Der Bayerische Landesbeauftragte für den Datenschutz

Bayer. Datenschutzbeauftragter • PF 22 12 19 • 80502 München

Bundesverfassungsgericht
Erster Senat

Ihr Zeichen, Ihre Nachricht vom | Unser Zeichen | München, den 26.03.2018

Stellungnahme zu den Verfassungsbeschwerden betreffend das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

Sehr geehrte Damen und Herren,

für die Übersendung der Verfassungsbeschwerden betreffend das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015, in Kraft seit 18. Dezember 2015, und die mir eingeräumte Möglichkeit zur Stellungnahme gemäß Art. 27a Bundesverfassungsgerichtsgesetz (BVerfGG) danke ich.

Die verfassungsrechtliche Beurteilung des Gesetzes hinsichtlich der Datenspeicherung hängt unter anderem davon ab, welche Auswirkungen es auf die tatsächlichen Speicherpflichten von Anbietern hat. Dementsprechend ist aus meiner Sicht zunächst zu klären, wie die gegenwärtigen technischen Gegebenheiten sind (Teil I 1.). Um es vorweg zu nehmen, scheint mir das Gesetz die Telekommunikationsvorgänge nicht angemessen zu beachten. Insbesondere werden die technischen Gegebenheiten nicht berücksichtigt, die sich durch die Umstellung der Internetprotokoll Version 4 (IPv4) auf IPv6 ergeben. Nach meiner Meinung wirkt sich dies auch auf die verfassungsrechtliche Beurteilung des Gesetzes aus (Teil I 2.).

./.

Wagmüllerstraße 18
80538 München
Postfach 22 12 19
80502 München

Telefon: 089 212672-0
Telefax: 089 212672-50
https://www.datenschutz-bayern.de
E-Mail: poststelle@datenschutz-bayern.de

Verkehrsverbindungen:
U4/U5, Haltestelle Lehel
Bus Linie 100, Straßenbahn Linie 18
Haltestelle Nationalmuseum / Haus der Kunst

Teil I

1. Technische Betrachtung bzw. Überlegungen

Während bei der Speicherung der Telefongesprächsdaten nach § 113b Abs. 2 Telekommunikationsgesetz (TKG) nicht nur die Rufnummer des Teilnehmers, sondern auch die gewählte Zielrufnummer gespeichert werden muss, müssen für die Speicherung der Internetnutzung nur Daten der „abrufenden Seite“ der Internetnutzung gespeichert werden, vgl. § 113b Abs. 3 TKG. Welche Internetseiten abgerufen werden, darf nach § 113b Abs. 5 TKG explizit nicht gespeichert werden.
Bei der Internetnutzung beispielsweise durch mobile Anwendungen („Apps“), die im Hintergrund Daten abrufen, handelt es sich im wörtlichen Sinn nicht um Daten, die nach § 113b Abs. 5 TKG nicht gespeichert werden dürfen, da es sich weder um Inhalte einer Kommunikation, noch um Daten über aufgerufene Internetseiten noch um Daten von Diensten der elektronischen Post handelt. Insofern existiert zwischen den verpflichtend zu speichernden und den Daten die nicht gespeichert werden dürfen, eine Vielzahl von Datenkategorien, über die das TKG keine Aussage trifft.

a) Entwicklung der Internetnutzung und Technik seit 2010

Im Vergleich zu 2010 haben sich nicht nur der Umfang und die Art der durchschnittlichen Internetnutzung geändert, sondern auch die genutzten Geräte und Techniken. Die Anzahl der Haushalte mit Internetanschluss war in Deutschland auch 2010 mit 82% schon relativ hoch. Der Anteil erreichte 2017 aber 93%, so dass aktuell angenommen werden kann, dass nahezu jeder Haushalt von den Speicherpflichten des § 113b TKG erfasst wird[1].
Auch der Umfang der Nutzung ist deutlich gestiegen. Nutzten 2010 ca. 50% das Internet täglich, stieg der Wert auf 72% im Jahr 2017[2].
Die Art der Nutzung des Internets hat sich von überwiegend „Surfen auf Webseiten“ hin zur Nutzung von Apps verschoben**.** Bereits 2014 nutzten mehr Personen das In-

[1] https://de.statista.com/statistik/daten/studie/153257/umfrage/haushalte-mit-internetzugang-in-deutschland-seit-2002/ (26. März 2018).

[2] http://www.ard-zdf-onlinestudie.de/files/2017/Artikel/Kern-Ergebnisse_ARDZDF-Onlinestudie_2017.pdf (26. März 2018).

ternet über Smartphones als über PCs[3]. Insofern greifen die Speicherpflichten des § 113b TKG nicht nur bei der Nutzung zum Aufruf von Webseiten, sondern auch bei ausschließlicher Nutzung beispielsweise von Gesundheits-Apps oder beim Hören von Musik (Streaming).

Dieses immer noch anhaltende Wachstum des Internets hat aber auch dazu geführt, dass sich die Zugangstechnik gewandelt hat bzw. sich in den nächsten Jahren weiter wandeln wird. Ob ein Internetnutzer sich über einen langsamen oder schnellen DSL-Anschluss mit dem Internet verbindet, ist für die Speicherpflichten nicht relevant. Auswirkungen hat aber die immer dringender werdende Knappheit von Internetprotokoll-Adressen (IP-Adresse).

Auch wenn an fast allen Stellen in der Literatur allgemein über „IP-Adressen“ geschrieben wird, gibt es technisch gesehen mehrere unterschiedliche Arten von IP-Adressen. Die wesentlichste Unterscheidung ist die Version des Internetprotokolls (IP).

IPv4 ist die vierte Version des Internet Protokolls und die Version, die auch heute noch am meisten genutzt wird. IPv4 benutzt Adressen mit 32-Bit Länge, so dass es rechnerisch ca. 4,2 Milliarden (2^{32}) unterschiedliche IPv4-Adressen gibt.

Bereits 1998 wurde mit IPv6 das Nachfolgeprotokoll von IPv4 entwickelt. Auch wenn IPv6 im Internet noch nicht mehrheitlich genutzt wird, so entfallen aktuell bereits ca. 33% des in Deutschland stattfindenden Internetverkehrs auf diese Protokollversion[4]. 2010 lag der IPv6 Anteil weltweit noch unter 0,5%. Fast alle aktuellen Mobiltelefone unterstützen IPv6, so dass der Anteil bei der mobilen Nutzung des Internets noch höher liegen dürfte[5].

IPv6 bietet deutlich längere Adressen, so dass 2^{128} IPv6-Adressen nutzbar sind. Dies entspricht einer Zahl mit 38 Stellen (10^{38}). Es gibt somit gegenwärtig keine Knappheit bei IPv6-Adressen. Um die Anzahl ungefähr zu verdeutlichen: Würde man die IPv6-Adressen auf die Erdoberfläche aufteilen, ergäben sich ca. 600 Billiarden Adressen für jeden Quadratmillimeter der Erdoberfläche[6].

---

[3] http://money.cnn.com/2014/02/28/technology/mobile/mobile-apps-internet/ (26. März 2018).

[4] http://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption (26. März 2018).

[5] https://t3n.de/news/ipv6-standard-traffic-usa-738223/ (26. März 2018).

[6] http://blog.united-domains.de/2011/06/600-billiarden-adressen-pro-quadrat-millimeter-mehr-platz-im-internet-mit-ipv6/ (26. März 2018).

Da die Verfügbarkeit und die Verwendung von IPv6-Adressen deutlich von der Verfügbarkeit und Verwendung von IPv4-Adressen abweichen, hat dies wesentliche Auswirkungen, die im Folgenden in die Betrachtung der Speicherpflichten des § 113b TKG miteinzubeziehen sind. Soweit keine Unterschiede bestehen, wird allgemein nur von „IP-Adressen“ gesprochen.

b) Zur Speicherpflicht gem. § 113b Abs. 2 TKG

In § 113b Abs. 2 und 3 TKG wird der Umfang der von den in § 113a Abs. 1 TKG Genannten (Anbieter) zu speichernden Daten vorgegeben.
In § 113b Abs. 2 TKG werden die für öffentlich zugängliche Telefondienste sowie für mobile Telefondienste üblichen Daten, im Wesentlichen die entsprechenden Telefonnummern und Beginn- und Endzeitpunkte, aufgeführt. Anders als bei der Internetprotokollierung ermöglichen die gespeicherten Daten ohne Zusatzinformationen einen Rückschluss auf die eigentliche Nutzung. Sowohl die Zielnummer als auch die Tatsache, dass ein Gespräch geführt wurde, wird gespeichert.
Nachdem in Deutschland inzwischen ein großer Teil der Festnetztelefonie keine klassische analoge bzw. ISDN-Telefonie mehr darstellt, sondern technisch ein „All-IP“-Anschluss ist, der Telefongespräche als Internet-Telefondienst (Voice-over-IP, kurz VoIP) vermittelt[7], sind von den Anbietern nach § 113b Abs. 2 Nr. 5 TKG regelmäßig auch die IP-Adressen des anrufenden und des angerufenen Anschlusses und zugewiesene Benutzerkennungen zu speichern. In naher Zukunft werden grundsätzlich alle Anschlüsse in Deutschland All-IP-Anschlüsse sein.
Ob bei All-IP-Anschlüssen die gleichen IP-Adressen verwendet werden, wie bei der normalen Internetnutzung gemäß § 113b Abs. 3 TKG, hängt von den technischen Gegebenheiten des jeweiligen Anbieters ab. Sollten andere IP-Adressen als bei der Internetnutzung gespeichert werden, so handelt es sich dabei um rein technische Betriebsdaten, die datenschutzrechtlich kein zusätzliches Risiko darstellen, da die gespeicherte Telefonnummer hier das wesentliche personenbezogene Datum darstellt. Sollten die gleichen IP-Adressen verwendet werden, so müssen diese für den Anrufer nach § 113b Abs. 3 TKG ohnehin gespeichert werden. Lediglich für den Fall, dass der Angerufene nicht unter die Speicherpflichten des § 113b TKG fällt, also

wenn er sich beispielsweise im Ausland befindet, wird dessen IP-Adresse zusätzlich gespeichert. Da die VoIP-Netze der unterschiedlichen Anbieter aber grundsätzlich nicht direkt gekoppelt sind, handelt es sich bei der sichtbaren IP-Adresse des Angerufenen aber wohl nur in Einzelfällen um die eigentliche IP-Adresse des Angerufenen, sondern vielmehr um die IP-Adresse eines Vermittlungsserver beim Anbieter des Angerufenen.
Der Wortlaut in § 113b Abs. 2 Nr. 5 TKG lässt aber den Schluss zu, dass All-IP-Anschlüsse hier nicht das eigentliche Ziel der Regelung waren, auch wenn diese technisch die Bedingungen erfüllen würden. Das Ziel der Regelung waren wohl „echte“ VoIP-Anbieter, bei denen ein Nutzer auch einen Vertrag zur VoIP-Nutzung schließt und nicht die Fälle, in denen vom Nutzer unbemerkt die normale Telefonie vom Anbieter technisch über VoIP zur Verfügung gestellt wird.
VoIP-Anbieter haben zusätzlich zu den vorhandenen Telefonnummern auch noch die IP-Adressen der Teilnehmer zu speichern. Da der Anrufer hier nicht ortsgebunden sein muss (er kann jeden Internetanschluss verwenden), entspricht die Speicherung der IP-Adresse hier ersatzweise der Speicherung der Funkzelle in § 113b Abs. 4 TKG, auch wenn eine Geolokation mittels der IP-Adresse oft ungenauer sein kann. Insofern ist technisch § 113b Abs. 2 Nr. 5 TKG analog zu § 113b Abs. 4 TKG zu bewerten.
Im Ergebnis berücksichtigt § 113b Abs. 2 S. 2 Nr. 5 TKG nicht die gegenwärtige Praxis, dass nicht mehr der Kunde selbst VoIP auf seinem IT-Gerät installiert, sondern, dass dies heute regelmäßig durch den Anbieter eingesetzt wird.

c) Zur Speicherpflicht nach § 113b Abs. 3 TKG

Eine datenschutzrechtliche Beurteilung der Auswirkungen der Speicherung der in § 113b Abs. 3 TKG genannten Daten ist nur möglich, wenn auch die Zugangstechnik, mit der die Teilnehmer eines Anbieters das Internet nutzen, in die Beurteilung mit einbezogen wird. Je nach Anbieter erhält der Nutzer einen klassischen „IPv4-Zugang“, einen IPv4-Zugang ohne öffentlicher IPv4-Adresse oder (zusätzlich) einen „IPv6-Zugang“.

---

[7] https://www.telekom.com/de/blog/netz/artikel/die-10-wichtigsten-fragen-und-antworten-zur-

Fall 1: Zugang mittels IPv4 und öffentlicher IPv4-Adresse

Bei dem bereits genannten klassischen IPv4-Zugang erhält der Teilnehmer zu Beginn der Nutzung, also wenn er beispielsweise den von ihm genutzten DSL-Router einschaltet, eine öffentliche (siehe auch Fall 2) IPv4-Adresse von seinem Anbieter. Ruft er eine Webseite auf, so wird gegebenenfalls diese IPv4-Adresse vom Betreiber der Webseite protokolliert. Die in § 113b Abs. 3 TKG geforderte Speicherung bewirkt, dass ermittelbar ist, welcher Teilnehmeranschluss die Webseite aufgerufen hat. Hierzu sind aber auch Daten außerhalb der Protokollierung beim Anbieter, also beispielsweise beim Betreiber der Webseite, erforderlich, so dass nur in der Verknüpfung der Speicherung beim Anbieter des Internetzugangs mit der Speicherung beim Betreiber der Webseite die Internetnutzung nachvollzogen werden kann. Ausschließlich mit der Speicherung der IPv4-Adresse beim Anbieter sind keine Rückschlüsse auf die eigentliche Internetnutzung des Teilnehmers möglich.

Fall 2: Zugang mittels IPv4 und privater IPv4-Adresse

Das starke Wachstum des Internets hat aber bei IPv4 zu einer Adressknappheit geführt. Dadurch können vor allem die noch nicht so lange am Markt aktiven Anbieter ihren Teilnehmern keine dieser Adressen mehr exklusiv zuteilen, da sie weniger Adressen zur Verfügung haben, als sie für alle ihre Teilnehmer benötigen würden.
Eine Lösung hierfür ist die Vergabe von privaten IPv4-Adressen, die nur innerhalb der Netze des jeweiligen Anbieters Geltung haben. Alleine mit diesen privaten IP-Adressen kann der Teilnehmer aber beispielsweise Webseiten im Internet nicht aufrufen. Um dies trotzdem zu ermöglichen, ersetzt der Anbieter die private IPv4-Adresse durch eine öffentliche, sobald ein Teilnehmer auf das Internet zugreift. Trifft die Antwort aus dem Internet ein, so wird die öffentliche Adresse wieder durch die private rückersetzt. Mehrere Teilnehmer können so gleichzeitig eine einzige öffentliche IPv4-Adresse verwenden („Carrier-grade NAT**“**). Die Rückersetzung funktioniert dadurch, dass für die einzelnen Teilnehmer unterschiedliche „Ports“ verwendet werden. Nur anhand dieser Ports kann die Antwort der Webseite den Teilnehmer erreichen.

---

umstellung-auf-den-ip-anschluss-65450 (26. März 2018).

Nach § 113b Abs. 3 Nr. 1 TKG ist vom Anbieter die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse zu speichern. Die „Häufig gestellte Fragen zur Speicherung und Übermittlung von speicherpflichtigen Verkehrsdaten nach den §§ 113a und 113b TKG“ der Bundesnetzagentur (Stand 05.05.2017) konkretisieren die gesetzlichen Anforderungen insofern, dass bei einer Mehrfachnutzungen von öffentlichen IP-Adressen, (nur) die öffentliche IP-Adresse nach § 113b Abs. 3 Nr. 1 TKG zu speichern ist – und nicht (auch) eine private. Weitere Verkehrsdaten wie die Portadressen dürfen demnach ebenfalls nicht gespeichert werden.
Insofern wäre es dadurch dann wohl für eine Strafverfolgungsbehörde grundsätzlich nicht mehr möglich, einen Teilnehmeranschluss eindeutig zu ermitteln[8]. Es können durchaus 60 oder mehr Teilnehmer für einen fraglichen Webseiten-Zugriff in Frage kommen. Hier lässt sich nicht ausschließen, dass unbeteiligte Dritte, die unbemerkt und von ihnen auch unvermeidbar die gleiche öffentliche IPv4-Adresse zugeteilt bekommen haben, von Auskunftsersuchen erfasst werden.

Fall 3: Zugang mittels IPv6

Bei dem IPv6 besteht keine „Adress-Knappheit“ mehr und Anbieter können jedem Teilnehmer öffentliche IPv6-Adressen zuteilen. Allerdings wird einem Teilnehmer nicht mehr *eine* Adresse zugeteilt, sondern mindestens ein ganzer Adressblock („Präfix“). Je nach Anbieter dürfte die Größe des Blocks variieren, aber eine Zuweisung von sehr viel mehr als eine Milliarde Adressen für einen einzelnen Teilnehmer dürfte nicht unüblich sein. Aus diesen IPv6-Adressen kann jedes Gerät, also beispielsweise der PC des Teilnehmers, grundsätzlich beliebig auswählen. Ein Gerät kann sogar für jede einzelne Abfrage im Internet jeweils eine andere zufällige Adresse benutzen. Es wird dem Teilnehmer somit keine wie in § 113b Abs. 3 Nr. 1 TKG genannte Internetprotokoll-Adresse zugewiesen, sondern ein gesamter Netzblock von IPv6-Adressen.
Aus technischen Gründen ist es aber auch nicht unüblich, einem Teilnehmer mehrere derartige Blöcke zuzuweisen, aus denen die Geräte dann beliebig IPv6-Adressen zur Nutzung wählen können[9].

---

[8] http://www.datacenterknowledge.com/archives/2013/02/06/carrier-grade-nat-a-look-at-the-tradeoffs (26. März 2018).

[9] https://www.comconsult-research.de/ipv6-interface-adresse/ (26. März 2018).

Im Ergebnis erscheint der Gesetzestext nicht ausreichend konkret, da er in § 113b Abs. 3 TKG nur von der Speicherung der dem Teilnehmer für eine Internetnutzung zugewiesenen Internetprotokoll-Adresse spricht, sodass - auch wenn das TKG als grundrechtskonform anzusehen sein sollte - in der konkreten technischen Umsetzung die Gefahr besteht, dass überschießend - oder aber auch im Sinne einer effektiven Strafverfolgung - zu wenig Daten protokolliert werden.

Fall 4: IPv4/IPv6 Mischbetrieb

Ohne technische Umsetzung sind mittels IPv6-Adressen Dienste im Internet, die nur IPv4-Adressen anbieten, nicht nutzbar. Daher existieren viele Techniken (z.B. Dual Stack / Dual Stack Lite[10]), die eine Adressumsetzung oder eine gleichzeitige IPv4 und IPv6 Nutzung ermöglichen. Analog zu Fall 2 dürfte eine eindeutige Zuordnung der öffentlich gemeinsam genutzten IPv4-Adresse zu einem konkreten IPv6-Teilnehmeranschluss nicht mit den nach § 113b TKG zu speichernden Daten möglich sein. Wie die Formulierung in § 113b TKG auf komplexere Szenarien wie einen IPv4/IPv6 Mischbetrieb ausgelegt werden kann, ist zumindest nicht offensichtlich.
Die im IPv6 zugeteilten IP-Adressen sind nicht nur dynamische IP-Adressen, sondern können auch statische IP-Adressen sein, da ja gerade keine Adressenknappheit mehr vorliegt. Allerdings wird in der Regel der Nutzer keine Kenntnis davon haben, welche Art von IP-Adresse er gerade nutzt. Er wird auch in der Regel nicht auswählen können, ob er eine dynamische oder eine statische IP-Adresse verwendet.

d) Zur Funkzellenspeicherung nach § 113b Abs. 4 TKG

Nach § 113b Abs. 4 Satz 2 TKG ist bei öffentlich zugänglichen Internetzugangsdiensten im Fall der mobilen Nutzung die Bezeichnung der bei Beginn der Internetverbindung genutzten Funkzelle zu speichern.
Aus technischer Sicht unklar erscheint hier der Begriff des „Beginns der Internetverbindung“**.** Ein Großteil der aktuellen Mobiltelefone dürfte dauerhaft mit dem Internet „verbunden“ sein, ein Beginn scheint hier nicht offensichtlich erkennbar zu sein.

[10] http://www.ipv6-portal.de/glossar/dual-stack.html (26. März 2018).

Die Bundesregierung antwortete auf die Frage 29a der Kleinen Anfrage der Abgeordneten Jan Korte, Dr. André Hahn, Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE (Drucksache des Deutschen Bundestags 18/5851[11]) nach der Definition des Begriffs „Beginn der Internetnutzung“:
„Der Beginn wird allgemein durch die Zuteilung einer IP-Adresse nach dem Anmeldeprozess bestimmt, der zum Beispiel durch das Anschalten des heimischen Routers ausgelöst wird.“
Nach dieser Antwort dürfte lediglich beim Einschalten des Mobiltelefons (nach dem Entsperren der SIM-Karte) die IP-Adresse protokolliert werden, sofern diese dauerhaft dem Mobiltelefon zugewiesen bleibt. Bei einem immer eingeschalteten Mobiltelefon, das in einem guten Empfangsgebiet betrieben wird, müsste bei dieser Auslegung des Gesetzestextes nur sehr selten die Funkzelle protokolliert werden.
Frage 29b und c versuchen die Speicherung gerade im Hinblick auf „immer-online“-Geräte zu konkretisieren. Leider lässt sich aus den Antworten nicht entnehmen, wann genau eine neue Verbindung aufgebaut wird.
Der im Gesetzestext genutzte Begriff der „Internetverbindung“ ist aus technischer Sicht nicht eindeutig. Denkbar wäre als Internetverbindung beispielsweise auch der Abruf einer einzelnen Webseite (danach folgt eine Zeit ohne aktiven Netzwerkverkehr, so dass man die Verbindung als beendet ansehen könnte), oder die einzelnen Abrufe der Elemente, die für eine Ansicht einer Webseite benötigt werden (technisch erfolgt die Übertragung einzelner Elemente grundsätzlich mit je einer eigenen Verbindung).
Im Extremfall könnte man bei einem Mobiltelefon das üblicherweise mittels IPv6 mit dem Internet kommuniziert und für jede Datenübertragung eine andere IPv6-Adresse wählt, bei jeder Verbindung von einer „neuen Verbindung“ ausgehen und damit ein sehr detailliertes Bewegungsprofil erhalten. Funkzellen sind in den letzten Jahren sehr klein geworden – einige sind lediglich 50m groß –, wodurch sich eine Bewegung sehr detailliert nachvollziehen ließe. Die immer höher benötigten Datenraten bei der mobilen Internetnutzung werden dazu führen, dass in Zukunft Funkzellen immer öfter immer kleiner werden müssen und somit die Genauigkeit der Standortdaten steigen wird. Die Zeiträume in denen ein Mobiltelefon nicht zumindest einige wenige Daten

[11] http://dipbt.bundestag.de/doc/btd/18/059/1805965.pdf (26. März 2018).

überträgt und damit zu einer neuen Verbindung führt, dürften nicht mehr sehr groß sein, in Zukunft aber jedenfalls immer kleiner werden.
Diese Auslegung des Gesetzes würde dazu führen, dass jeder einzelne Datenabruf eine eigene Internetverbindung darstellt, was früher oder später zu einer lückenlosen und detaillierten Überwachung des Aufenthaltsortes führen würde.
Über die durch die Speicherpflichten des § 113b TKG umfassten Daten hinaus speichern Anbieter insbesondere aus Abrechnungsgründen aber ebenfalls – unter Umständen auch noch wesentlich umfangreicher – personenbezogene Daten. 2010 waren dies wohl hauptsächlich Einzelverbindungsnachweise über die geführten Telefongespräche bzw. die versendeten Kurznachrichten (SMS). Auch dies hat sich durch die Volumentarife der mobilen Internetnutzung und viele „Flat-Rate“-Angebote für Telefonie und SMS verschoben. Es werden also wohl vermehrt die Internet-Nutzung und weniger die Telefongespräche protokolliert. Offen bleibt hier die Frage, ob auch die gesetzlichen Regelungen für diese Speicherungen den aktuellen technischen Gegebenheiten noch gerecht werden.

2. Eingriffsintensität der Vorratsdatenspeicherung – rechtliche Beurteilung

Nach Beleuchtung der technischen Gegebenheiten und Entwicklungen möchte ich nun auf die daraus zu ziehenden rechtlichen Konsequenzen eingehen.

a) Es bestehen bereits Zweifel an der Verfassungsmäßigkeit der angegriffenen Normen im Hinblick auf die Anforderung des BVerfG hinsichtlich der Normenklarheit. Der Gesetzgeber hat Anlass, Zweck und Umfang des jeweiligen Eingriffs bereichsspezifisch, präzise und normenklar festzulegen (BVerfGE 100, 313 (359f., 372); 13, 348 (375); 125, 260 (328)). Unter Bezugnahme auf das oben Gesagte ist nicht normenklar und bestimmt genug gewährleistet, welche Daten der Speicherpflicht unterfallen. Es ist vom Wortlaut her unklar, ob VoIP und All-IP angemessen berücksichtigt sind. Drüber hinaus lässt sich bei der Vergabe von IP-Adressen mittels IPv4 nicht ausschließen, dass unbeteiligte Dritte, die unbemerkt und von ihnen auch unvermeidbar die gleiche öffentliche IPv4-Adresse zugeteilt bekommen haben, von Auskunftsersuchen erfasst werden. Bei einem Zugang mittels IPv6 erscheint der Gesetzestext außerdem nicht ausreichend konkret, da er in § 113b Abs. 3 TKG nur von der Speicherung der dem Teilnehmer für eine Internetnutzung zugewiesenen IP-Adresse

spricht, sodass - auch wenn das TKG als grundrechtskonform anzusehen sein sollte - in der konkreten technischen Umsetzung die Gefahr besteht, dass überschießend, da Blöcke von IP-Adressen vergeben werden, - oder aber auch im Sinne der Strafverfolgung - zu wenig Daten protokolliert werden.
Im Rahmen der Funkzellenspeicherung gem. § 113b Abs. 4 Satz 2 TKG ist aus technischer Sicht der Begriff des „Beginns der Internetverbindung“ und der Begriff „Internetverbindung“ selbst unklar. Im Extremfall könnte man bei einem Mobiltelefon das üblicherweise mittels IPv6 mit dem Internet kommuniziert und für jede Datenübertragung eine andere IPv6-Adresse wählt, bei jeder Verbindung von einer „neuen Verbindung“ ausgehen und damit ein sehr detailliertes Bewegungsprofil erhalten. Funkzellen sind in den letzten Jahren sehr klein geworden, wodurch sich eine Bewegung sehr detailliert nachvollziehen ließe. Die immer höher benötigten Datenraten bei der mobilen Internetnutzung werden dazu führen, dass in Zukunft Funkzellen immer öfter immer kleiner werden müssen und somit die Genauigkeit der Standortdaten steigen wird. Eine solche Auslegung würde zu einem sehr gewichtigen Eingriff führen.
Im Ergebnis lässt der Gesetzestext je nach technischen Gegebenheiten und Auslegung einen Speicherungsumfang in beiden Extremen zu. Von der Speicherung des Standorts nur beim Einschalten des Geräts bis hin zu einer möglicherwiese lückenlosen Protokollierung aller Funkzellenwechsel könnte alles von den Pflichten des § 113b TKG umfasst sein.

b) Zu berücksichtigen ist im Zusammenhang mit der Umstellung von IPv4 auf IPv6 zudem der Beschluss des BVerfG vom 24. Januar 2012 (1 BvR 1299/05, BVerfGE 130, 151). In diesem Beschluss hat der Senat zu einigen Aspekten Stellung genommen, die nach dem Vorratsdatenurteil vom 02. März 2010 (BVerfGE 125, 260) offen geblieben waren. Dies betrifft insbesondere die Zulässigkeit der Zuordnung einer dynamischen IP-Adresse, die nach dieser Entscheidung nicht im manuellen Auskunftsverfahren nach § 113 Abs. 1 S. 1 TKG a.F. erfolgen darf (Leitsatz). Begründet wurde dies unter anderem damit, dass es an einer hinreichend deutlichen und normenklaren Regelung, ob und unter welchen Voraussetzungen eine Identifizierung – Deanonymisierung – erlaubt werden soll, fehlt (BVerfGE 130, 151 (204f.)).
Mit der Umstellung der Vergabe von IP-Adressen auf das IPv6 steigt auch die Bedeutung von statischen IP-Adressen wieder. So können im IPv6 neben dynamischen auch statische IP-Adressen an private Endnutzer vergeben werden. Diesbezüglich

hat das BVerfG bereits in seiner Entscheidung vom 24.01.2012 festgestellt, dass bei weiterer Verbreitung der *„Vergabe statischer IP-Adressen, etwa auf der Basis des Internetprotokolls Version 6 … der Vorschrift [§ 112 TKG a.F.] ein deutlich größeres Eingriffsgewicht zukommen [kann]“* (BVerfGE 130, 151 (190)). Dem Gesetzgeber wurde deshalb mit dem Beschluss vom 24. Januar 2012 eine Beobachtungs- und gegebenenfalls Nachbesserungspflicht aufgegeben (BVerfGE 130, 151 (199)). Dieser Nachbesserungspflicht ist der Gesetzgeber – trotz Zunahme dieser Verwendung von IPv6 – nicht nachgekommen. So findet sich auch in der Gesetzesbegründung (BT-Drucksache 15/5508) kein Hinweis auf die Änderung der Zugangstechnik von IPv4 auf IPv6.

Nach dieser Rechtsprechung wurde eine Zuordnung – Deanonymisierung – von dynamischen IP-Adressen im manuellen Auskunftsverfahren für unzulässig erklärt. Es wurde bei der Zuordnung von statischen IP-Adressen kein schwerer Eingriff angenommen, da zum einen diese statischen IP-Adressen ohnehin öffentlich zugänglich seien und zum anderen sich im Wesentlichen auf Institutionen und Großnutzer beschränkten. Der Bürger sei also kaum davon betroffen.

Nach der Gesetzesbegründung enthält § 113c Abs. 1 Nr. 3 TKG eine Regelung *„für die Fälle, in denen die verpflichtend gespeicherten Daten vom Erbringer öffentlich zugänglicher Telekommunikationsdienste herangezogen werden dürfen, um für dynamische Internetprotokoll-Adressen Bestandsdatenauskünfte nach § 113 Absatz 1 Satz 3 zu erteilen“* (BT-Drucksache 18/5088, S. 40). Damit ist gerade das erlaubt, was das BVerfG in seiner Entscheidung vom 24. Januar 2012 als unzulässig erachtete, nämlich die Identifizierung von Nutzern von dynamischen IP-Adressen im Wege des manuellen Auskunftsverfahrens. Die Kombination der gem. § 113b Abs. 3 TKG zu speichernden Daten ermöglicht dann im Fall einer Bestandsdatenabfrage die Zuordnung zu einer bestimmten Person. Mit diesem Regelungskomplex ist damit die Deanonymisierung aller Nutzer, sei es dass sie statische oder dynamische IP-Adressen nutzen, möglich. Insofern wird man folglich annehmen müssen, dass die Eingriffsintensität zunimmt, da dies *„dazu führen [kann], dass hierdurch generell oder zumindest in weitem Umfang die Identität von Internetnutzern ermittelt und Kommunikationsvorgänge im Netz nicht nur für eine begrenzte Zeit, sondern auch dauerhaft deanonymisiert werden können“* (BVerfGE 130, 151 (198)).

c) In Ansehung der technischen Entwicklung und insbesondere der verschiedenen Auslegungsmöglichkeiten des Gesetzes im Hinblick auf den Speicherumfang kommt – bei einer extensiven Auslegung – durchaus in Betracht, dass das angegriffene Gesetz den Wesensgehalt der Grundrechte berührt. Das BVerfG hat in seinem Urteil vom 02. März 2010 zwar festgestellt, dass in den Wesensgehalt der geprüften Grundrechte nicht eingegriffen wird (BVerfGE 125, 260 (322); 73, 339 (387); 102, 147 (162f.)), da der Inhalt der Telekommunikation von der auf die Verkehrsdaten beschränkten Speicherung ausgespart bleibt. Auch der EuGH (Urteil vom 08. April 2014, Az.: C-293/12 und C-594/12 (Digital Rights Ireland Ltd/Minister for Communications, Marine and Naturale Recourses u.a.; NJW 2014, 2169)) vertritt die Auffassung, dass der Wesensgehalt nicht tangiert ist, soweit keine Inhaltsdaten gespeichert und abgerufen werden können (NJW 2014, 2169 (Rn. 39f.)). E contrario wird bei einer Erfassung von Inhaltsdaten der Wesensgehalt der Grundrechte tangiert und eine Rechtfertigung des Eingriffs ist nicht mehr möglich. Dies hängt allerdings unter Umständen aber auch davon ab, was die Internetdiensteanbieter für ihre eigenen Zwecke speichern und ob den öffentliche Stellen – vorausgesetzt es besteht eine Abrufnorm – Zugang zu diesen Daten gewährt werden kann. Bei einem Smartphone wird der Anbieter möglicherweise die abgerufenen Webseiten, die App-Nutzung etc. für seine Abrechnungszwecke und zur Feststellung des verbrauchten Datenvolumens speichern. Mittelbar könnte dann unter Umständen nicht ausgeschlossen werden, dass auch auf Inhaltsdaten zurückgegriffen wird, wenn beispielsweise im Rahmen einer Bestandsdatenauskunft über eine statische oder dynamische IP-Adresse der Nutzer einer Webseite identifiziert werden soll.
Es wird dabei nicht verkannt, dass das Gesetz auch verfassungskonform restriktiv ausgelegt werden kann. Dann aber ist der Nutzen für die Strafverfolgungsbehörden gering. In der Praxis besteht allerdings das Risiko, dass die Ermittlungsbehörden die Vorschriften extensiv auslegen und damit der Wesensgehalt der Grundrechte berührt wird bzw. werden kann.

d) Auch wurden nicht sämtliche vom BVerfG in seinem Urteil vom 02. März 2010 (BVerfGE 125, 260) getroffenen Feststellungen hinsichtlich der verfassungsrechtlichen Anforderungen an eine VDS umfassend umgesetzt. Auf Ausführungen an dieser Stelle kann verzichtet werden, da auf diese Aspekte die eingereichten Verfassungsbeschwerden umgehend eingehen.

e) Entscheidend ist außerdem, eine Zusammenschau der Regelungen zur Speicherung und der Abrufnormen sowie ihrer jeweilige Ausgestaltung zu betreiben. Dies insbesondere vor dem Hintergrund der Zunahme der neu geschaffenen Abrufbefugnisse. Insoweit ist festzustellen, dass Landesgesetzgeber die Vorschriften des TKG dahingehend (weit) auslegen, dass nicht nur Strafverfolgungsbehörden, sondern auch Nachrichtendienste befugt sind, Vorratsdaten abzurufen und das TKG hierfür auch korrespondierend Übermittlungsbefugnisse vorsieht. Folgt man dieser Auffassung, so wird man annehmen können, dass durch die Ausweitung der Abrufbefugnisse, insbesondere von Nachrichtendiensten, siehe beispielsweise Art. 15 Abs. 3 Bayerisches Verfassungsschutzgesetz (BayVSG), sich die Eingriffsintensität der gesetzlichen Befugnisse im Verhältnis zu 2010 insgesamt sogar erhöht hat.

Teil II

Vor dem Hintergrund des bereits Gesagten möchte ich auf die von Ihnen gestellten Fragen wie folgt eingehen:

1. Sind die angegriffenen Vorschriften mit den Anforderungen des Europäischen Gerichtshofs an entsprechende Regelungen zur vorsorglichen Datenspeicherung vereinbar (EuGH, Urteil der Großen Kammer vom 21.12.2016 – C-203/15 u.a. – Tele2 Sverige ua/Post- och telestyrelsen u.a.)?

Der EuGH hat in seiner Entscheidung vom 21. Dezember 2016 – C-203/15 u. C-698/15 – Tele2 Sverige ua/Post- och telestyrelsen u.a. (NVwZ 2017, 1025) die in seiner Entscheidung vom 08. April 2014 in der Sache C-293/12 und C-594/12 (Digital Rights Ireland Ltd/Minister for Communications, Marine and Naturale Recourses u.a. (NJW 2014, 2169)) getroffenen Feststellungen hinsichtlich der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (VDS-RL 2006/24/EG), ausdrücklich auch für nationalen Vorratsdatenspeicherungs-Gesetze bestätigt.

a) Diese EuGH-Rechtsprechung ist auf das streitgegenständliche Gesetz übertragbar. So sind die streitgegenständlichen Regelungen mit den vom EuGH geprüften Regelungen vergleichbar. Der EuGH hatte über nationale Regelungen über die Vorratsdatenspeicherung Schwedens und des Vereinigten Königsreichs zu entscheiden. Beide Regelungskonzepte verfolgten jeweils – wie auch die hier angegriffenen Normen – den (vorwiegenden) Zweck der Terrorismus- und Kriminalitätsbekämpfung. Zudem waren auch Vorschriften im Hinblick auf den Zugang zu den gespeicherten Daten streitgegenständlich.
Zweifel an der Übertragbarkeit dieser Rechtsprechung könnten allenfalls damit begründet werden, dass die in dieser Verfassungsbeschwerde angegriffenen Regelungen nicht auf der Rechtsgrundlage der VDS-RL 2006/24/EG erlassen worden sind. Zum Zeitpunkt des Inkrafttretens des angegriffenen Gesetzes war die VDS-RL 2006/24/EG bereits für ungültig erklärt worden. Die vom EuGH in seinem Urteil vom 21. Dezember 2016 geprüften Regelungen waren dagegen noch nationale Umsetzungsakte dieser inzwischen ungültigen VDS-RL 2006/24/EG. Insofern war es auch im Ergebnis nur konsequent, die nationalen Umsetzungsakte für nicht mit dem Unionsrecht – respektive den Grundrechten der Europäischen Grundrechtecharta (GRCh) – für vereinbar zu erklären. Deshalb versteht sich auch die Entscheidung vom 21. Dezember 2016 als Bestätigung der getroffenen Feststellungen im Urteil des EuGH vom 08. April 2014 in Bezug auf nationale Umsetzungsakte zur ungültigen VDS-RL 2006/24/EG.
In seiner Entscheidung vom 21. Dezember 2016 hat der EuGH jedoch klargestellt, dass die in Frage stehenden nationalen Gesetze der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation, sog. „e-Privacy-RL“, RL 2002/58 EG) unterliegen.
Ausgehend von der Rechtsprechung des EuGH in seinem Urteil vom 21. Dezember 2016 (EuGH, Urteil vom 21. Dezember 2016, NVwZ 2017, 1025 (Rn. 65ff.)) unterliegen alle nationale VDS-Gesetze der RL 2002/58/EG. In den Geltungsbereich der RL 2002/58/EG fallen nach der Rechtsprechung des EuGH nicht nur die Speicherung von Verkehrs- und Standortdaten auf Vorrat, sondern auch Rechtsvorschriften, die den Zugang der nationalen Behörden zu den von den Betreibern elektronischer

Kommunikationsdienste auf Vorrat gespeicherten Daten betreffen (EuGH, Urteil vom 21. Dezember 2016, NVwZ 2017, 1025 (Rn. 75ff.)).
Die Anforderungen des EuGH sind daher auf die hier angegriffenen Normen übertragbar, da die hier gegenständlichen Regelungen der RL 2002/58/EG unterliegen, insbesondere an Art. 15 Abs. 1 RL 2002/58/EG zu bemessen sind.

b) Die angegriffenen Vorschriften sind mit den Anforderungen des Europäischen Gerichtshofs an entsprechende Regelungen zur vorsorglichen Datenspeicherung nicht vereinbar.

aa) Mit dem Urteil des EuGH vom 08. April 2014 (EuGH, Urteil vom 08. April 2014, NJW 2014, 2169) stellte der Gerichtshof im Wesentlichen fünf Defizite sowohl materiell-rechtlicher als auch prozeduraler Natur fest, die kumulativ – dies lässt die Lesart des Urteils zu, da die Gesamtheit der Erwägungen die fehlende Erforderlichkeit begründen (EuGH, Urteil vom 08. April 2014, NJW 2014, 2169 (Rn. 69)) – zur Unverhältnismäßigkeit des Eingriffs führen. Diese bestätigte der EuGH dann in seinem Urteil vom 21. Dezember 2016 (EuGH, Urteil vom 21. Dezember 2016, NVwZ 2017, 1025) im Hinblick auf die nationalen Umsetzungsakte – jedoch im Zusammenhang mit der RL 2002/58/EG als Rechtsgrundlage der Vorratsdatenspeicherung.
Zunächst hat der EuGH kritisiert, dass der Personenkreis und der Umfang der betroffenen elektronischen Kommunikation praktisch unbegrenzt sei (EuGH, Urteil vom 08. April 2014, NJW 2014, 2169 (Rn. 56ff.); EuGH vom 21. Dezember 2016, NVwZ 2017, 1025 (Rn. 105f.)). Alle Bürger und die von ihnen verwendeten Kommunikationsmittel würden anlasslos, ausnahmslos und zusammenhangslos erfasst. Darunter fielen auch Berufsgeheimnisträger, deren elektronische Kommunikation umfassend gespeichert werde, ohne zu differenzieren, ob diese dem Berufsgeheimnis unterliegen oder nicht (EuGH, Urteil vom 08. April 2014, NJW 2014, 2169 (Rn. 58); EuGH, Urteil vom 21. Dezember 2016, NVwZ 2017, 1025 (Rn. 105f.)). Es sei keine Notwendigkeit eines Zusammenhangs zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit vorgesehen (EuGH, Urteil vom 08. April 2014, NJW 2014, 2169 (Rn. 58f.); EuGH, Urteil vom 21. Dezember 2016, NVwZ 2017, 1025 (Rn. 106, 110)).
Als Zweites sei der Zugang zu diesem geschaffenen „Datenpool“ zu weit ausgestaltet und ohne hinreichenden prozeduralen Grundrechtsschutz bei der Kontrolle der Zu-

griffskriterien (EuGH, Urteil vom 08. April 2014, NJW 2014, 2169 (Rn. 60ff.); EuGH, Urteil vom 21. Dezember 2016, NVwZ 2017, 1025 (Rn. 115ff.)). Es sei kein objektives Kriterium für den Zugang und die spätere Nutzung vorgesehen. Materielle und verfahrensrechtliche Voraussetzungen für den Zugang sowie dessen strikte Begrenzung auf Zwecke der Verhütung und Bekämpfung genau begrenzter schwerer Straftaten fehlten ebenso wie vorherige Kontrollen „durch ein Gericht oder eine unabhängige Verwaltungsstelle“ (EuGH, Urteil vom 08. April 2014, NJW 2014, 2169 (Rn. 60ff.); EuGH, Urteil vom 21. Dezember 2016, NVwZ 2017, 1025 (Rn. 115ff., 120)). Die pauschale Frist mit erheblichen Variationsmöglichkeiten (sechs Monate bis 24 Monate) ohne objektive Kriterien für die nähere Eingrenzung ist der dritte Kritikpunkt (EuGH, Urteil vom 08. April 2014, NJW 2014, 2169 (Rn. 63ff.)).
Als Viertes vermisst der EuGH – wie auch bereits das BVerfG in seiner Entscheidung vom 02. März 2010 (BVerfGE 125, 260 (325 ff.)) – einen angemessenen Missbrauchsschutz und dazu technische sowie organisatorische Schutzmechanismen einschließlich entsprechender Löschpflichten (EuGH, Urteil vom 08. April 2014, NJW 2014, 2169 (Rn. 66ff.); EuGH, Urteil vom 21. Dezember 2016, NVwZ 2017, 1025 (Rn. 109, 122)). Dies sei aber umso notwendiger, als die die Daten speichernden Unternehmen sich durch wirtschaftliche Erwägungen leiten lassen könnten (EuGH, Urteil vom 08. April 2014, NJW 2014, 2169 (Rn. 66ff.); EuGH, Urteil vom 21. Dezember 2016, NVwZ 2017, 1025 (Rn. 109)).
Als fünften Punkt fordert der EuGH schließlich eine Speicherung im Unionsgebiet, um eine Überwachung durch Behörden der EU-Mitgliedstaaten zu ermöglichen (EuGH, Urteil vom 08. April 2014, NJW 2014, 2169 (Rn. 68)).
In seiner Rechtsprechung vom 21. Dezember 2016 fordert der EuGH zusätzlich, dass der Betroffene in Kenntnis zu setzen ist, sobald die Mitteilung die behördlichen Ermittlungen nicht mehr beeinträchtigen kann (EuGH, Urteil vom 21. Dezember 2016, NVwZ 2017, 1025 (Rn. 121)).
Es bleibt bisher allerdings unklar, wie scharf dieser Kriterienkatalog vom nationalen Gesetzgeber abzuarbeiten ist, da die Unverhältnismäßigkeit gerade aus der „Gesamtheit“ aller Defizite abgeleitet wird.
Eine der Kernaussagen des Urteils des EuGH vom 08. April 2014 ist, dass die Bekämpfung des internationalen Terrorismus sowie die Bekämpfung schwerer Kriminalität eine *„dem Gemeinwohl dienende Zielsetzung“* ist, aber dennoch eine VDS nicht zu rechtfertigen vermag, wenn der damit verbundene Grundrechtseingriff nicht *„auf*

das absolut Notwendige“ beschränkt ist (EuGH, Urteil vom 08. April 2014, NJW 2014, 2169 (Rn. 52)). Klar wird durch diese Aussage aber auch, dass eine nationale VDS-Regelung mit Art. 15 Abs. 1 RL 2002/58/EG dann vereinbar sein kann, wenn sie sich in allen Punkten auf das absolut Notwendige beschränkt.
Im Übrigen werden die Voraussetzungen an eine verhältnismäßige VDS auch in dem PNR-Gutachten des EuGH vom 26. Juli 2017 (EuGH, Gutachten vom 26. Juli 2016, ZD 2018, 23) wiederholt und nochmals konkretisiert. Der EuGH lehnte in diesem Gutachten erneut eine anlasslose Vorratsdatenspeicherung von personenbezogenen Daten ab und bezog sich dabei auf die von ihm in seiner langjährigen Rechtsprechung aufgestellten Anforderungen an die VDS. Dieses Gutachten nahmen auch die unabhängigen Datenschutzbehörden des Bundes und der Länder in der 94. Konferenz am 8./9. November 2017 in Oldenburg zum Anlass und erteilten der anlasslosen Vorratsdatenspeicherung von Reisedaten eine Absage.

bb) Der deutsche Gesetzgeber hat in seiner Begründung (BT-Drucksache 18/5088, S. 23 f.) angenommen, dass die vom EuGH in seiner Entscheidung vom 08. April 2014 getroffenen Feststellungen, die im Hinblick auf die Vorgaben an eine VDS-Regelung gestellt werden, nicht vollständig übertragbar seien, da sie an einem anderen Prüfgegenstand entwickelt wurden. Dieses Argument kann nach der Rechtsprechung des EuGH vom 21. Dezember 2016 nicht mehr herangezogen werden, da der EuGH mit diesem Urteil die Vorgaben auf die nationalen VDS-Regelungen übertragen und bestätigt hat.
Der deutsche Gesetzgeber hat sich zwar bemüht, im Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 den Anforderungen des EuGH in seinem Urteil vom 08. April 2014 in vielen Detailregelungen gerecht zu werden. Den Hauptkritikpunkt - den der EuGH nun auch ausdrücklich im Urteil vom 21. Dezember 2016 für die nationalen VDS-Gesetze bestätigt hat –, nämlich die alle Nutzer erfassende, anlasslose, flächendeckende und personell, zeitlich und geografisch undifferenzierte Speicherung aller relevanten Telekommunikations-Verkehrsdaten, hat der deutsche Gesetzgeber jedoch nicht umgesetzt. Zwar ist der Bundesgesetzgeber der Auffassung, dass mit Ausnahme von Daten von Diensten der elektronischen Post (E-Mail) die Speicherung auf das absolut Notwendige beschränkt worden sei (Begründung, BT-Drucksache 18/5088, S. 23 f.). Dieser Argumentation kann allerdings nicht gefolgt werden. Allein das Verbot der

Speicherung von Inhaltsdaten der Kommunikation gem. § 113b Abs. 5 TKG führt noch nicht zu einer Beschränkung auf das absolut Notwendige. In diesem Zusammenhang fehlt auch die Begrenzung auf das „absolut Notwendige“, wenn die VDS-Regelung keine Ausnahme für Kommunikationsvorgänge vorsieht, die einem Berufsgeheimnis unterliegen. Eine solche Ausnahme sieht § 113b Abs. 6 TKG nur für Beratungsstellen i.S.v. § 99 Abs. 2 TKG, nicht aber für die anderen in § 53 Abs. 1 StPO genannten Berufsgeheimnisträger vor. Das Argument der technischen und organisatorischen Unmöglichkeit kann nicht nachvollzogen werden, da auch für die in § 99 Abs. 2 TKG aufgelisteten Stellen eine Möglichkeit gefunden wurde, die Daten schon gar nicht zu speichern. Dies wird in der Umsetzung sicherlich einer der schwerer lösbaren Punkte sein, allerdings erscheint es nicht unmöglich. Auch wenn das BVerfG in seinem Urteil vom 02. März 2010 (BVerfGE 125, 260 (334)) lediglich den Schutz vor Übermittlung von Daten von Berufsgeheimnisträgern gefordert hat, so wie es nun auch in § 100g Abs. 4 StPO teilweise – aber m.E. unzureichend – umgesetzt worden ist, dürfte man hier eine Gleichbehandlung mit den Stellen i.S.d. § 99 Abs. 2 TKG fordern. Wenn für diese Stellen eine Lösung zur Vermeidung der Speicherung, also eine Stufe vorher, gefunden worden ist, so wird man dies auch für die anderen Berufsgeheimnisträger fordern müssen. Insbesondere hatte der EuGH in seinem Urteil vom 21. Dezember 2016 gefordert, dass nur dann eine unionsrechtskonforme VDS vorliege, wenn bereits die Speicherung von Verkehrsdaten aus der Kommunikation von Berufsgeheimnisträgern, die dem Berufsgeheimnis unterliegen, ausgenommen ist (EuGH, Urteil vom 21. Dezember 2016, NVwZ 2017, 1025 (Rn. 105)). Mit der Verlagerung auf die „zweite Tür“ droht die Umgehung einer originären Prüfung der Legitimation des Speicherungs- bzw. Übermittlungsvorgangs als solchem, der unbestrittenermaßen einen eigenständigen Grundrechtseingriff darstellt. Eine unverhältnismäßige Datenspeicherung wird nicht dadurch verhältnismäßig, dass der Abruf erhöhten Anforderungen unterliegt.

Zudem fordert der EuGH auch eine Beschränkung der Verwendung der VDS-Daten für eine Bestandsdatenauskunft zu dynamischen IP-Adressen auf die Bekämpfung schwerer Straftaten. Das BVerfG hat in seinem Urteil vom 02. März 2010 eine solche Beschränkung zwar nicht als zwingend vorgesehen. Jedoch hat das BVerfG in seinem Beschluss vom 24. Januar 2012 (BVerfGE 130, 151) festgestellt, dass das manuelle Auskunftsersuchen nicht zur Zuordnung dynamischer IP-Adressen herangezogen werden darf.

Auch stellt sich die derzeitige Regelung so dar, dass nach § 113a TKG nicht zwischen dem Rufenden und dem Empfangenden unterschieden wird. Dies führt dazu, dass alle Daten doppelt gespeichert werden. Die Verpflichteten müssen also so ausgewählt werden, dass nur die absolut notwendigen Daten erfasst werden. Es würde folglich genügen, dass immer der Anbieter des Rufenden die Verkehrsdaten speichert. Dies hat zwar das BVerfG in seiner Entscheidung 2010 nicht bemängelt.
Der EuGH aber hat klargestellt, dass „…*im Zusammenhang mit dem Zweck der Bekämpfung von Straftaten Zugang grundsätzlich nur zu den Daten von Personen gewährt werden [kann], die im Verdacht stehen, eine schwere Straftat zu planen, zu begehen oder begangen zu haben oder auf irgendeine Weise in eine solche Straftat verwickelt zu sein (vgl. entsprechend EGMR, Urt. v. 4.12.2015 –47143/06 , CE:ECHR:2015:1204JUD004714306 Rn. 260 – Zakharov/Russland). Allerdings könnte in besonderen Situationen wie etwa solchen, in denen vitale Interessen der nationalen Sicherheit, der Landesverteidigung oder der öffentlichen Sicherheit durch terroristische Aktivitäten bedroht sind, der Zugang zu Daten anderer Personen ebenfalls gewährt werden, wenn es objektive Anhaltspunkte dafür gibt, dass diese Daten in einem konkreten Fall einen wirksamen Beitrag zur Bekämpfung solcher Aktivitäten leisten könnten.“* (EuGH, Urteil vom 21. Dezember 2016, NVwZ 2017, 1025 (Rn. 119)). Diese Einschränkung erfüllt die Zugangsregelung des § 113 c TKG nicht. Auch die Abrufbefugnis des § 100g Abs. 2 StPO setzt nicht voraus, dass nur Verkehrsdaten der in vorstehender Weise in Verdacht stehenden Personen übermittelt werden, sondern ermöglicht auch die Übermittlung von Verkehrsdaten tatunbeteiligter Personen zur Überführung tatverdächtiger Personen.
Die übrigen Vorgaben des EuGH dürften in den gesetzlichen Regelungen des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 umgesetzt worden sein.

2. Welche Folgen ergeben sich hieraus für die verfassungsrechtliche Beurteilung des Bundesverfassungsgerichts?

a) Der EuGH legt das Tatbestandsmerkmal *„Durchführung des Rechts der Union“* i.S.d. Art. 51 Abs. 1 S. 1 GRCh naturgemäß weit aus, wohingegen das BVerfG dieses – zwar europarechtsfreundlich – jedoch eher eng auslegt. Insbesondere hat der EuGH in seiner Entscheidung *Åckerberg Fransson* (EuGH, Urteil vom 26. Februar

2013, C-617/10, NJW 2013, 1415) den Begriff *„Durchführung des Unionsrechts“* mit dem Begriff *„Handeln im Anwendungsbereich des Unionsrechts“* gleichgesetzt, wonach ein recht mittelbarer Zusammenhang für die Eröffnung des Anwendungsbereichs des Unionsgrundrechte ausreichend sein soll.

Geht man nun davon aus, dass der Geltungsbereich der RL 2002/58/EG eröffnet ist, so muss dies aber – in Anlehnung an die bisherige Rechtsprechung des BVerfG – nicht zwingend zur Folge, dass die nationalen VDS-Rechtsvorschriften eine „Durchführung des Rechts der Union“ darstellen und damit an der GRCh zu bemessen sind, mithin der Anwendungsbereich des Art. 51 Abs. 1 S. 1 GRCh eröffnet ist.

Der Gesetzgeber hat in seiner Gesetzesbegründung (BT-Drucks. 18/5088, S. 22f.) angenommen, dass sich die Regelungen an den Grundrechten der Europäischen Union messen lassen müssen.

Das BVerfG hat – unter anderem – in seiner Entscheidung vom 24. April 2013 – 1 BvR 1215/07 (BVerfGE 133, 277 – „Antiterrordatei“) eine Vorlagepflicht an den EuGH mit der Begründung verneint, dass die europäischen Grundrechte der Grundrechte-Charta auf den zu entscheidenden Fall nicht anwendbar seien, da die angegriffenen Vorschriften nicht durch Unionsrecht determiniert seien (BVerfGE 133, 277, (313ff.); 118, 79 (95); 121, 1 (15); 125, 260 (306f.); 129, 78 (90f.)). Damit sei der Anwendungsbereich der Grundrechte-Charta i.S.d. Art. 51 Abs. 1 GRCh nicht eröffnet (BVerfGE 133, 277, (313ff.)). Es gebe keine unionsrechtliche Bestimmung, die *„die Bundesrepublik dazu verpflichtet, sie daran hindert oder ihr diesbezüglich inhaltliche Vorgaben macht“* (BVerfGE 133, 277 (315f.)). Für die Anwendung der GRCh reiche nicht jeder sachliche Bezug einer Regelung zum bloß abstrakten Anwendungsbereich des Unionsrechts oder rein tatsächliche Auswirkungen auf dieses aus (BVerfGE 133, 277 (316)).

Der EuGH konkretisierte in den Entscheidungen Siragusa (EuGH, Urteil vom 06. März 2014, C-206/13, NVwZ 2014, 575) und Hernández (EuGH, Urteil vom 10. Juli 2014, C-198/13, EuZW 2014, 795), wann der Anwendungsbereich des Unionsrechts eröffnet sein soll. Für die Frage, ob eine „Durchführung“ i.S.d. Art. 51 Abs. 1 GRCh gegeben ist, stellt der EuGH abstrakte Kriterien auf: Es komme darauf an, ob die vom Mitgliedstaat angewandte Regelung auch andere Zwecke verfolge als die unionsrechtlichen Normen, ob eine Durchführung des Unionsrechts bezweckt werde oder eine unionsrechtliche Norm den Sachverhalt beeinflussen könne. Ein angren-

zender unionsrechtlich beeinflusster Regelungsbereich oder allein mittelbare Auswirkungen auf das Unionsrecht genügen aber nicht.
Projiziert man diese Rechtsprechung des BVerfG und des EuGH auf die vorliegenden Verfassungsbeschwerden, so gibt es derzeit keine unionsrechtliche Bestimmung, die die Bundesrepublik Deutschland zur Einrichtung einer solchen VDS verpflichtet oder sie daran hindert. Entscheidende Bedeutung kommt hier jedoch der Auslegung der Richtlinie, insbesondere des Art. 15 RL 2002/58/EG, zu. Nach Art. 15 Abs. 1 S. 1 und 3 RL 2002/58/EG sind nationale Regelungen zur VDS für die nationale Sicherheit (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft zulässig, sofern sie notwendig, angemessen und verhältnismäßig sind und sie den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Art. 6 Abs. 1 und 2 EUV niedergelegten Grundsätzen entsprechen. Gemäß Art.15 Abs. 1 RL 2002/58/EG ist es also dem nationalen Gesetzgeber überlassen, ob er die VDS einführt; wenn er es aber tut, dann muss er auch die Vorgaben des Art. 15 Abs. 1 S. 3 RL 2002/58/EG erfüllen. Fraglich ist, ob dies als inhaltliche Vorgabe und damit für eine Determination durch Unionsrecht ausreichend ist.
Im Urteil vom 08. April 2014 hat der EuGH insbesondere betont, dass der EU-Gesetzgeber in der Richtlinie nicht wesentliche Punkte offen lassen und die Regelung von Wesentlichkeiten den Mitgliedstaaten überlassen könne. So hatte auch der Generalanwalt Cruz Villalón in seinem Schlussantrag am 12. Dezember 2013 in der Sache Digital Rights Ireland (BeckRS 2013, 82347 Rn. 120) geäußert, dass der Unionsgesetzgeber die Festlegung der Mindestgarantien nicht vollständig den Mitgliedstaaten überlassen dürfe. Er müsse vor dem Hintergrund des Art. 51 Abs. 1 GRCh die Grundprinzipien selbst definieren, die für die Festlegung, Einführung, Anwendung und Kontrolle der Beachtung dieser Garantien gelten sollen.
Überträgt man diese Anforderungen auf die RL 2002/58/EG, so beinhaltet auch diese Richtlinie – wie die RL 2006/24/EG – nicht die erforderliche Festlegung der Mindestgarantien. Insofern kann man die Auffassung vertreten, dass die RL 2002/58/EG keine inhaltlichen verpflichtenden Vorgaben trifft und deshalb auch keine „Determination durch Unionsrecht“ gegeben ist.

Das BVerfG hat in seiner ersten VDS-Entscheidung vom 02. März 2010 (BVerfGE 125, 260) eine Vorlage an den EuGH im Wege des Vorabentscheidungsverfahrens mit der Begründung verneint, dass es auf einen möglichen Vorrang des Gemeinschaftsrechts nicht ankomme (BVerfGE 125, 260 (307)). Die Wirksamkeit der Richtlinie 2006/24/EG und ein sich hieraus möglichweise ergebender Vorrang des Gemeinschaftsrechts vor deutschen Grundrechten sei nicht entscheidungserheblich. Der Inhalt der Richtlinie belässt der Bundesrepublik Deutschland für die Gestaltung der in ihr vorgeschriebenen Speicherung von Telekommunikationsverkehrsdaten einen weiten Entscheidungsspielraum (BVerfGE 125, 260 (308f.)). Die Regelungen der Richtlinie 2006/24/EG sind im Wesentlichen auf die Speicherungspflichten selbst beschränkt und regeln nicht den Zugang zu den Daten oder deren Verwendung durch die Behörden der Mitgliedstaaten (BVerfGE 125, 260 (308f.))
Mit der Rechtsprechung des EuGH muss man allerdings annehmen, dass die Richtlinie 2002/58/EG den Mitgliedstaaten bei der Umsetzung verpflichtende Vorgaben macht und damit auch der Anwendungsbereich der GRCh gem. Art. 51 Abs. 1 GRCh eröffnet ist. Dies hat dann zur Konsequenz, dass das streitgegenständliche Gesetz an der GRCh zu bemessen wäre. Folglich müsste das BVerfG *grundsätzlich* die Sache dem EuGH im Wege des Vorabentscheidungsverfahrens vorlegen, sofern das BVerfG das Gesetz nicht schon für mit dem GG unvereinbar ansieht.

b) Für den Fall, dass das BVerfG das Gesetz als nicht schon mit dem GG schlechthin unvereinbar ansieht, und damit eine Vorlagepflicht gem. Art. 267 Abs. 3 AEUV grundsätzlich gegeben ist – unter Zugrundelegung der unionsrechtlichen Determination – kann das BVerfG jedoch dann von der Vorlage absehen, wenn ein acte éclairé vorliegt. Darunter fallen Konstellationen, in denen *„bereits eine gesicherte Rechtsprechung des Gerichtshofs vorliegt, durch die die betreffende Rechtfrage gelöst ist, gleich in welcher Art von Verfahren sich diese Rechtsprechung gebildet hat und selbst dann, wenn die (…) Fragen nicht vollkommen identisch sind“* (EuGH, Urteil vom 06. Dezember 1982, Rs 283/81, NJW 1983, 1257 (Rn. 14) – C. I. L. F. I. T.; EuGH, verb. Rs. 28–30/62, Da Costa u. a./Niederländische Finanzverwaltung, Slg. 1963, 63 (81); Rs. C-337/95, Parfums Christian Dior/Evora, Slg. 1997, I-6013 Rn. 31; Rs. C-428/06, UGT-Rioja, Slg. 2008, I-6747 Rn. 43).
In concreto kann man allerdings annehmen, dass – vorausgesetzt das BVerfG hat Zweifel mit der Vereinbarkeit der angegriffenen Regelungen mit dem Unionsrecht

und geht von einer Entscheidungserheblichkeit aus, erklärt das Gesetz also nicht schon mit dem GG als schlechthin unvereinbar – keine Vorlagepflicht besteht, da die Thematik mit dem Urteil vom 21. Dezember 2016 bereits entschieden wurde, auch wenn – im Unterschied zu den Ausgangsfällen des EuGH – keine im deutschen Recht vergleichbaren verfahrensrechtlichen Defizite bestehen.

Mit freundlichen Grüßen

Prof. Dr. Thomas Petri