Ingo Ruhmann, Ute Bernhardt

Der EuGH-Entscheid als Anstoß für mehr Rechtssicherheit in der IT-Sicherheit

Das Urteil des Europäischen Gerichtshofs zur Speicherung von Internet-Protokolldaten bei Telemedien ist eindeutig in seiner Aussage, dass das deutsche Telemediengesetz mit EU-Recht nicht vereinbar ist, soweit es die Gewährleistung der „generellen Funktionsfähigkeit der Dienste" verhindert. Doch das deutsche Recht enthält zur IT-Sicherheit weit mehr Konfliktzonen. Der Gesetzgeber sollte das EuGH-Urteil zum Anlass nehmen, diese Konflikte aufzulösen und Rechtssicherheit für die Praxis der IT-Sicherheit zu schaffen.

1 Einleitung

Der Europäische Gerichtshof (EuGH) war vom Bundesgerichtshof (BGH) zur Klärung angerufen worden, ob das deutsche Telemediengesetz (TMG) mit EU-Recht vereinbar ist. Nach § 15 TMG ist die Speicherung von Nutzungsdaten allein erlaubt für vertraglich festgelegte Zwecke und – in pseudonymisierter Form – für Werbezwecke. Verboten ist dagegen, personenbezogene Daten wie „IP-Adressen zur generellen Gewährleistung und Aufrechterhaltung der Sicherheit und Funktionsfähigkeit von Telemedien zu speichern"[1] – was somit auch für Zwecke der Verfolgung von Angriffen auf Webangebote gilt. Grund dafür ist die Verknüpfung des Personenbezuges von IP-Daten mit dem Verbot, diese Daten über die bei Telemedien eng gezogenen Grenzen hinaus zu speichern.

Der EuGH befand nun zunächst, dass „eine dynamische Internetprotokoll-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine Website, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, für den Anbieter ein personenbezogenes Datum im Sinne der genannten Bestimmung darstellt, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen."[2] Der Personenbezug wird somit von der Verfügung über Zusatzinformationen im Einzelfall abhängig gemacht[3]. Wesentlich für den weiteren Fortgang des Verfahrens vor dem BGH ist jedoch, dass das Bundesverfassungsgericht (BVerfG) bereits 2012 dynamische IP-Adressen als personenbezogene Daten einordnete[4]. Unmissverständlich ist auch die Rechtslage nach der EU-Datenschutz-Grundverordnung, in deren Artikel 4 „personenbezogene Daten" definiert sind 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 zukünftig zweifellos auf jede IP-Adresse zu.

1 Urteil des Gerichtshofes in der Rechtssache C582/14 vom 19.10.2016, Rd.-Nr. 28, http://curia.europa.eu/juris/document/document.jsf?docid=184668&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=DE&cid=1065466

2 Ebd., Beschlussgrund Nr. 1, Rd.-Nr. 65.

3 Prägnanter formulierte der Generalanwalt Manuel Campos Sanchez-Bordona im Schlussantrag in dem Verfahren und stufte dynamische IP-Adressen schon deswegen als personenbezogenes Datum ein, weil sich ein Internetdienstanbieter an einen Dritten „wenden könnte, um andere zusätzliche Daten zu erhalten, die in Verbindung mit dieser IP-Adresse die Identifizierung eines Nutzers ermöglichen". Schlussantrag des Generalanwalts Manuel Campos Sanchez-Bordona in der Rechtssache C-582/14, Rd.-Nr. 74, http://curia.europa.eu/juris/document/document.jsf?docid=178241&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=DE&cid=1065466 .

4 BVerfG, 1 BvR 1299/05 vom 24.01.2012, http://www.bverfg.de/entscheidungen/rs20120124_1bvr129905.html, Rd.-Nr. 121f, 161

Ingo Ruhmann

ist wissenschaftlicher Referent, Lehrbeauftragter im Studiengang „Security Management" an der TH Brandenburg und Mitglied im Netzwerk Datenschutzexpertise.

E-Mail: ruhmann@netzwerk-datenschutzexpertise.de

Ute Bernhardt

ist wissenschaftliche Referentin und Mitglied im Netzwerk Datenschutzexpertise.

E-Mail: bernhardt@netzwerk-datenschutzexpertise.de

Des Weiteren entschied der EuGH über das Verbot im TMG, personenbezogene Daten zur „Gewährleistung und Aufrechterhaltung der Sicherheit und Funktionsfähigkeit von Telemedien" – also für Zwecke der IT-Sicherheit – speichern zu dürfen. Der Gerichtshof erklärte dies für unvereinbar mit EU-Recht, da für Anbieter von Webservices die Speicherung von IP-Protokolldaten auch zum „Erhalt der Funktionsfähigkeit" zulässig sein müsse[5], um Angriffe zu deren Verursachern verfolgen zu können.

Eine absehbare Konsequenz des EuGH-Urteils ist ein Novellierungsbedarf am TMG, um auch die IT-Sicherheit als zulässigen Speicherungsgrund aufzunehmen. Das Urteil beendet aber weit mehr als die seit fast 10 Jahren schwelende Debatte, ob „Ministerien IP-Nummern"[6] auch für Zwecke der IT-Sicherheit speichern dürfen. Für Bundesbehörden war dies aus Sicht der Bundesregierung bereits 2009 mit der Novelle des BSI-Gesetzes gelöst, durch die das Bundesamt für Sicherheit in der Informationstechnik (BSI) unter strengen Auflagen die Befugnis erhielt, die „an den Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten" auf Schadcode zu analysieren sowie Protokolldaten für weitere Ermittlungen auszuwerten[7]. Für die Allgemeinheit der Webseiten-, Webshop- und Diensteanbieter hatte die Bundesregierung dagegen erst in dem 2014 verbreiteten Entwurf des IT-Sicherheitsgesetzes (ITSiG) eine Änderung des TMG durch Adaption des für die Störungsbeseitigung formulierten §100 Telekommunikationsgesetz (TKG) geplant, um „Regelungslücken zu schließen", dies dann aber im Dezember des Jahres u.a. wegen des EuGH-Verfahrens wieder gestrichen[8].

Mit der Änderung des TMG wären aber die bestehenden Probleme mit der juristischen Behandlung der IT-Sicherheit keineswegs gelöst. Denn mit dem ITSiG wurde 2015 ein Rechtsrahmen geschaffen, der für die konkrete Arbeit von IT-Sicherheitsfachleuten nicht nur die vom EuGH nun beanstandete Lücke bei der Sicherheit von Telemedien bestehen ließ. Für dieselbe Internet-Technik wurde den Praktikern bei Telekommunikationsangeboten eine nahezu unbegrenzte Erlaubnis zur Datenspeicherung und –verarbeitung eingeräumt und mit zusätzlichen Informationspflichten verknüpft. Die Verwendung solcher Daten aus Telekommunikationsvorgängen wiederum führt in der Praxis regelmäßig zu einem Verstoß gegen das Strafrecht.

Die rechtliche Lage in der IT-Sicherheit in Deutschland ist verfahren. Das EuGH-Urteil kann daher nur ein Anlass sein, das Recht der IT-Sicherheit zu vereinheitlichen und verfassungskonform zu regeln.

2 Das Strafrecht und die Neuregelung des TKG

Wir alle verlassen uns bei der IT-Sicherheit auf CERTs und IT-Sicherheitsfachleute in Rechenzentren von Behörden und Unternehmen. Ihre verantwortungsvolle Aufgabe ist es, Manipulationen an IT-Systemen zu verfolgen – in Telemedien ebenso wie Telekommunikationsangeboten. Die Arbeit der CERTs wird aber auf einer rechtlich prekären Grundlage ausgeübt.

Der gegenseitige Austausch über Stör- und Gefahrenquellen im Internet und über Details der erkannten Gefahren der CERTs soll es Rechenzentrums-Betreibern ermöglichen, Schadcode verbreitende (Kunden-) Rechner in deren Rechenzentrum vom Netz zu nehmen oder abzuschalten. Das ITSiG unterstützt diese von den CERTs mit dem BSI und anderen Behörden geübte Risikokommunikation durch die Verpflichtung von Betreibern kritischer Infrastrukturen, erkannte Angriffe und Manipulationen zu melden. Die Kooperation von IT-Sicherheitsverantwortlichen und Systemadministratoren ist vor allem bei kleinen Providern eines der wichtigsten Werkzeuge insbesondere bei den zur Verschleierung von Angriffen eingesetzten mehrstufigen Attacken. Auch die Bundesregierung erläutert die Arbeit des Verwaltungs-CERT-Verbunds damit, dass darin „ein Austausch zu Sicherheitsthemen inklusive Bewertung, technischer Analyse und Abstimmung von Maßnahmen" stattfinde; „Schwachstelleninformationen werden vertraulich ausgetauscht"[9]. CERTs tauschen Informationen der Art aus, dass eine oder mehrere spezifische IP-Adressen Teil eines Botnetzes oder eines DDoS-Angriffes sind, dass sich dahinter ein Command-and-Control-Server eines Botnetzes verbirgt oder von einer spezifischen IP-Adresse aus Schadcode per Mail-Anhang verbreitet wird. Betrachten wir, warum zumindest letzteres in der Regel eine Straftat darstellen dürfte.

Bevor der Bruch des Fernmeldegeheimnisses gemäß § 206 (1) Strafgesetzbuch (StGB) strafrechtlich relevant wird, müssen gleich drei Tatmerkmale zugleich erfüllt sein. Voraussetzung ist, dass ein Täter

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.

Wer als IT-Sicherheitsverantwortlicher eines Providers ein anderes Rechenzentrum bittet, den Schadcode versendenden Rechner eines dortigen Kunden vom Netz zu nehmen, erfüllt alle drei der für diese Straftat notwendigen Tatmerkmale:

a) Der oder die IT-Sicherheitsverantwortliche ist Mitarbeiter eines Providers oder TK-Unternehmens.
b) Er oder sie hat die Ergebnisse einer zunächst vermutlich automatischen – und soweit noch legalen – Analyse der Kommu-

5 Urteil des Gerichtshofes in der Rechtssache C582/14 vom 19.10.2016, Beschlussgrund Nr. 2, Rd.-Nr. 65.

6 Patrick Beuth: Ministerien dürfen IP-Adressen speichern; Zeit Online, 19.10.2016, http://www.zeit.de/digital/datenschutz/2016-10/eugh-urteil-ip-adressen-personenbezogene-daten. Die Verfahrensgeschichte seit 2006 geht auf das Urteil gegen die damalige Justizministerin Zypries zurück, die dazu verurteilt wurde, die Sammlung von IP-Daten im Webauftritt des Justizressorts einzustellen. http://www.daten-speicherung.de/data/Beschluss_AG-Mitte_2008-01-10.pdf.

7 So §5 BSIG. Die Bundesregierung begründete dies in der Novelle: „Der Begriff „Kommunikationstechnik des Bundes" umfasst grundsätzlich alle informationstechnischen Systeme und deren Bestandteile, soweit sie durch den Bund oder im Auftrag des Bundes für diesen betrieben werden und der Kommunikation oder dem Datenaustausch dienen". In der Begründung wurde zu „Schadprogrammen" ohne Differenzierung zwischen Telemedien und Telekommunikation ausgeführt: „Auch der Versand von Spam, also die massenhafte Versendung unerwünschter E-Mails, oder sogenannte DoS-Angriffe […] sind informationstechnische Routinen, die geeignet sind, unbefugt informationstechnische Prozesse zu beeinflussen", Vgl. Bt.-Drs. 16/11967

8 Stefan Krempl: Keine Vorratsdatenspeicherung mit neuem IT-Sicherheitsgesetz, heise News, 09.12.2014; http://www.heise.de/newsticker/meldung/Keine-Vorratsdatenspeicherung-mit-neuem-IT-Sicherheitsgesetz-2485524.html .

9 Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan Korte, Frank Tempel, Annette Groth, Pläne der Bundesregierung für eine neue Cybersicherheitsstrategie Bt.-Drs 18/9445, auf Frage 15

nikationsinhalte zu Verifikationszwecken manuell ausgewertet, sodann die IP-Daten eines verdächtigen Nutzers und damit die durch das Fernmeldegeheimnis geschützten Kommunikationsdaten persönlich „zur Kenntnis" genommen und das zu der IP-Adresse gehörende Rechenzentrum ermittelt.

c) Abschließend hat der Sicherheitsverantwortliche dem externen Rechenzentrum als rechtlichem „Dritten" eine Nachricht über den Inhalt der Kundenkommunikation – den Schadcode und die Umstände der Verbreitung – und die Kenndaten des spezifischen Kunden des Rechenzentrums gegeben – genauer: die vom Fernmeldegeheimnis geschützten näheren Umstände sowie Angaben aus den Inhalten der Telekommunikation.

Die vermeintliche Abhilfe durch einen Austausch zwischen IT-Sicherheitsverantwortlichen und Rechenzentrum über dessen Kunden stellt sich bei einer rechtlichen Bewertung als die drei nach § 206 StGB erforderlichen Tatmerkmale eines Bruchs des Fernmeldegeheimnisses dar, die klarer selten zu finden sind. Zentrale Abläufe der IT-Sicherheit fußen somit auf strafrechtlich sanktionierten Eingriffen in das Fernmeldegeheimnis nach Artikel 10 Grundgesetz.

Die IT-Sicherheit in Deutschland ließe sich wirksam behindern durch die Anzeige von IT-Sicherheitsverantwortlichen; allein schon ein solches Risiko dürfte die Kommunikation über Sicherheitsrisiken einschränken. Umso bedeutsamer wäre es, hier Rechtsklarheit zu schaffen.

3 Rechtssicherheit durch das Telekommunikationsrecht?

Dass CERT-Mitarbeiter wegen eines Bruches des Fernmeldegeheimnisses angezeigt werden, war unwahrscheinlich, solange sich ihre Arbeit auf konkrete Verdachtsfälle und die Abwehr von Schäden konzentrierte und der Alltag der Nutzer davon kaum betroffen war. IT-Sicherheitsverantwortliche messen daher der Strafbarkeit ihres zur Gefahrenabwehr sinnvollen Tuns wenig Bedeutung bei. Bei einigen Providern gab es aber zunehmende Bedenken, dass die rechtliche Basis für den Informationsaustausch über Gefahren und Verursacher fehlt. Von einigen Providern wurde daher der Wunsch formuliert, im ITSiG Regelungen zu verankern, um die Datenerhebung und den Datenaustausch über IT-Sicherheitsvorfälle klarer zu normieren. Umgesetzt wurde mit dem ITSiG eine Gesetzesänderung, die massiv in die Telekommunikationsvorgänge der Allgemeinheit eingreift und neue Informationspflichten definiert, ohne jedoch eine Lösung der strafrechtlichen Risiken für IT-Sicherheitsverantwortliche zu finden.

Für die analoge Telefonie und die technisch sehr begrenzten Möglichkeiten zur Fehlererkennung formulierte der Gesetzgeber 1996 in § 100 (1) TKG die Befugnis „zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer (zu) erheben und verwenden". Danach war es zulässig, ohne Einschränkung jede Form von Daten aus Telekommunikationsvorgängen zur Störungserkennung zu sammeln, zu analysieren und sich sogar auf Kommunikationsverbindungen aufzuschalten. Im heute fast vollständig auf ein All-IP-Netz umgebauten Telekommunikationsnetz lassen sich Störungen – wie auch in Telemedien – durch die Analyse durchlaufender Datenpakete und an den Netzknoten auflaufender Kommunikationsprotokolle erkennen. Durch diese heutigen Analysemöglichkeiten bei der IP-Kommunikation war die alte Befugnis des § 100 TKG zur beliebigen Sammlung von Datenflüssen – eingeschränkt allein durch den Zweck einer konkreten Störungsanalyse – grundrechtlich bereits hochgradig bedenklich.

Um auf Wünsche von Unternehmensseite zur Verrechtlichung des Informationsaustauschs der CERTs zu reagieren, räumte der Gesetzgeber mit der Novellierung des § 100 TKG im ITSiG den Internet- und Telekommunikationsprovidern – nicht aber staatlichen Stellen[10] – die Befugnis ein, 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".

Die vormalig formulierte Befugnis zur Messung flüchtiger analoger Daten im Falle einer *konkret bekannten* Störung wurde so ausweitet auf die Vorfeldkontrolle von „Störungen", die zu den genannten Leistungseinschränkungen potentiell „führen *können*", aber keineswegs schon geführt haben. Als Anlässe der Datenerhebung genannt werden die „Verfügbarkeit" nicht näher spezifizierter „Informations- und Kommunikationsdienste" sowie der Schutz vor einem „unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer".

Nach § 3 Nr. 14 TKG sind „Nutzer" aber keineswegs die Kunden eines Anbieters, sondern „natürliche oder juristische Personen, die einen öffentlich zugänglichen Telekommunikationsdienst für private oder geschäftliche Zwecke in Anspruch" nehmen – also *beliebige Beteiligte* an Kommunikationsvorgängen, deren Daten gemäß Internet-Protokoll aufgrund zufällig verfügbarer Kapazitäten über das Netz eines der angeschlossenen Telekommunikationsanbieter geleitet wird. Während ein Provider bei seinen Kunden aufgrund des Vertragsverhältnisses deren spezifische Dienstenutzung kennen und mögliche unerlaubte Zugriffe erkennen kann, bleibt es ein Rätsel, wie ein Provider bei beliebigen Nutzern anderer Anbieter eine mögliche Störung der Verfügbarkeit oder gar einen „unerlaubten Zugriff" auf deren IT-System erkennen sollte.

Die Erkennung von „Störungen" oder „unerlaubter Zugriffe" wiederum macht es erforderlich, den Inhalt einer Datenkommunikation, in der sich Schadcode verbirgt, einer genauen Analyse zu unterziehen. Jedem Anwender eines Virenscanners ist nachvollziehbar, dass sich nur durch die Analyse von Dateninhalten möglicher Schadcode von einer legitimen Datenkommunikation unterscheiden lässt. Der neu gefasste § 100 TKG stellt also die Befugnis zu einer „deep packet inspection" der IP-Kommunikation beliebiger Beteiligter an Kommunikationsvorgängen dar. Dieser Eingriff in das Fernmeldegeheimnis ist umso bedenklicher, da er Providern ohne jede Einschränkung erlaubt, Daten über beliebige Netznutzer zu sammeln, auszuwerten, zu speichern und weiterzugeben.

Die nach dem § 100 TKG gewonnenen Daten bedeuten für Provider nicht nur den möglichen Nutzen, die eigenen Systeme gegen Angriffe und Schäden schützen zu können, sondern auch die Pflicht, andere Betroffene über Gefährdungen aufzuklären. Der ebenfalls neu eingeführte § 109a TKG fordert Diensteanbie-

10 Dass sich die Bundesregierung nicht selbst an der Datensammlung beteiligt, zeigt die Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan Korte, Frank Tempel, Annette Groth, Pläne der Bundesregierung für eine neue Cybersicherheitsstrategie Bt.-Drs 18/9445, Frage 20 – 21. Nach der Nutzung dieser Daten durch staatliche Stellen wurde dagegen nicht gefragt.

ter auf, 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".

Für die strafrechtliche Bewertung relevant ist dabei, dass keine Information eines Rechenzentrums – wie von Providern gefordert – vorgesehen ist, sondern die eines „Nutzers", der sein Schadcode verbreitendes IT-System wahrscheinlich nicht mehr unter seiner Kontrolle hat[11].

Auf dieser Rechtsgrundlage sieht die vom BMI vorgelegte Cyber-Sicherheitsstrategie 2016 als nächste Stufe vor, mit Providern den „Ausbau der Sensorik im Netz" zu verfolgen[12], um Cyber-Angriffe durch einen Informationsaustausch zu erkennen und zu bekämpfen. Zum Schutz der Rechte Betroffener sollen die Erkenntnisse pseudonymisiert werden. Welche Hilfe pseudonymisierte IP-Adressen bei der Bekämpfung eines konkreten Angriffs geben sollen, gehört zu den Rätseln, die das BMI den Praktikern aufgibt.

Trotz der neuen TKG-Regelungen fehlen CERTs und Providern weiterhin die Befugnis, sich mit Rechenzentren über Schadcode-Verbreiter auszutauschen; ihre Arbeit bleibt mit einem strafbaren Bruch des Fernmeldegeheimnisses verbunden.

4 Verfassungsrechtliche Bewertung

Die Entscheidung des BVerfG zur Vorratsdatenspeicherung lässt keinen Zweifel daran, in welchem Umfang durch die neu geregelten §§ 100 und 109a TKG in das Fernmeldegeheimnis nach Art. 10 GG 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 neue § 100 TKG sieht keine Eingrenzung bei Datensammlung, Speicherdauer, Analyseformen oder Weitergaben von Kommunikationsdaten und -inhalten vor. Notwendig wäre aber eine an den Verhältnismäßigkeitsgrundsatz gebundene gesetzliche Regelung, die zur Erreichung definierter Zwecke geeignet, erforderlich und angemessen ist. Diese muss

- an die Angabe eines konkreten und gravierenden Gefährdungsanlasses und nicht an eine „Störung" sowie
- 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 wurde beachtet. All dies legt es nahe, dass die Neuregelung im TKG mit Art. 10 GG unvereinbar und damit verfassungswidrig sein dürfte. Hingewiesen sei hier zusätzlich darauf, dass aus dem Urteil des EuGH zur Vorratsdatenspeicherung[14] zudem eine Unvereinbarkeit der TKG-Neuregelung mit EU-Recht folgt[15]. In Stellungnahmen[16] und der Anhörung des Bundestages[17] zum ITSiG[18] wurden die erheblichen verfassungsrechtlichen Bedenken von Rechtsexperten klar benannt. Das Parlament zog daraus keine Konsequenzen und ließ das Gesetz unverändert passieren.

5 Rechtsangleichung und neue Strategien

In der Bilanz hat das ITSiG für die Praxis der IT-Sicherheit nicht zu mehr Rechtssicherheit geführt:

- Bislang ist in Telemedien eine Datensammlung zu IT-Sicherheitszwecken verboten; der EuGH hat dies für unzulässig erklärt.
- Das TKG sieht für Telekommunikationsunternehmen und Internetprovider mit einer allein auf Verdacht erlaubten deep packet inspection tief gehende Eingriffe in das Fernmeldegeheimnis vor, die verfassungs- und europarechtlich unhaltbar sind.
- Nicht beseitigt ist für CERTs und IT-Sicherheitsverantwortliche die Gefahr strafrechtlicher Konsequenzen aus einem Bruch des Fernmeldegeheimnisses, wenn Daten wie bisher an andere Provider weitergegeben werden.

Jeder IT-Sicherheitsverantwortliche kann daher Bundesinnenminister Thomas de Maiziere bei seiner Aussage nur zustimmen: „Die rechtliche Trennung von „Telekommunikationsdiensten" und „Telemediendiensten", soweit diese zur Kommunikation genutzt werden, ist überholt"[19]. Es ging de Maiziere allerdings darum, die Regelungen zur Telekommunikationsüberwachung anzugleichen. So bleibt offen, ob das BMI auch die Konsequenzen zieht und die fortbestehende Trennung bei den Regelungen zur IT-Sicherheit in beiden Bereichen aufheben will.

11 Der das IT-System des Nutzers kontrollierende aktive Angreifer dürfte auch kaum der richtige Adressat der in § 109a TKG vorgesehenen Information und Aufforderung zur Unterlassung der laufenden Störung sein.

12 Cyber-Sicherheitsstrategie für Deutschland 2016, BMI, Berlin, 9.11.2016, S. 24

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

14 Urteil des Europäischen Gerichtshofs vom 08.04.2014: „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.

15 Vgl. Ute Bernhardt, Ingo Ruhmann: IT-Sicherheit, das EU-Recht und die Grundrechte: Neustart erforderlich; Gutachten des Netzwerks Datenschutzexpertise, 27.05.2016, http://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_eugh-itsig-2016.pdf, S. 9f

16 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.

17 Wortprotokoll der Öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), 20.04.2015, v. a. S. 19, 29, 46f.

18 Stellungnahme des FIfF e.V. zum Entwurf des IT-Sicherheitsgesetzes, vorgelegt zur Anhörung des Innenausschusses des Deutschen Bundestages am 20.04.2015, https://www.bundestag.de/blob/366560/22f1e6ca62f137b23349c02ab6b2ec14/18-4-252-data.pdf.

19 Handout des Bundesinnenministeriums zur Pressekonferenz von Bundesinnenminister de Maiziere zur Vorstellung „geplanter Maßnahmen zur Erhöhung der Sicherheit in Deutschland" am 11.08.2016 in Berlin.

Der vom BMI verantworteten „Cybersicherheitsstrategie für Deutschland 2016“ und Aussagen der Bundesregierung zufolge[20] ist vielmehr mit weiteren rechtlichen Fallstricken zu rechnen. So ist ein zentrales nationales CERT und der personelle Ausbau des Cyber-Abwehrzentrums im BSI geplant sowie die Stärkung der „CERT-Strukturen in Deutschland“[21] – ohne Rechtsgrundlagen eine nur halb so gute Idee. Aus dem BSI heraus soll eine „Mobile Incident Response Team (MIRT)“ zur Unterstützung von Behörden und Betreibern kritischer Infrastrukturen jederzeit zu Einsatzorten ausrücken. Das BKA soll eine mobile „Quick Reaction Force“ zur Unterstützung der Strafverfolgung erhalten, der Verfassungsschutz eine Sondereinsatzgruppe für Cyber-Angriffe mit nachrichtendienstlichem oder extremistischem/terroristischem Hintergrund mit speziellen Kenntnissen über Methoden militärisch-nachrichtendienstlicher Cyberattacken[22]. Ergänzt wird dies um die Absicht, verstärkt „private vertrauenswürdige IT-Firmen“ – für staatliche Aufgaben einzubinden[23] wie auch die Bundeswehr[24]. Als Reaktion auf die Enthüllungen von Edward Snowden und nach Cyber-Angriffen auf die Bundeskanzlerin und den Bundestag sind dies überfällige[25] Ansätze. Allerdings muss die Frage hier lauten, ob operative Überlegungen zur IT-Sicherheit abgekoppelt bleiben von einer grundrechtskonformen Regelung der IT-Sicherheit mit Rechtssicherheit für die handelnden Personen und dem Schutz der Rechte der Betroffenen. Diese Pläne werfen neue Fragen nach der rechtlichen Zulässigkeit solcher Eingriffe bei der Arbeit von CERTs und IT-Sicherheitsfachleute auf.

6 Fazit

Der Vergleich der praktischen Erfordernisse der IT-Sicherheit und der Rechtslage macht klar, dass es zahlreiche Baustellen bei der grundrechtskonformen Regelung der IT-Sicherheit gibt. Zu den essentiellen Feststellungen des EuGH-Urteils gehört, dass weder IT-Sicherheit noch Datenschutz allein betrachtet werden dürfen. Genauer besehen, dient der Schutz der IT-Sicherheit in vernetzten IT-Systemen der Umsetzung von drei in Einklang zu bringenden Grundrechten – dem Schutz des Fernmeldegeheimnisses, des Rechts auf informationelle Selbstbestimmung (Datenschutz) und des vom BVerfG 2008 definierten Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Sicherheit)[26].

Aus dem EuGH-Entscheid folgt die Notwendigkeit, das deutsche Telemedienrecht zu ändern. Doch auch nach diesem Urteil kommt jener seit 2006 andauernde Rechtsstreit um die Speicherung von IP-Daten zu Zwecken der IT-Sicherheit keineswegs an sein Ende, der für den Gesetzgeber in den letzten Jahren aus politischen und taktischen Erwägungen Grund genug war, daran festzuhalten, dass es bei Telemedien keine legal erhobenen IP-Daten für IT-Sicherheit und Strafverfolgung gibt. Nun ist dieser Grund entfallen, mit dem bisher gegen eine umfassende und einheitliche Regelung argumentiert wurde.

Im Telekommunikationsbereich blieb der strafrechtlich problematische Informationsaustausch von IT-Sicherheitsfachleuten ungeklärt. Stattdessen lädt die verfassungs- und EU-rechtliche Bewertung zweier neuer Normen im TKG zu erneuten und langwierigen Klagen geradezu ein. Haben wir wirklich weitere 10 Jahre Zeit, auf höchstrichterliche Entscheidungen mit heute schon absehbarem Ausgang zu warten?

Für IT-Sicherheitsverantwortliche ist nicht nachvollziehbar, warum es trotz gleicher Technologien und Analysewerkzeuge in IP-Netzen keine für den Telemedien- und Telekommunikationssektor einheitliche und vor allem grundrechtskonforme gesetzliche Basis für ihr Tun gibt. Ihr strafrechtliches Risiko besteht weiterhin. Die Cybersicherheitsstrategie führt neue operative Ideen an, deren größter Mangel die auf breiter Front ebenfalls fehlenden Rechtsgrundlagen ist.

Praxisgerechte, datensparsame und vor allem grundrechtskonforme Lösungen für den Umgang mit Daten beim Schutz der IT-Sicherheit in allen Anwendungsbereichen liegen dem Gesetzgeber vor[27]. Jetzt sollte der Weg frei sein, zu sachgerechten Regelungen der IT-Sicherheit zu kommen, die – anders als bestehende Gesetze – vor dem Bundesverfassungsgericht und dem EuGH bestehen können.

20 Kai Biermann; Patrick Beuth; Falk Steiner: Innenministerium plant drei neue Internet-Eingreiftruppen; Die Zeit, 07.07.2016, http://www.zeit.de/digital/internet/2016-07/cyberangriffe-hacker-innenministerium-thomas-de-maiziere

21 Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan Korte, Frank Tempel, Annette Groth, Pläne der Bundesregierung für eine neue Cybersicherheitsstrategie Bt.-Drs. 18/9445, auf Frage 11-11d

22 Ebd. Antwort auf Frage 17, Cyber-Sicherheitsstrategie 2016, S. 29

23 Ebd. Antwort auf Frage 27-27d, ebenso Cyber-Sicherheitsstrategie 2016, S. 29

24 Vgl. den Abschlussbericht Aufbaustab Cyber- und Informationsraum des Bundesministeriums der Verteidigung, April 2016. Die Frage nach dem Einsatz von Bundeswehr-Kräften bei IT-Sicherheitsvorfällen allgemein bedarf einer eigenen rechtlichen Würdigung, die den Rahmen hier sprengen würde.

25 Vgl.: Ingo Ruhmann: NSA, IT-Sicherheit und die Folgen. Eine Schadensanalyse; in: DuD 1, 2014, S. 40-46

26 Urteil des Ersten Senats vom 27.02.2008, 1 BvR 370/07, 1 BvR 595/07.

27 So in der Stellungnahme des FIfF e.V. zum Entwurf des IT-Sicherheitsgesetzes, ebd. https://www.bundestag.de/blob/366560/22f1e6ca62f137b23349c02ab6b2ec14/18-4-252-data.pdf.