IT-Sicherheit, das EU-Recht und die Grundrechte: Neustart erforderlich

Stand: 27. Mai 2016

Inhalt

Ingo Ruhmann, Ute Bernhardt
Elchdamm 56a, 13503 Berlin
030-2804 6695
ruhmann@netzwerk-datenschutzexpertise.de
bernhardt@netzwerk-datenschutzexpertise.de

Bei der IT-Sicherheit ist das deutsche Telemedien-Recht mit EU-Recht nicht vereinbar. Die Untersuchung relevanter Regelungen zur IT-Sicherheit im deutschen Telekommunikations- und Telemedienrecht zeigt, dass Grundrechte missachtet, die Praxis von IT-Sicherheitsprofis und der Schutz der Daten erschwert und Konflikte mit dem Strafrecht heraufbeschworen werden. Ihrer Praxisferne wegen werden die Vorschriften von weiten Teilen der Anwender im Alltag ignoriert. Das EuGH-Verfahren „Breyer vs. Deutschland“ macht deutlich, dass zur Gewährleistung der IT-Sicherheit in Deutschland rechtliche Nachbesserungen dringend erforderlich sind.

1 IT-Sicherheitsrecht vor dem EuGH

Wer Angriffe auf IT-Systeme erkennen will, kann verschiedenste Detektionssysteme einsetzen, die mehr oder weniger umfangreiche Datensammlungen anlegen und analysieren. Wer Angriffe aus dem Internet zu den Urhebern zurückverfolgen will, muss auf die Kommunikationsdaten zurückgreifen. Im Internet sind Datenschutz und IT-Sicherheit eng miteinander verwoben: Zum Schutz vor Datenmissbrauch schreibt das Datenschutzrecht effektive IT-Sicherheitsmaßnahmen vor, die ihrerseits datenschutzkonform gestaltet sein müssen. Dem Internet-Protocol-(IP)-Kommunikationsstandard gemäß setzen sich IP-Daten zusammen aus den Adressinformationen über Absender und Empfänger und den Kommunikationsinhalten; IT-Sicherheitssysteme nutzen Adressdaten und Inhalte dieser IP-Daten sowohl zur Angriffserkennung als auch zu forensischen Analysen. Die Erhebung und Verarbeitung solcher Daten zur Bekämpfung von Angriffen auf IT-Systeme ist ein tiefer Eingriff in die informationelle Selbstbestimmung und das Fernmeldegeheimnis und sollte in möglichst geringem Maß, mit großer Sorgfalt und unter genauer Kontrolle erfolgen. Von besonderer Bedeutung sind daher die Rechtsgrundlagen dieser Art von Datenverarbeitung.

Während IT-Sicherheitsexperten auf technischer Seite für den Schutz jeder Art von IP-Kommunikation dieselben Werkzeuge einsetzen, unterscheidet das deutsche Recht für die Internet-Welt zwischen Web-Angeboten – juristisch: Telemedien –, der Telekommunikation und der Kommunikationstechnik des Bundes. Für den Umgang mit Daten, die zu Zwecken der IT-Sicherheit erhoben werden, gibt es drei höchst unterschiedliche Regelungen im Telemediengesetz (TMG), im Telekommunikationsgesetz (TKG) und im BSI-Gesetz (BSIG).

Der schleswig-holsteinische Landtagsabgeordnete Patrick Breyer will auf dem Klageweg als erstes für die Interpretation der genannten gesetzlichen Regelungen die zentrale, in Deutschland nicht einheitlich entschiedene Frage klären lassen, ob IP-Adressen personenbezogene Daten sind oder nicht. Dabei geht es im zweiten und für Breyer entscheidenden Schritt um die Klärung der Erlaubnis zur Erhebung solcher Daten bei Webangeboten – Telemedien wie Webseiten, e-Commerce-Angebote, Telebanking und anderes –, da personenbezogene Daten in Deutschland von Telemedienanbietern nur unter engen Vorgaben gespeichert werden dürfen. Der deutsche Bundesgerichtshof (BGH) hat dem Europäischen Gerichtshof (EuGH) die Fragen zur Entscheidung vorgelegt,

a) ob IP-Adressen personenbezogene Daten sind und
b) ob ein Telemedienanbieter von beliebigen Besuchern die IP-Adressen und die zugegriffenen Seiten speichern darf oder nicht, um „die generelle Funktionsfähigkeit des Telemediums zu gewährleisten“.

In dem Verfahren liegt nun der Schlussantrag des Generalanwalts Manuel Campos Sánchez-Bordona[1] vor. Der Generalanwalt stellt in seiner Würdigung den eindeutigen Bezug her zwischen der Erhebung von IP-Daten und deren Nutzung zur Verfolgung rechtswidrigen Verhaltens:

> „In Wirklichkeit dienen die Speicherung und Aufzeichnung dieser Daten dann als ein weiteres Beweismittel, mit dem der Inhaber der Internetseite vom Staat die Verfolgung eines rechtswidrigen Verhaltens auf Antrag verlangen kann. Es handelt sich um ein strafrechtliches Mittel zur Verteidigung von Rechten, die die Rechtsordnung dem Einzelnen zuerkennt."[2]

Der Generalanwalt argumentiert unter differenzierter Bezugnahme auf EU-Recht mit den realen technischen Möglichkeiten der Zusammenführung von Daten und kommt zu dem Schluss:

> „Gemäß Art. 2 Buchst. a der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ist eine dynamische IP-Adresse, über die ein Nutzer die Internetseite eines Telemedienanbieters aufgerufen hat, für Letzteren ein „personenbezogenes Datum", soweit ein Internetzugangsanbieter über weitere zusätzliche Daten verfügt, die in Verbindung mit der dynamischen IP-Adresse die Identifizierung des Nutzers ermöglichen."[3]

Was der Generalanwalt hier auf der Grundlage der EU-Datenschutzrichtlinie aus dem Jahre 1995 begründet, wird künftig in der EU-Datenschutzgrundverordnung (DSGVO) klarer formuliert: Artikel 4 DSGVO definiert „personenbezogene Daten" als „alle Informationen, die sich auf eine […] identifizierbare natürliche Person […] beziehen", die mittels „Zuordnung zu einer Kennnummer, […] zu einer Online-Kennung […] identifiziert werden kann". Dies trifft zweifellos auf eine IP-Adresse zu.

Der Generalanwalt nimmt bei der Beurteilung der Bedeutung von IP-Adressen dieselbe Bewertung vor wie das deutsche Bundesverfassungsgericht (BVerfG), das bereits 2012 dynamische IP-Adressen als personenbezogene Daten einordnete, die durch das Grundrecht auf informationelle Selbstbestimmung zu schützen sind.[4]

Für Telemedienanbieter folgt aus dieser Einordnung, dass IP-Adressen nach den Vorschriften des TMG für personenbezogene Daten behandelt werden müssen. Das TMG erlaubt in § 12 deren Speicherung und Verarbeitung nur, sofern

a) diese gesetzlich erlaubt ist,
b) sie zur Abrechnung in Vertragsverhältnissen nötig ist, oder
c) der Nutzer eingewilligt hat.

[1] Schlussanträge des Generalanwalts Manuel Campos Sánchez-Bordona vom 12. Mai 2016, Rechtssache C‑582/14, Patrick Breyer gegen Bundesrepublik Deutschland: „Verarbeitung personenbezogener Daten – Richtlinie 95/46/EG – Art. 2 Buchst. a und Art. 7 Buchst. f – Begriff ‚personenbezogene Daten' – IP-Adressen – Speicherung durch einen Diensteanbieter für Telemedien – Nationale Regelung, die eine Berücksichtigung des berechtigten Interesses des für die Verarbeitung Verantwortlichen nicht zulässt",
http://curia.europa.eu/juris/document/document_print.jsf?doclang=DE&text=&pageIndex=0&part=1&mode=req&docid=178241&occ=first&dir=&cid=915724.
[2] Ebd., Nr. 91.
[3] Ebd., Nr. 106 (1).
[4] http://www.bverfg.de/entscheidungen/rs20120124_1bvr129905.html

Nutzungsdaten dürfen für Zwecke der Werbung anonym oder pseudonym gespeichert werden. Für alle anderen Zwecke einschließlich der IT-Sicherheit erlaubt § 15 TMG nur eine Datenverarbeitung bis zum „Ende der Nutzung“ und schreibt ausdrücklich die nachfolgende Datenlöschung vor.[5]

Diese nationale Löschungsvorschrift im TMG ist für den Generalanwalt des EuGH unvereinbar mit EU-Recht, weil sie dem „berechtigten Interesse“ des Anbieters entgegensteht, „die Funktionsfähigkeit des Telemediums zu gewährleisten“.[6] Damit klärt er mehr als die an den EuGH gerichteten Fragen. Denn der Ausgangspunkt der Begründung des EuGH ist die Auffassung, dass das absolute Verbot der Speicherung von IP-Adressen im TMG „die Funktionsfähigkeit des Telemediums“ bei Angriffen gefährdet, also in der Praxis den Einsatz jener IT-Sicherheitsanwendungen verhindert, die personenbezogene Daten wie etwa IP-Adressen verarbeiten.

Schon seit ersten einschlägigen Urteilen im Jahr 2006[7] setzten sich in Deutschland IT-Sicherheitsverantwortliche dem Risiko einer Verurteilung aus, wenn sie zum Schutz ihrer Telemedien IT-Sicherheitswerkzeuge einsetzen, die auf der Speicherung und Analyse personenbezogener Daten aufbauen, für die keine Einwilligung der Nutzer vorliegt. Doch da die vorherige Zustimmung der Angreifer auf Webseiten zur Protokollierung der Daten ihrer eigenen Missetaten eine allzu realitätsferne Idee ist, wird diese gesetzliche Regelung im Alltag von IT-Sicherheitsanwendern geflissentlich übersehen. Dies führt dazu, dass nach Angriffen auf Webangebote zwar möglicherweise Datenmaterial vorliegt, dieses jedoch nicht als rechtmäßig gesammeltes Beweismittel in Gerichtsprozesse eingeführt werden kann. Oder, wie der Generalanwalt das Dilemma formuliert: Es darf bei Telemedien in Deutschland keine „Aufzeichnung dieser Daten als ein weiteres Beweismittel [geben], mit dem der Inhaber der Internetseite vom Staat die Verfolgung eines rechtswidrigen Verhaltens auf Antrag verlangen kann“.[8]

Genau dieses Verbot der Datensammlung zur Verfolgung eines rechtswidrigen Verhaltens ist für den Generalanwalt der Grund, von der Bundesregierung die Lockerung des absoluten Speicherverbotes zugunsten der IT-Sicherheit zu fordern. Dabei geht es ihm nicht um eine ungeregelte Datenspeicherung oder um Details wie Speicherfristen. Durch die rechtliche Klärung, dass (dynamische) IP-Adressen personenbezogene Daten sind, folgt zwangsläufig nach deutschem ebenso wie nach EU-Recht die Pflicht des Gesetzgebers, für die Erhebung, Speicherung und Verarbeitung dieser personenbezogenen Daten bei Telemedienanbietern eine gesetzliche Grundlage zu schaffen, um die Verarbeitung dieser Daten klar zu regeln, um eine praktikable Missbrauchsvorsorge und den Missbrauchsnachweis zu ermöglichen.

Der EuGH schließt sich in aller Regel den Schlussanträgen der Generalanwälte an. Es ist daher davon auszugehen, dass der EuGH die Bundesregierung dazu verurteilen wird, für das Angebot von Telemedien zwei Grundrechte der Informationsgesellschaft in Einklang zu bringen, nämlich den

[5] Ausführlich dazu: Ingo Ruhmann: IT-Sicherheit und das geplante IT-Sicherheitsgesetz; in: telepolis, 11.04.2013, http://www.heise.de/tp/artikel/38/38891/1.html und: ders.: Wann wird IT-Sicherheit kein Rechtsbruch mehr sein? in DANA, Heft 3, 2013, S. 95 – 100.
[6] Schlussanträge des Generalanwalts Manuel Campos Sánchez-Bordona, a.a.O., Nr. 106 (2).
[7] Die damalige Justizministerin Zypries wurde erstmals 2006 vom Amtsgericht Berlin Mitte und rechtskräftig 2008 dazu verurteilt, die Sammlung von IP-Daten im Webauftritt des Justizressorts einzustellen. http://www.daten-speicherung.de/data/Beschluss_AG-Mitte_2008-01-10.pdf. Als Reaktion darauf hat sich die Bundesregierung selbst mit der Novelle des BSI-Gesetzes 2009 mit § 5 BSIG die an strikte Einschränkungen geknüpfte Befugnis geschaffen, IP-Daten zur Angriffserkennung zu sammeln.
[8] Schlussanträge des Generalanwalts Manuel Campos Sánchez-Bordona, a.a.O., Nr. 91.

Datenschutz und das 2008 vom BVerfG definierte IT-Sicherheits-"Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“.[9] Mit den Feststellungen des Generalanwalts steht das TMG auch im Widerspruch zu diesem IT-Sicherheits-Grundrecht, weil das TMG den Einsatz wesentlicher Schutzwerkzeuge der IT-Sicherheit verhindert.

Der absehbare Ausgang des EuGH-Verfahrens wird eine Änderung des TMG unausweichlich machen. In den Entwurfsversionen des zweiten Anlaufs zum IT-Sicherheitsgesetz (ITSiG) 2014 hatte die Bundesregierung kurzfristig auch die Absicht offenbart, den damals schon erkennbar rechtswidrigen Zustand im TMG zu beheben. Sie hatte im Referentenentwurf des ITSiG vom Sommer 2014 eine Ergänzung des § 15 TMG vorgesehen, nach der es Diensteanbietern mit einer Formulierung analog zum damaligen §100 des Telekommunikationsgesetzes erlaubt werden sollte, „Nutzungsdaten zum Erkennen, Eingrenzen oder Beseitigen von Störungen seiner für Zwecke seines Telemedienangebotes genutzten technischen Einrichtungen [zu] erheben und verwenden“, weil – so die Begründung – „eine Lücke im Bereich der Erlaubnistatbestände des Telemediengesetzes“ bestand. Der AK Vorratsdatenspeicherung forderte im August des Jahres, diese Befugnis zu streichen.[10] Innen- und Justizressort einigten sich darauf, in der Kabinettsvorlage auf diese Regelung zu verzichten.[11] Dieser Weg einer Angleichung des Telemedien- an das Telekommunikationsrecht nach dem heutigen Stand wäre allerdings mit Grundrechten und der EU-Grundrechtecharta nicht annähernd vereinbar und daher keine akzeptable Lösung.

2 IT-Sicherheit im Telekommunikationsrecht

Der 1996 formulierte § 100 (1) des TKG regelte eine aus der Zeit der analogen Telefonie stammende Befugnis „zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen, die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer (zu) erheben und verwenden“, also ohne Einschränkung jede Form von Daten aus Telekommunikationsvorgängen zur Störungserkennung zu sammeln, zu analysieren und sich sogar auf Kommunikationsverbindungen aufzuschalten. Technisch erforderlich war dies zur Ermittlung strafbarer Eingriffe in Fernmeldesysteme, weil Störungen bei der analogen Telefonie nur durch Messungen im Betrieb erkannt und beseitigt werden können.

Die Zeit der analogen Telefonie ist jedoch absehbar Vergangenheit. Im deutschen Telekommunikationsnetz ist der Umbau auf ein All-IP-Netz bald abgeschlossen. In einem solchen All-IP-Netz lassen sich Störungen mit denselben Werkzeugen ermitteln, analysieren und beseitigen, wie in jedem IP-gestützten Netz: durch Analyse durchlaufender Datenpakete und der an den Netzknoten auflaufenden Kommunikationsprotokolle. Durch die Möglichkeiten der IP-Kommunikation war die alte Befugnis zur beliebigen Sammlung von Datenflüssen gemäß § 100 TKG bereits als eine grundrechtlich hochgradig bedenkliche Befugnis zu einer Datenspeicherung zu bewerten – eingeschränkt allein durch den gesetzlichen Zweck einer Störungsanalyse.

[9] Urteil des Ersten Senats vom 27. Februar 2008, 1 BvR 370/07, 1 BvR 595/07.
[10] AK Vorratsdatenspeicherung: Bundesinnenminister plant verdachtslose Aufzeichnung des Surfverhaltens im Internet (20.08.2014); http://www.vorratsdatenspeicherung.de/content/view/748/1/lang,de/
[11] Stefan Krempl: Keine Vorratsdatenspeicherung mit neuem IT-Sicherheitsgesetz, heise News, 9.12.2014; http://www.heise.de/newsticker/meldung/Keine-Vorratsdatenspeicherung-mit-neuem-IT-Sicherheitsgesetz-2485524.html

Der Gesetzgeber hatte im zweiten Anlauf zum ITSiG auf Wünsche von Unternehmensverbänden reagiert. Denn das Geschäft von Internet-Hostingprovidern ist es, im eigenen Rechenzentrum die Systeme ihrer Kunden an Netzwerke anzubinden und deren Betrieb sicherzustellen. Die Rechner werden zumeist von den Kunden administriert. Wenn nun ein in einem Rechenzentrum gehostetes IT-System eines Kunden von einem Angreifer gekapert wurde, hat der Kunde des Providers oft keine Kontrolle mehr über sein nun Schadcode verbreitendes oder in Angriffe verwickeltes System. Es ist daher im Interesse aller Betroffenen, den Internet- und Telekommunikationsprovidern die Überwachung von Kommunikationsdaten zur Behebung von Störungen und Angriffen zu erlauben und bei erkannten Anomalien die Beteiligten – das Rechenzentrum und den dortigen Kunden, dessen Rechner gekapert wurde - über Abhilfemöglichkeiten informieren zu dürfen. In der Praxis halten sich IT-Sicherheitsverantwortliche bei Providern und Computer Emergency Response Teams (CERTs) gegenseitig möglichst detailliert über Störquellen informiert. Sie versuchen kooperativ, auftretende Störungen an der Quelle, nämlich im Rechenzentrum des Providers, zu beenden. Mit diesem Informationsaustausch wird in der Praxis eine schnelle Abhilfe durch das Abschalten des verursachenden IT-Systems bzw. dessen Abkoppeln vom Netz erreicht.

Die durch das ITSiG nun im TKG verankerte Neuregelung geht jedoch an diesem Ziel vorbei und kann kein Maßstab für eine nach einem EuGH-Urteil notwendige Neuregelung des TMG sein. Sie nutzt der IT-Sicherheit nicht, sondern provoziert Konflikte mit dem Strafrecht.[12] Die Neuregelung verstößt zugleich massiv gegen das Fernmeldegeheimnis in Art. 10 GG. Beide Konflikte werden in den folgenden Abschnitten näher erläutert.

Die im ITSiG getroffene Neuregelung des § 100 TKG erlaubt es Telekommunikationsanbietern, auch Daten zu speichern und zu analysieren über

> „Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können“.

Damit wurde die früher in § 100 TKG formulierte Befugnis für die Messung flüchtiger analoger Daten im Falle einer *konkret bekannten* Störung ausgeweitet auf die Vorfeldkontrolle von „Störungen“, die zu den genannten Leistungseinschränkungen „führen *können*“, aber keineswegs schon geführt haben. Als Anlässe für die zulässige Datenerhebung werden „Verfügbarkeit“ nicht näher spezifizierter „Informations- und Kommunikationsdienste“ und der Schutz vor einem „unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer“ genannt.

„Nutzer“ wiederum sind keineswegs die Kunden eines Anbieters (also z.B. ein Betreiber eines beim Provider gehosteten Systems), sondern nach § 3 Nr. 14 TKG „natürliche oder juristische Personen, die einen öffentlich zugänglichen Telekommunikationsdienst für private oder geschäftliche Zwecke in Anspruch“ nehmen. Es handelt sich dabei somit um *beliebige Beteiligte*, deren Kommunikation dem Internet-Protokoll entsprechend der zufällig verfügbaren Leitungskapazität über das Netz eines der angeschlossenen Telekommunikationsanbieter geleitet wird. Der „Nutzer“-Begriff ist auch insofern unglücklich, da ein Provider zwar aufgrund eines Vertragsverhältnisses mit seinen Kunden deren

[12] Vgl. dazu auch: Ute Bernhardt, Ingo Ruhmann: IT-Sicherheit nach dem neuen IT-Sicherheitsgesetz; Beitrag zur Sommerakademie „Vertrauenswürdige IT-Infrastruktur – ein (un?)erreichbares Datenschutzziel“ am 31.08.2015 in Kiel; https://www.datenschutzzentrum.de/uploads/sommerakademie/2015/SAK2015_02-Vormittag_BernhardtRuhmann_IT-Sicherheitsgesetz_Handout.pdf.

spezifische Dienstenutzung kennen und mögliche unerlaubte Zugriffe erkennen kann, es aber im Dunkeln bleibt, wie ein Provider bei beliebigen Nutzern anderer Provider eine mögliche Störung der Verfügbarkeit oder gar einen „unerlaubten Zugriff“ auf deren IT-System erkennen sollte.

Dabei ist für jeden Anwender eines Virenscanners nachvollziehbar, dass es für die Erkennung einer potenziellen „Störung“, einer „Einschränkung der Verfügbarkeit“ oder „unerlaubter Zugriffe“ erforderlich ist, den Inhalt einer Datenkommunikation, in denen sich Schadcode verbirgt, einer genauen Analyse – einer „deep packet inspection“ – zu unterziehen, um möglichen Schadcode von einer legitimen Datenkommunikation unterscheiden zu können.

Außerdem fehlt neben dem unklaren Anlass jegliche Einschränkung der Datennutzung. Den Buchstaben des § 100 TKG nach sind Internetprovider und Telekommunikationsunternehmen heute daher befugt, *unbegrenzt* Daten über *beliebige Netznutzer* – also jeden – zu sammeln und auszuwerten, um zu erkennen, ob es unerlaubte „Zugriffe“ auf die IT-Systeme von Nutzern geben „könnte“.

2.1 Welcher Nutzen für Provider und die IT-Sicherheit?

Für Provider folgt aus den durch den § 100 TKG gewonnenen Daten jedoch nicht nur der mögliche Nutzen, die eigenen Systeme gegen Angriffe und Schäden schützen zu können, sondern auch die Pflicht, andere Betroffene über Gefährdungen aufzuklären. Dies regelt der neu eingeführte § 109a TKG mit der Aufforderung an Diensteanbieter, bei „Störungen, die von Datenverarbeitungssystemen der Nutzer ausgehen“, diese Nutzer

> „soweit ihm diese bereits bekannt sind, unverzüglich darüber zu benachrichtigen. Soweit technisch möglich und zumutbar, hat er die Nutzer auf angemessene, wirksame und zugängliche technische Mittel hinzuweisen, mit denen sie diese Störungen erkennen und beseitigen können“.

Relevant dabei ist, dass die Information eines „Nutzers“ als Verursacher vorgesehen ist und ***nicht*** – wie von Providern gefordert – des Rechenzentrums eines Providers, in dem dieser Nutzer seine IT betreibt. Es gehört zu den schwer nachvollziehbaren Lösungen im ITSiG, hierbei auf „Nutzer“ abzuzielen, von denen bereits bekannt ist, dass ihre IT-Systeme „Störungen“ produzieren – also beispielsweise Schadcode versenden. Diese Systeme stehen in der Regel nicht mehr unter Kontrolle der legitimen „Nutzer“, sondern unter der eines Angreifers. Der Nutzer kann, je nach Störung, diese möglicherweise gar nicht mehr selbst beseitigen. Der dieses IT-System kontrollierende aktive Angreifer wiederum dürfte jedenfalls kaum der richtige Adressat der in § 109a TKG vorgesehenen Information und Aufforderung zur Unterlassung der laufenden Störung sein.

2.2 IT-Sicherheit vs. Strafrecht

Wie bereits angeführt, tauschen sich CERTs über Stör- und Gefahrenquellen im Internet aus und informieren sich gegenseitig über Details der erkannten Gefahren. So bieten diverse CERTs im Internet Informationen darüber an, dass von einer spezifischen IP-Adresse aus Schadcode verbreitet wird, dass sich dahinter ein Command-and-Control-Server eines Botnetzes verbirgt oder eine solche IP-Adresse Teile eines Botnetzes oder eines DDoS-Angriffes ist. Damit wird jedoch die Schwelle zur Straftat überschritten. Bei oberflächlicher Betrachtung ist der neue § 109a TKG geeignet, diese Informationsbereitstellung möglicherweise sogar für zulässig zu halten.

Das deutsche Strafrecht legt die Hürden hoch, bevor ein Bruch des Fernmeldegeheimnisses strafrechtlich relevant wird. § 206 (1) Strafgesetzbuch (StGB) setzt voraus, dass der Täter bei seiner Tat alle der folgenden drei Merkmale erfüllt, also

a) ein Mitarbeiter oder Inhaber eines Telekommunikationsunternehmens bzw. Internetproviders ist, der
b) die Kommunikation eines Kunden „zur Kenntnis nimmt" – also nicht durch Computer automatisch analysieren lässt, sondern zusätzlich persönlich in Augenschein nimmt, und außerdem
c) diese Kommunikation bzw. deren näheren Umstände – wozu bereits Kommunikationskennungen wie etwa IP-Adressen gehören – Dritten mitteilt.

Es ist offensichtlich, dass die Weitergabe einer Information über Schadcode-Vorkommen durch den IT-Sicherheitsverantwortlichen eines Providers an das betroffene Rechenzentrum mit der Bitte, den Schadcode versendenden Rechner eines dortigen Kunden vom Netz zu nehmen, alle drei dieser für eine Straftat notwendigen Merkmale erfüllt:

a) Der oder die IT-Sicherheitsverantwortliche ist Mitarbeiter eines TK-Unternehmens.
b) Er oder sie hat die Ergebnisse einer zunächst vermutlich automatischen Analyse der Kommunikationsinhalte manuell ausgewertet und verifiziert, sodann die IP-Daten eines verdächtigen Nutzers und damit die durch das Fernmeldegeheimnis geschützten Kommunikationsdaten persönlich zur Bewertung in Augenschein und damit „zur Kenntnis" genommen und das zu der IP-Adresse gehörende Rechenzentrum ermittelt.
c) Abschließend hat jener Sicherheitsverantwortliche dem externen Rechenzentrum als Drittem eine Nachricht über den Inhalt der Kundenkommunikation – den Schadcode oder den Angriff – und die Kenndaten des spezifischen Kunden des Rechenzentrums als die vom Fernmeldegeheimnis geschützten näheren Umstände der Telekommunikation – gegeben.

Was als vermeintliche Abhilfe durch einen Austausch eines IT-Sicherheitsverantwortlichen mit einem anderen Rechenzentrum über dessen Kunden abläuft, stellt sich in der Abfolge dieser drei Schritte als eindeutiger Bruch des Fernmeldegeheimnisses nach § 206 StGB dar.

Selbst in Fällen, in denen es aus Sicht des Providers den Anschein hat, dass ein IT-System aus einem zu einem Unternehmen gehörenden Rechenzentrum gekapert worden ist (der Unternehmens-„Nutzer" ausnahmsweise also mit dem Rechenzentrumsbetreiber identisch scheint), ist Vorsicht geboten: Von außen ist bei den heutigen Verhältnissen mit Cloud- und Outsourcing-Betrieb nicht mit angemessener Sicherheit ablesbar, welche Besitz- und Verantwortlichkeitsverhältnisse zwischen dem Rechenzentrum und dem „Nutzer" in Sinne des ITSiG bestehen. Somit kann ein CERT- oder ein IT-Sicherheitsverantwortlicher nur unvollkommen einschätzen, ob er oder sie mit einer Meldung das Fernmeldegeheimnis verletzen würde oder nicht.

Da die beschriebenen Meldeabläufe zwischen Providern oder CERTs jedoch zum state-of-the-art der IT-Sicherheit gehören, ist den Beteiligten die Ungesetzlichkeit, ja Strafbarkeit ihres Tuns meist überhaupt nicht bewusst.

Vielmehr stellt die Kooperation von IT-Sicherheitsverantwortlichen und Systemadministratoren vor allem bei kleinen Providern eines der wichtigsten und nicht ersetzbaren Werkzeuge gegen mehrstufige Attacken dar, die üblicherweise zur Verschleierung von Angriffen eingesetzt werden. Somit fußen zentrale Abläufe der IT-Sicherheit nach deutschem Recht auf strafrechtlich sanktionierten

Grundrechtseingriffen. Der Praxis der IT-Sicherheit wäre die Grundlage entzogen, sollten diese Abläufe jemals zur Anzeige gebracht werden.

Mit der Neuregelung des TKG im ITSiG sollte mehr Rechtssicherheit für IT-Sicherheitsverantwortliche geschaffen werden. Dies ist nicht gelungen. Stattdessen setzen sich IT-Sicherheitsverantwortliche weiterhin dem Risiko aus, bei ihrer Arbeit das Fernmeldegeheimnis zu brechen. Die Rechtssicherheit für CERT-Mitarbeiter und IT-Sicherheitsverantwortliche ist ebenso dringend herzustellen wie die Rechtssicherheit für alle Internet-Nutzer im Umgang mit ihren Kommunikationsdaten.

3 Neuregelung unvereinbar mit Grundgesetz und EU-Recht

Wie oben dargestellt, wurden im ITSiG Regelungen getroffen, die am Ziel vorbeigehen und sinnvolle praktische Abläufe verhindern. Noch weit bedenklicher ist aber, dass die nicht zielführende Regelung im Telekommunikationsrecht mit gravierenden Grundrechtseingriffen und einem weiteren Verstoß gegen EU-Recht verbunden ist.

Mit dem ITSiG und der Befugnis in den §§ 100 und 109a TKG wurde eine datenschutzrechtlich nicht hinnehmbare Möglichkeit zur unzureichend zweckbestimmten Sammlung und Weitergabe von sensitiven Daten geschaffen. Während selbst bei der „Vorratsdatenspeicherung“ (die vermutlich auch in der neuen Fassung bei der verfassungsrechtlichen Prüfung scheitern wird) eine Löschungsfrist vorgesehen war und Kommunikationsinhalte nicht bei allen Kommunikationsformen gespeichert werden sollen, sorgt der neu gefasste § 100 TKG für eine unbegrenzte Datensammlung ohne solche Einschränkungen. Der § 109a TKG sieht sogar eine Verpflichtung zur Weitergabe von dabei erhobenen Daten an Dritte – „Nutzer“ im Sinne des Telekommunikationsrechts – vor.

Diese Befugnisse stellen einen deutlichen Eingriff in das Recht auf informationelle Selbstbestimmung dar und sind schon allein vom Umfang der Datensammlung her mit Grundrechten unvereinbar. Mit diesen Befugnissen in den §§ 100 und 109a TKG wird vor allem aber in nahezu unbegrenzter Weise in das grundrechtlich geschützte Fernmeldegeheimnis nach Art. 10 GG eingegriffen. Der neue § 100 TKG sieht keine Eingrenzung auf Kriterien der Datensammlung, Speicherdauer oder Analyseformen für Kommunikationsdaten und -inhalte vor. Die Entscheidung des BVerfG zur Vorratsdatenspeicherung lässt keinen Zweifel daran, dass hier in das Fernmeldegeheimnis eingegriffen wird:

> „In der Erfassung von Telekommunikationsdaten, ihrer Speicherung, ihrem Abgleich mit anderen Daten, ihrer Auswertung, ihrer Selektierung zur weiteren Verwendung oder ihrer Übermittlung an Dritte liegen damit je eigene Eingriffe in das Telekommunikationsgeheimnis.“[13]

Der in § 100 TKG geregelte Eingriff in das Grundrecht nach Art. 10 GG setzt eine an den Verhältnismäßigkeitsgrundsatz gebundene gesetzliche Regelung voraus, die zur Erreichung der Zwecke geeignet, erforderlich und angemessen ist. Sie muss

- an die Angabe eines konkreten und gravierenden Gefährdungsanlasses und nicht an eine „Störung“,

[13] Urteil des BVerfG zur Verfassungswidrigkeit der konkreten Ausgestaltung der Vorratsdatenspeicherung, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Nr. 190; http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs20100302_1bvr025608.html;jsessionid=6A24FB2EC041695356EAA1EE118F1936.2_cid383.

- an einen genügend spezifischen Zweck und nicht nur der Erkennung eines „unerlaubten Zugriffs“ gebunden sein,
- mit spezifischen Kriterien formuliert werden und
- Vorgaben zu Speicherdauer und zur Datennutzung enthalten.

Kein einziger dieser Maßstäbe für Eingriffe in Grundrechte wurde beachtet. Deshalb dürfte diese Ausweitung des TKG – wie schon in Stellungnahmen[14] und der Anhörung des Bundestages zum Gesetz[15] zu hören[16] – mit Art. 10 GG unvereinbar und damit verfassungswidrig sein.

Der Vergleich der Regelungen mit den Vorgaben des EuGH in dessen Urteil zur Vorratsdatenspeicherung[17] zeigt den vom Generalanwalt aufgezeigten Konflikt mit EU-Recht. Der EuGH hat bereits die Verpflichtung von TK-Providern zur Vorratsdatenspeicherung (die viel weniger umfangreich war als die durch § 100 TKG neu ermöglichten Datensammlungen) als „einen Eingriff in die durch Art. 7 der Charta garantierten Rechte“ sowie in das in „Art. 8 der Charta garantierte Grundrecht auf den Schutz personenbezogener Daten“ beurteilt.[18] Während der EuGH jedoch den Wesensgehalt der Grundrechte durch die Vorratsdatenspeicherung noch nicht angetastet sah, weil die Einsichtnahme in die Inhalte untersagt war, ist die Sachlage bei der Neuregelung des § 100 TKG eine andere: Das TKG ermöglicht nun, ohne jeden Anlass und ohne jede Eingrenzung Einblick in Kommunikationsinhalte genau deswegen zu nehmen, um prüfen zu können, ob die Inhalte schädigender Art sind oder nicht. Durch diese Unbestimmtheit wird der Wesensgehalt der Grundrechte angetastet. Der EuGH bestimmte als Maßstab für eine reine Erhebung personenbezogener Daten bei der Vorratsdatenspeicherung:

> „Daher muss die fragliche Unionsregelung klare und präzise Regeln für die Tragweite und die Anwendung der fraglichen Maßnahme vorsehen und Mindestanforderungen aufstellen, so dass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen.“[19]

Solche klaren Regeln und Grenzen fehlen aber der Neuregelung des § 100 TKG. Es ist daher naheliegend, dass diese bei einer Klage vor dem EuGH wegen Verletzung der EU-Grundrechtecharta keinen Bestand haben wird.

---

[14] Unabhängiges Zentrum für Datenschutz Schleswig-Holstein: ULD-Stellungnahme zum IT-Sicherheitsgesetz-Entwurf vom 13.02.2015; https://www.datenschutzzentrum.de/artikel/877-ULD-Stellungnahme-zum-IT-Sicherheitsgesetz-Entwurf.html.

[15] Stellungnahme des FIfF e.V. zum Entwurf des IT-Sicherheitsgesetzes, vorgelegt zur Anhörung des Innenausschusses des Deutschen Bundestages am 20. April 2015, https://www.bundestag.de/blob/366560/22f1e6ca62f137b23349c02ab6b2ec14/18-4-252-data.pdf.

[16] Wortprotokoll der Öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), 20. April 2015, v. a. S. 19, 29, 46f.

[17] Urteil des Europäischen Gerichtshofs vom 8. April 2014: „Elektronische Kommunikation – Richtlinie 2006/24/EG – Öffentlich zugängliche elektronische Kommunikationsdienste oder öffentliche Kommunikationsnetze – Vorratsspeicherung von Daten, die bei der Bereitstellung solcher Dienste erzeugt oder verarbeitet werden – Gültigkeit – Art. 7, 8 und 11 der Charta der Grundrechte der Europäischen Union“ In den verbundenen Rechtssachen C‑293/12 und C‑594/12; http://curia.europa.eu/juris/document/document_print.jsf?doclang=DE&text=&pageIndex=0&part=1&mode=lst&docid=150642&occ=first&dir=&cid=456823.

[18] Ebd., Nr. 34 und 36.

[19] Ebd., Nr. 54.

4 Fazit: Rechtskonforme IT-Sicherheit ermöglichen

Das ITSiG zielte den Aussagen der Bundesregierung zufolge auf eine Steigerung der IT-Sicherheit durch den verstärkten Einsatz technischer Schutzwerkzeuge, eine verbesserte Kommunikation über Risiken und Gefährdungen und eine bessere Aufklärung der Allgemeinheit ab. Diesen uneingeschränkt positiv zu bewertenden Zielen stehen in der Praxis weiter bestehende und teilweise verschärfte Probleme gegenüber.

- Das **Telemedienrecht** ist für den Bereich IT-Sicherheit mit EU-Recht unvereinbar. Es bedarf gemäß dem Verfahren vor dem EuGH einer Befugnis zur Sammlung solcher Daten, die für den Einsatz wichtiger IT-Sicherheitssysteme erforderlich sind.
- Im **Telekommunikationsrecht** wurde eine nach bisherigen Maßstäben nicht verfassungskonforme Regelung zur ausufernden Datensammlung getroffen. Den Maßstäben des EuGH im Urteil zur Vorratsdatenspeicherung gemäß ist diese Neuregelung ebenfalls ein Verstoß gegen die EU-Grundrechtecharta und mit EU-Recht unvereinbar.
- Das **strafrechtliche Risiko** für erforderliche Handlungen von IT-Sicherheitsverantwortlichen besteht in Deutschland weiterhin fort. Es fehlt die für den Austausch und die Kommunikation über Angreifer und Risiken notwendige Rechtsgrundlage.

Der Schutz der IT-Sicherheit in vernetzten IT-Systemen dient letztlich der Umsetzung von drei Grundrechten – dem Schutz des Fernmeldegeheimnisses, des Rechts auf informationelle Selbstbestimmung und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Jede Regelung muss diese drei Grundrechte in Einklang bringen. Trotz gleicher IP-Technologie und gleichen Analysewerkzeugen in der IT-Sicherheit in IP-Netzen fehlt es weiterhin an einer einheitlichen und grundrechtskonformen gesetzlichen Basis für die IT-Sicherheit im Telemedien- und Telekommunikationssektor.

Der EuGH wird voraussichtlich die Bundesregierung dazu verurteilen, im TMG eine neue Regelung für IT-Sicherheit zu schaffen. Dies sollte zum Anlass genommen werden, auch die grundrechtswidrigen Regelungen im Telekommunikationsrecht zurückzunehmen und durch eine einheitliche Regelung der IT-Sicherheit in allen auf IP-Kommunikation beruhenden Bereichen zu ersetzen, die ebenso grundrechtskonform wie praxisgerecht sind.

Lösungen sind durchaus nicht schwer zu finden. Die Bundesregierung selbst hat mit der 2009 in Kraft getretenen BSI-Gesetzesnovelle in § 5 BSIG deutlich gemacht, dass ihr das Problem bekannt ist und sich eine grundrechtskonforme Lösung formulieren lässt. Der gefundene Ansatz ist allerdings nur für eine zentrale Behörde wie das BSI anwendbar, nicht aber in der Vielfalt der Internet-Welt mit verschiedensten Beteiligten. Im Zuge der ITSiG-Beratungen wurden dem Bundestag grundrechtskonforme technisch-organisatorische Lösungen mit weniger Datenbedarf, einem weit geringeren Aufwand bei der Datenverarbeitung und einem deutlich größeren Praxisnutzen vorgelegt.[20]

Die alten und neuen Ansätze belegen, dass der Schutz der Daten und der IT-Sicherheit auch in Deutschland rechtskonform umsetzbar wäre. Das kommende EuGH-Urteil sollte Anlass sein, die bestehenden rechtlichen Defizite und Risiken zu beseitigen.

[20] Stellungnahme des FIfF e.V. zum Entwurf des IT-Sicherheitsgesetzes, a.a.O., https://www.bundestag.de/blob/366560/22f1e6ca62f137b23349c02ab6b2ec14/18-4-252-data.pdf.