen. Ein Spion könnte sich beispielsweise im Vorfeld ausführlich über das soziale Umfeld des Opfers informieren und sich sein Vertrauen erschleichen. Entscheidungsträger und Mitarbeiter im Forschungsbereich können mit diesem Hintergrundwissen gezielt kontaktiert werden.[127] Die Hemmschwelle zur Kommunikation sinkt, weil man denkt, man habe es mit einem Kollegen zu tun. So ist auch das Szenario eines „bösen Zwillings"[128] vorstellbar: Der Spion erstellt ein Profil mit den Daten eines Kollegen des Opfers, das er von einer anderen Plattform her kennt, und nimmt so dessen Identität an. Auf diese Weise könnte er leichter erreichen, dass über Unternehmensinterna geplaudert wird. Der „Unsicherheitsfaktor Mensch" ist in diesem Zusammenhang keinesfalls zu unterschätzen.

[126] *Seidl/Beyvers*, AnwZert-ITR 15/2011, Anm. 3.
[127] Wirtschaftsspionage in Baden-Württemberg und Bayern, 2006, S. 30.
[128] http://www.stern.de/digital/online/soziale-netzwerke-der-spion-der-mich-kopierte-641364.html.