MMR
MÜLLER MÜLLER RÖSSNER
RECHTSANWÄLTE PARTNERSCHAFT

MMR | MÜLLER MÜLLER RÖSSNER | Mauerstr. 66 | 10117 Berlin

Bundesverfassungsgericht
Schlossbezirk 3

76131 Karlsruhe

CARL CHRISTIAN MÜLLER, LL.M.
Rechtsanwalt
Fachanwalt für Urheber- und Medienrecht

THOMAS G. MÜLLER, LL.M.
Rechtsanwalt

SÖREN RÖSSNER, LL.M.
Rechtsanwalt

Vorab per Fax: 0721 9101-461

Berlin, den 06.11.2015
20-0443.15ccmMMR

Antrag auf Erlass einer einstweiligen Anordnung

1. Rechtsanwalt Carl Christian Müller, Mauerstraße 66, 10117 Berlin

Antragsteller zu 1.,

2. Rechtsanwalt Thomas Gerald Müller, Mauerstraße 66, 10117 Berlin

Antragsteller zu 2.,

3. Rechtsanwalt Sören Rößner, Mauerstraße 66, 10117 Berlin

Antragsteller zu 3.,

4. Deutscher Medienverband e. V., Jägerstraße 67 – 69, 10117 Berlin, vertreten durch dessen Bundespräsidiumsvorsitzenden, Herrn Diplom Kaufmann Manfred Orle, ebenda

Antragsteller zu 4.,

5. Diplom Kaufmann Manfred Orle, Jägerstraße 67 – 69, 10117 Berlin

Antragsteller zu 5.,

6. DJV Deutscher Journalisten-Verband, Landesverband Berlin-Brandenburg e.V., vertreten durch dessen ersten Vorsitzenden, Herrn Klaus D. Minhardt, ebenda

Antragsteller zu 6.,

7. Herr Klaus D. Minhardt, Bayernallee 8, 14052 Berlin,

Antragsteller zu 7.,

8. Herr Michael Truckenbrodt, Erkelenzdamm 59, 10999 Berlin

Antragsteller zu 8.,

9. Frau Dilek Güngör, Schlegelstraße 13, 10115 Berlin

Antragstellerin zu 9.,

10. Frau Tabea Rößner, Platz der Republik 1, 11011 Berlin

Antragstellerin zu 10.,

11. Herr Jürgen Döschner, Schweinheimer Str. 71, 51067 Köln

Antragsteller zu 11.,

12. Herr .....Berlin,

Antragsteller zu 12.,

13. Herr Dr. Martin Hulpke-Wette, Nikolaistraße 29, 37073 Göttingen

Antragsteller zu 13.,

14. Herr Benedikt Lux, Niederkirchnerstraße 5, 10111 Berlin,

Antragsteller zu 14.,

15. Frau Canan Bayram, Niederkirchnerstraße 5, 10111 Berlin,

Antragstellerin zu 15.,

16. Herr Stefan Gelbhaar, Niederkirchnerstraße 5, 10111 Berlin,

Antragsteller zu 16.,

17. Herr Dirk Behrendt, Niederkirchnerstraße 5, 10111 Berlin,

Antragsteller zu 17.,

18. Frau Ramona Pop, Niederkirchnerstraße 5, 10111 Berlin,

Antragstellerin zu 18.,

19. Herr Joschka Langenbrinck, Niederkirchnerstraße 5, 10111 Berlin,

Antragsteller zu 19.,

20. Herr Sven Kohlmeier, Niederkirchnerstraße 5, 10111 Berlin,

Antragsteller zu 20.,

21. Herr Martin Delius, Niederkirchnerstraße 5, 10111 Berlin,

Antragsteller zu 21.,

22. Herr Simon Weiß, Niederkirchnerstraße 5, 10111 Berlin,

Antragsteller zu 22.

Verfahrensbevollmächtigte:

1. Rechtsanwalt Carl Christian Müller, LL.M.,
   in Sozietät MMR Müller Müller Rößner Rechtsanwälte Partnerschaft,
   Mauerstraße 66, 10117 Berlin

2. Rechtsanwalt Sören Rößner, LL.M.,
   in Sozietät MMR Müller Müller Rößner Rechtsanwälte Partnerschaft,
   Mauerstraße 66, 10117 Berlin

Der Antrag auf Erlass einer einstweiligen Anordnung wird gestellt im Hinblick auf die im Entwurf beigefügte Verfassungsbeschwerde (nur per Post),

mit der ein Verstoß durch die Art. 1 und Art. 2 des heute zustande gekommenen Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten gemäß dem vom Deutschen Bundestag am 16.10.2015 verabschiedeten Gesetzentwurf der Fraktionen der CDU/CSU und SPD (BT-Drucks. 18/5088) in der vom Ausschuss für Recht und Verbraucherschutz geänderten Fassung (BT-Drucks. 18/6391) hinsichtlich dessen der Bundesrat heute keinen Antrag gemäß Art. 77 Abs. 2 GG gestellt hat, gegen

Art. 10 Abs. 1 GG, Art. 5 Abs. 1 GG, Art. 2 Abs. 1 i. V. m. Art. 1. Abs.1 GG, Art. 12 Abs. 1 GG sowie Art. 3 Abs. 1 GG

und ausdrücklich

Art. 7, Art. 8, Art. 11, Art. 15 sowie Art. 20 der Charta der Grundrechte der Europäischen Union

gerügt wird und die unmittelbar nach Inkrafttreten des vorgenannten Gesetzes erhoben werden wird.

Unter Bezugnahme auf die diesem Antrag beigefügten Vollmachten beantragen wir namens und im Auftrag sämtlicher Antragsteller,

im Wege der einstweiligen Anordnung Artikel 1 und Artikel 2 des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten gemäß dem vom Deutschen Bundestag am 16.10.2015 verabschiedeten Gesetzentwurf der Fraktionen der CDU/CSU und SPD (BT-Drucks. 18/5088) in der vom Ausschuss für Recht und Verbraucherschutz geänderten Fassung (BT-Drucks. 18/6391) mit Wirkung von ihrem Inkrafttreten an außer Kraft zu setzen

hilfsweise,

über den vorgenannten Antrag erst nach Verkündung des vorgenannten Gesetzes im Bundesgesetzblatt zu entscheiden.

Sollte das Bundesverfassungsgericht Zweifel daran haben, dass Artikel 1 und Artikel 2 des vorgenannten Gesetzes mit Art. 7, Art. 8, Art. 11, Art. 15 sowie Art. 20 der Charta der Grundrechte der Europäischen Union unvereinbar sind, beantragen wir,

dem Gerichtshof der Europäischen Union folgende Fragen vorzulegen:

1. **Ist eine nationale Regelung, die die Vorratsspeicherung von Daten der elektronischen Kommunikation vorschreibt und**

   - **die in umfassender Weise alle Personen betrifft, die elektronische Kommunikationsdienste nutzen, ohne dass sich jedoch die Personen, deren Daten auf Vorrat gespeichert werden, auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte, und also auch für Personen gilt, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte,**

   - **die zwar zur Bekämpfung schwerer Kriminalität beitragen soll, aber keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit verlangt und insbesondere die Vorratsspeicherung weder auf die Daten eines bestimmten Zeitraums und/oder eines bestimmten geografischen Gebiets**

und/oder eines bestimmten Personenkreises beschränkt, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnten;

- **die lediglich Ausnahmen dahingehend vorsieht, dass Daten von Diensten der elektronischen Post sowie Daten, die den Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen zugrunde liegen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit besonderen Verschwiegenheitsverpflichtungen unterliegen, nicht gespeichert werden dürfen, aber darüber hinaus keinerlei Ausnahme vorsieht, so dass sie auch für sämtliche sonstigen Personen gilt, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen,**

mit dem in Art. 7 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta) verankerten Recht auf Privatleben, mit dem in Art. 8 der Charta verankerten Recht auf Schutz personenbezogener Daten, mit dem in Art. 11 der Charta verankerten Recht auf Freiheit der Meinungsäußerung, mit der in Art. 15 der Charta verankerten Berufsfreiheit sowie mit dem in Art. 20 der Charta verankerten allgemeinen Gleichheitssatz vereinbar?

2. **Ist eine nationale Regelung, die die Vorratsspeicherung von Daten der elektronischen Kommunikation vorschreibt, in Anbetracht der von Herrn Edward Snowden enthüllten Überwachungstätigkeiten von Nachrichtendiensten und anderen Behörden insbesondere der USA, die im Rahmen der von ihnen praktizierten massenhaften und wahllosen Überwachung und Erfassung weltweit und auch in der Europäischen Union auf Daten und Inhalte der elektronischen Kommunikation zugreifen, ohne dass die Unionsbürger insoweit einen wirksamen Anspruch auf rechtliches Gehör haben oder in irgendeiner Form benachrichtigt werden, und deren Zugriff auf die aufgrund der vorgeschriebenen Vorratsspeicherung gespeicherten Daten der elektronischen Kommunikation nicht ausgeschlossen werden kann,**

derzeit mit dem in Art. 7 der Charta verankerten Recht auf Privatleben, mit dem in Art. 8 der Charta verankerten Recht auf Schutz personenbezogener Daten, mit dem in Art. 11 der Charta verankerten Recht auf Freiheit der Meinungsäußerung, mit der in Art. 15 der Charta verankerten Berufsfreiheit sowie dem in Art. 47 der Charta verankerten Recht auf effektiven Rechtsschutz vereinbar?

Begründung:

I. Gegenstand des Verfahrens

Die Antragsteller begehren mit ihrem Eilantrag, die mit dem Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten gemäß dem vom Deutschen Bundestag am 16.10.2015 verabschiedeten Gesetzentwurf der Fraktionen der CDU/CSU und SPD (BT-Drucks. 18/5088) in der vom Ausschuss für Recht und Verbraucherschutz geänderten Fassung (BT-Drucks. 18/6391) von Telekommunikationsdiensteanbietern vorzunehmende Vorratsspeicherung von Telekommunikationsverkehrsdaten mit Wirkung von seinem Inkrafttreten an einstweilen auszusetzen.

Telekommunikationsverkehrsdaten sind Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden (vgl. § 3 Nr. 30 des Telekommunikationsgesetzes - im Folgenden: TKG). Durch das vorgenannte Gesetz sollen diese Daten über einen Zeitraum von vier bzw. zehn Wochen von den Erbringern öffentlich zugänglicher Telekommunikationsdienste gespeichert werden, damit sie von Be-

hörden zu repressiven Zwecken der Strafverfolgung und präventiven Zwecken der Gefahrenabwehr erhoben werden können.

1.) Vorratsdatenspeicherung

Ein Abruf von Telekommunikationsverkehrsdaten hat seit der Entscheidung des Bundesverfassungsgerichts vom 02.03.2010, mit dem die Vorgängerregelungen des angegriffenen Gesetzes für nichtig erklärt wurden, nur dann Erfolg, wenn der ersuchte Diensteanbieter die Daten zu eigenen Zwecken gespeichert hatte. Hingegen waren die Diensteanbieter seitdem nicht verpflichtet oder auch nur berechtigt, Verkehrsdaten unabhängig von ihrem eigenen Bedarf zu öffentlichen Zwecken wie der Strafverfolgung oder der Gefahrenabwehr zu speichern.

Das Bundesverfassungsgericht sah in der anlasslosen Speicherung von Telekommunikationsverkehrsdaten einen erheblichen Eingriff in die Rechte sämtlicher Nutzer elektronischer Kommunikationsdienste und entwickelte vor allem aus dem Verhältnismäßigkeitsprinzip Voraussetzungen, die vom Gesetzgeber zu beachten sind, wenn er einen Abruf und die Nutzung von Daten vorsieht. Das Urteil des Bundesverfassungsgerichts steht in Tradition seiner bisherigen Rechtsprechung, insbesondere zu den Entscheidungen zur Vertraulichkeit und Integrität informationstechnischer Systeme[1] sowie dem Volkszählungsurteil.[2] Die Grundsätze aus diesen Entscheidungen werden mit dem Urteil zur Vorratsdatenspeicherung konsequent fortgesetzt. Demnach sind Eingriffe in Persönlichkeitsrechte der Nutzer im Interesse der Strafverfolgung und Gefahrenabwehr nur unter sehr hohen Voraussetzungen und nur dann, wenn sie strengen rechtstaatlichen Anforderungen Genüge tun, zulässig. Die Rechtfertigung der Maßnahme hängt davon ab, dass gewährleistet wird, dass alle Überwachungsmaßnahmen zusammen keine Totalüberwachung der Bürger ermöglichen (Überwachungsgesamtrechnung). Die Freiheitswahrnehmung der Bürger darf nicht total erfasst und registriert werden. Dieser Grundsatz gehört nach den Feststellungen des Bundesverfassungsgerichts zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland. Damit ist bei künftigen Überwachungsmaßnahmen eine doppelte Verhältnismäßigkeitsprüfung

[1] Urt. v. 27.2.2008 – 1 BvR 370/07.

[2] Urt. v. 15.12.1983 – 1 BvR 209/83.

vorzunehmen: Die einzelne Maßnahme muss für sich genommen verhältnismäßig sein und auch die Verhältnismäßigkeit der Gesamtbelastungen muss festgestellt werden.[3]

Mit dem Koalitionsvertrag für die 18. Legislaturperiode vom 27.11.2013 hatten CDU, CSU und SPD vereinbart, die EU-Richtlinie zur Vorratsdatenspeicherung umzusetzen, um die Verhängung von Zwangsgeldern gegen Deutschland zu vermeiden.[4]

Mit Urteil vom 08.04.2014 erklärte der Europäische Gerichtshof die EU-Richtlinie zur Vorratsdatenspeicherung für ungültig und stellte insofern fest, dass sie mit der Charta der Grundrechte der Europäischen Union nicht vereinbar war.[5] Die europarechtliche Verpflichtung Deutschlands, eine Vorratsdatenspeicherung einzuführen, ist damit entfallen.

Der Europäische Gerichtshof sieht in der Verpflichtung zur anlasslosen Vorratsspeicherung von Telekommunikationsverkehrsdaten und der Gestattung des Zugangs der zuständigen nationalen Behörden zu diesen Daten einen besonders schwerwiegenden Eingriff in die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten. Nach den Feststellungen des Europäischen Gerichtshofs waren die mit der Richtlinie verbundenen Eingriffe von derart großem Ausmaß und besonderer Schwere, ohne dass sich die Eingriffe hierbei auf das tatsächlich absolut Notwendige beschränkten. Eine Regelung, die sich zur Überwachung von Telekommunikationsverkehrsdaten generell auf sämtliche Personen, elektronische Kommunikationsmittel und Verkehrsdaten bezieht, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des Ziels der Bekämpfung schwerer Straftaten vorzusehen, ist nach der Rechtsprechung des Europäischen Gerichtshofs unverhältnismäßig. Zudem stellte der Europäische Gerichtshof fest, dass eine gesetzliche Regelung, die eine anlass- und ausnahmslose Speicherung von Telekommunikationsverkehrsdaten vorsehe und damit auch für Berufsgeheimnisträger gelte, den damit einhergehenden Grundrechtseingriff nicht auf das absolut Erforderliche begrenze und damit unverhältnismäßig ist.

---

[3] BVerfG, Urt. v. 2.3.2010 – 1 BvR 246/08, Rz. 218.

[4] Seite 147 des Koalitionsvertrages, zuletzt am 06.11.2015 abgerufen unter: http://www.bundesregierung.de/Content/DE/_Anlagen/2013/2013-12-17-koalitionsvertrag.pdf?__blob=publicationFile.

[5] EuGH, Urt. v. 8.4.2014 – C-293/12 und C-594/12.

Der Anschlag auf die Redaktion von „Charlie Hebdo“ in Paris, der trotz der in Frankreich praktizierten Vorratsdatenspeicherung nicht verhindert werden konnte, befeuerte die innenpolitische Debatte um die Vorratsdatenspeicherung erneut. Der Bundesminister der Justiz und für Verbraucherschutz, der seit seinem Amtsantritt im Januar 2014 wiederholt darauf hingewiesen hatte, dass „eine anlasslose Vorratsdatenspeicherung gegen das Recht auf Privatheit und gegen den Datenschutz“ verstoße[6] und für den Fall, dass der EuGH die Richtlinie kippe, dem Koalitionsvertrag, was die Vorratsdatenspeicherung angehe, die Geschäftsgrundlage entzogen sei,[7] vollzog schließlich eine Kehrtwende und legte am 15.04.2015 „Leitlinien zur Einführung einer Speicherfrist und Höchstspeicherfrist für Verkehrsdaten“[8] vor, die am 15.05.2015 in einen Referentenentwurf für ein Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten mündete.

Am 16.10.2015 hat der Bundestag nach zweiter und dritter Lesung die Wiedereinführung der Vorratsdatenspeicherung beschlossen. Der von der Regierungskoalition eingebrachte Gesetzentwurf[9] wurde in der vom Rechtsausschuss geänderten Fassung[10] in namentlicher Abstimmung mit den Stimmen der Koalition verabschiedet. Für den Gesetzentwurf stimmten 404 Abgeordnete, 148 stimmten mit Nein, sieben weitere enthielten sich.

Das Gesetz passierte als Einspruchsgesetz am heutigen Tage den Bundesrat. Es wird am Tag nach seiner Verkündung in Kraft treten.

Das Gesetz verpflichtet Telekommunikationsunternehmen, die folgenden Telekommunikationsverkehrsdaten zu speichern:

- Standortdaten der Teilnehmer aller Mobiltelefonate sind bei Beginn des Telefonats für die Dauer von vier Wochen zu speichern.

---

[6] DER SPIEGEL 13/2015, S. 34 f.

[7] http://www.heise.de/newsticker/meldung/Justizminister-Heiko-Maas-legt-Vorratsdatenspeicherung-auf-Eis-2075205.html, zuletzt abgerufen am 02.11.2015.

[8] Abrufbar unter: http://www.bmjv.de/SharedDocs/Kurzmeldungen/DE/2015/20150415_Leitlinien-HSF.html?nn=3433226, zuletzt abgerufen am 02.11.2015.

[9] BT-Drs. 18/5088.

[10] BT-Drs. 18/6391.

- Standortdaten bei Beginn einer mobilen Internetnutzung sind ebenfalls für die Dauer von vier Wochen zu speichern.

- Rufnummern, Zeit und Dauer aller Telefonate sind für die Dauer von zehn Wochen zu speichern.

- Rufnummern, Sende- und Empfangszeit aller SMS-Nachrichten sind für die Dauer von zehn Wochen zu speichern.

- Dem Internetnutzer zugewiesene IP-Adressen sowie Zeit und Dauer der Internetnutzung sind für die Dauer von zehn Wochen zu speichern.

Die Daten sind im Inland zu speichern und nach Ablauf der vorgeschriebenen Frist zu löschen.

In der Gesetzesbegründung wird mit Blick auf das mit dem Gesetz verfolgte Ziel auf Lücken bei der Strafverfolgung und bei der Gefahrenabwehr abgestellt. Nach geltender Rechtslage sei es vom Zufall abhängig, ob Verkehrsdaten zum Zeitpunkt der Anfrage noch vorhanden gewesen seien oder nicht.[11] Belastbare Angaben dazu, in wie vielen Fällen Abrufe von Verkehrsdaten seit dem 02.03.2010 erfolglos blieben, weil die Verkehrsdaten nicht über das Verbindungsende hinaus gespeichert oder zwischenzeitlich gelöscht worden waren, sind jedoch nicht bekannt.

Dies gilt auch dafür, wie viele Straftaten und Gefahren im Zeitraum bis zum 02.03.2010 ausschließlich aufgrund der Möglichkeit der Erhebung von auf Vorrat gespeicherten Telekommunikations-Verkehrsdaten aufgeklärt bzw. abgewehrt werden konnten und bei wie vielen Straftaten und Gefahren eine Aufklärung bzw. Abwehr wegen der bereits erfolgten Löschung dieser Daten nicht möglich war. Belastbares Zahlenmaterial existiert auch nicht in Bezug auf die Frage nach dem Nutzen des angegriffenen Gesetzes. Eine seriöse Studie hierzu gibt es nicht.[12] Ob allerdings mit einer Speicherung der Telekommunikationsdaten von mehr als 80 Millionen Bürgern tatsächlich Kriminalität, insbesondere der internationale Terrorismus, wirksam bekämpft werden kann, darf mit guten Gründen bezweifelt werden. Nach einem Gutachten des wissenschaftlichen Dienstes des Deutschen Bundestages, das sich auf Zahlen des Bundeskriminalamtes beruft,

[11] BT-Drs. 18/5088, Seite 21.

[12] Vgl. Nachbaur, ZRP 2015, 215, 216.

hat die Vorratsdatenspeicherung auf die Aufklärungsquoten in den EU- Mitgliedsstaaten „praktisch keine Auswirkungen". Die Aufklärungsquote steige mit der Vorratsdatenspeicherung nur marginal, nämlich um 0,006 %.[13] Umgekehrt liegen zu der Frage, welche Auswirkungen mit dem Wegfallen der Vorratsdatenspeicherung seit dem Urteil des Bundesverfassungsgerichts verbunden sind, insbesondere zu der Frage, ob die Aufklärungsquote signifikant gesunken ist, ebenfalls keine belastbaren Erkenntnisse vor.[14] Der Deutsche Anwaltverein führt hierzu in einer Stellungnahme zu dem Gesetzesentwurf aus wie folgt:

> *„Obwohl also keine gesicherten empirischen Erkenntnisse darüber vorliegen, ob mit der flächendeckenden Vorratsdatenspeicherung das Ziel der Gefahrenabwehr und der Strafverfolgung überhaupt erreicht werden kann, soll in das Grundrecht aus Art. 10 GG von 80 Millionen Bundesbürgerinnen und Bundesbürgern eingegriffen und die eine Demokratie ausmachende freie und offene Kommunikation gefährdet sowie das Risiko eines Datenmissbrauchs angelegt werden."*[15]

Diese Gefährdungslage für die Kommunikationsfreiheiten verschärft sich etwa auch in Bezug auf die durch die Enthüllungen von Herrn Edward Snowden bekannt gewordenen Tätigkeiten nationaler und internationaler Nachrichtendienste auch in Deutschland in Bezug auf die massenhafte Überwachung und Erfassung von Daten und Inhalten der elektronischen Telekommunikation einschließlich rechtswidrigen Kooperation der in Deutschland tätigen Telekommunikationsunternehmen mit diesen Diensten.

2.) Antragsteller

Zu den Antragstellern im Einzelnen:

---

[13] Wissenschaftlicher Dienst des Deutschen Bundestages, Sachstandsbericht v. 18.03.2011, WD 7-3000-036/11, zitiert nach Stellungnahme des Deutschen Anwaltvereins durch die Ausschüsse Gefahrenabwehrrecht, Informationsrecht und Strafrecht zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz für ein Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (Stand: 15.05.2015)

[14] Vgl. Gutachten Max-Planck-Institut (zweite erweiterte Fassung) Juli 2011, S. 218, abrufbar unter: https://www.mpg.de/5000721/vorratsdatenspeicherung.pdf, zuletzt abgerufen am 3.11.2015.

[15] Stellungnahme des Deutschen Anwaltvereins durch die Ausschüsse Gefahrenabwehrrecht, Informationsrecht und Strafrecht zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz für ein Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (Stand: 15.05.2015), Seite 11.

Den Antrag auf Erlass einer einstweiligen Androhung stellen die Antragsteller zu 1. bis 3. als Rechtsanwälte und Partner der Kanzlei MMR Müller Müller Rößner Rechtsanwälte Partnerschaft in eigenem Namen und aus eigener Rechtsbetroffenheit. Die übrigen Antragsteller haben den Rechtsanwälten Carl Christian Müller sowie Sören Rößner, in Sozietät MMR Müller Müller Rößner Rechtsanwälte Partnerschaft, Vollmacht erteilt und diese mit der Wahrnehmung ihrer rechtlichen Interessen beauftragt.

a) Antragsteller 1. bis 3.

Die Antragsteller zu 1., 2. und 3. sind Rechtsanwälte in Sozietät MMR Müller Müller Rößner Rechtsanwälte Partnerschaft mit Sitz in Berlin. Für die Sozietät ist ein Festnetzanschluss angemeldet. Die Kommunikation der Antragsteller wird hierüber in Form von Telefonaten, Faxen und E-Mails geführt. Jeder der Antragsteller verfügt über eine eigene E-Mailadresse sowie eine gemeinsam genutzte E-Mail-Adresse. Zudem hat jeder Rechtsanwalt einen eigenen Mobilfunk-Telefonvertrag abgeschlossen. Die Mobiltelefone werden sowohl privat wie auch vornehmlich beruflich genutzt. In ihrer Eigenschaft als Rechtsanwälte sind die Antragsteller von der verdachts- und anlasslosen Vorratsspeicherung von Telekommunikations- und Standortdaten insbesondere mit Blick auf das Mandatsgeheimnis als selbständige Rechtsanwälte und Strafverteidiger betroffen.

b) Antragsteller zu 4. bis 7.

Bei dem Antragsteller zu 4. handelt es sich um den Deutschen Medienverband e. V. (DMV), der als Journalistenverband überwiegend freie Journalisten vertritt. Er wurde 1990 gegründet und besitzt damit eine über zwei Jahrzehnte gewachsene medienspezifische Kompetenz. Seine Mitglieder arbeiten in den unterschiedlichsten Mediengattungen und eint das Bekenntnis zur Qualität im Journalismus. Der Antragsteller verfügt über die üblichen Telekommunikationsmittel (Telefon, Fax, Internet, E-Mail), über die er mit seinen Mitgliedern und anderen korrespondiert. Der Verband bietet für seine Mitglieder Rechtsberatungen an, die die Antragsteller zu 1.) und 2.) für den Antragsteller zu 4.) leisten. Hierbei wenden sich Mitglieder auch an den Verband, um kritische Berichte oder Verdachtsberichterstattung auf deren Zulässigkeit hin überprüfen zu lassen. Da der Verband im gesamten Bundesgebiet über Mitglieder verfügt, kann und muss dies unter Zuhilfenahme von Telekommunikationsmitteln geschehen. Insofern ist

hier der Informanten- und Quellenschutz von der verdachts- und anlasslosen Vorratsspeicherung von Telekommunikationsverbindungsdaten betroffen.

Der Antragsteller zu 5. ist Bundespräsidiumsvorsitzender des Deutschen Medienverbandes und führt auch in dem vorangestellten Rahmen Korrespondenz mit den Mitgliedern des vom ihm geführten Verbandes.

Bei dem Antragsteller zu 6. handelt es sich um den DJV Deutschen Journalisten-Verband Landesverband Berlin-Brandenburg e.V., dessen satzungsgemäße Aufgabe darin besteht, alle beruflichen, rechtlichen und sozialen Interessen der hauptberuflich für Presse, Hörfunk, Fernsehen und andere Publikationsmittel beschäftigten Journalistinnen und Journalisten zu wahren und zu fördern. Der Antragsteller hält die üblichen Telekommunikationsmittel (Telefon, Fax, Internet, E-Mail) vor, über die u. a. der Antragsteller zu 7., der Vorsitzende des Antragstellers zu 6., der selbst auch als Journalist tätig ist, Kommunikation mit seinen Mitgliedern führt.

c) Antragsteller zu 8. bis 12.

Der Antragsteller zu 8. ist Filmproduzent und Inhaber der Filmproduktionsfirma TIME PRINTS KG. In dieser Tätigkeit produziert er Dokumentarfilme und journalistische Reportagen.

Die Antragstellerin zu 9. war zunächst für die Berliner Zeitung tätig und arbeitet nunmehr als Autorin und freie Journalistin.

Die Antragstellerin zu 10. ist Journalistin und war als solche von 1991 bis 2009 als freie Redakteurin und Autorin im öffentlich-rechtlichen wie privaten Rundfunk tätig, unter anderem bei der Kindernachrichtensendung „logo!“ des Zweiten Deutschen Fernsehens (ZDF). Sie ist seit 2009 Mitglied des Bundestages. Sie ist Sprecherin für Medienpolitik, Kreativwirtschaft und digitale Infrastruktur der Fraktion Bündnis 90/Die Grünen, Mitglied des Ausschusses für Kultur und Medien und stellvertretendes Mitglied im Ausschuss für Wirtschaft und Energie, im Ausschuss Digitale Agenda sowie im Ausschuss für Verkehr und digitale Infrastruktur.

Der Antragsteller zu 11. ist Fachredakteur für Energie im WDR Hörfunk und als solcher auch für den gesamten ARD-Hörfunk offizieller ARD-Energieexperte. In dieser Eigenschaft und als Mitglied des Story- und Recherchepools des WDR-Hörfunks arbeitet er

regelmäßig an investigativen Recherchen und ist auf Zuarbeit von Informanten angewiesen.

Der Antragsteller zu 12. war vormals Korrespondent im ARD-Hauptstadtstudio und arbeitet jetzt als freier Journalist mit einem Themenschwerpunkt zu bundespolitischen Themen. Er ist Mitglied der Bundespressekonferenz.

Bei den Antragstellern ist hier der Informanten- und Quellenschutz von der verdachts- und anlasslosen Vorratsspeicherung von Telekommunikationsverbindungsdaten betroffen. Die Antragstellerin zu 10 ist zudem als Abgeordnete im Rahmen ihrer Tätigkeit als Abgeordnete betroffen, insbesondere mit Blick auf das Vertrauensverhältnis zu den Bürgerinnen und Bürgern.

d) Antragsteller zu 13.

Der Antragsteller zu 13 arbeitet seit zehn Jahren als niedergelassener Kinderarzt und Kinderkardiologe in Göttingen. Er kommuniziert täglich mit den Eltern seiner Patienten über eine https gesicherte Website bzw. Cloud (www.befundnet.de) und teilt hierüber den Eltern die Ergebnisse der Untersuchungsbefunde ihrer Kinder mit. Er sieht sich insofern durch die anlasslose Vorratsdatenspeicherung in erheblichem Maße betroffen.

e) Antragsteller zu 14. bis 22.

Der Antragsteller zu 14. ist seit 2006 Mitglied des Abgeordnetenhauses von Berlin und als solcher seit 2012 parlamentarischer Geschäftsführer der Fraktion Bündnis 90/Die Grünen im Abgeordnetenhaus von Berlin. Zudem ist er seit 2012 als Rechtsanwalt zugelassen und in dieser Funktion als Strafverteidiger tätig.

Die Antragstellerin zu 15. ist seit 2006 Mitglied des Abgeordnetenhauses von Berlin und ebenfalls Mitglied der Fraktion Bündnis 90/Die Grünen. Sie ist zudem als Rechtsanwältin tätig.

Der Antragsteller zu 16. ist seit 2011 Mitglied des Abgeordnetenhauses von Berlin und als solcher Fraktionär von Bündnis 90/Die Grünen. Er ist zudem als Rechtsanwalt tätig.

Der Antragsteller zu 17. ist seit 2006 Mitglied des Abgeordnetenhauses von Berlin. Er ist ebenfalls Mitglied Fraktion Bündnis 90/ Die Grünen. Außerdem ist er Richter.

Die Antragstellerin zu 18. ist seit 2001 Mitglied des Berliner Abgeordnetenhauses und seit 2009 Fraktionsvorsitzende der Fraktion Bündnis 90/Die Grünen im Abgeordnetenhaus von Berlin.

Der Antragsteller zu 19. ist seit 2011 Mitglied des Abgeordnetenhauses von Berlin und als solches Mitglied der SPD-Fraktion.

Der Antragsteller zu 20. ist seit 2006 Mitglied des Abgeordnetenhauses von Berlin und ebenfalls Mitglied der SPD-Fraktion. Er ist zu dem als Rechtsanwalt tätig.

Die Antragsteller zu 21 und 22. sind seit 2011 Mitglied des Abgeordnetenhauses von Berlin und als solche Mitglieder der PIRATEN-Fraktion.

Die unter 14. bis 22. genannten Antragsteller nutzen in ihrer beruflichen Eigenschaft als Abgeordnete und – soweit sie als Rechtsanwälte zugelassen sind – auch als solche alle denkbaren Telekommunikationsmittel, insbesondere Telefon, Mobilfunk, E-Mail, Fax, SMS oder sonstige Telekommunikationsdienste zur Kontaktaufnahme und Kommunikation mit Bürgerinnen und Bürgern sowie mit Mandanten.

Von der verdachts- und anlasslosen Vorratsspeicherung von Telekommunikations- und Standortdaten ist das Vertrauensverhältnis zwischen den Antragstellern zu 14. bis 22. als Abgeordnete und den Bürgerinnen und Bürgern betroffen. Zudem ist, sofern die Antragsteller Rechtsanwälte sind, auch das Mandatsgeheimnis hiervon berührt.

II. Vorbedingungen für den Erlass einer einstweiligen Anordnung

Gemäß § 32 Abs. 1 BVerfGG kann das Bundesverfassungsgericht im Streitfall einen Zustand durch einstweilige Anordnung vorläufig regeln, wenn dies zur Abwehr schwerer Nachteile, zur Verhinderung drohender Gewalt oder aus einem anderen wichtigen Grund zum gemeinen Wohl dringend geboten ist. Dabei haben die Gründe, die für die Verfassungswidrigkeit des angegriffenen Hoheitsakts vorgetragen werden, grundsätzlich außer Betracht zu bleiben, es sei denn, die Verfassungsbeschwerde erwiese sich von vornherein als unzulässig oder offensichtlich unbegründet.[16] Dies ist hier nicht der Fall.

[16] BVerfG, Beschl. v. 11.3.2008 – 1 BvR 256/08; vgl. auch BVerfG, Beschl. v. 22.3.2005 – 1 BvR 2357/04, 1 BvQ 2/05.

1.) Zulässigkeit der Verfassungsbeschwerde

Die Verfassungsbeschwerde ist zulässig.

a) Keine Normen, die zwingendes Unionsrecht umsetzen

Insbesondere richtet sich die Verfassungsbeschwerde nicht gegen Normen, die zwingendes Recht der Europäischen Union umsetzen. Seit dem Urteil des Gerichtshofs der Europäischen Union vom 08.04.2014,[17] durch das die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15.03.2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (ABl L 105 vom 13.04.2006, S. 54; im Folgenden: Richtlinie 2006/24/EG), deren Umsetzung die Vorgängerregelungen der angegriffenen Normen diente, für ungültig erklärt wurde, steht deren umfassender Prüfung durch das Bundesverfassungsgericht am Maßstab der deutschen Grundrechte von vornherein nichts im Wege.

b) Rüge von (Unions-)Grundrechten

Die Verfassungsbeschwerde ist auch im Übrigen zulässig.

Die Antragsteller rügen zulässigerweise eine Verletzung von Art. 10 Abs. 1 GG, Art. 3 Abs. 1, Art. 5 Abs. 1, Art. 12 Abs. 1 GG sowie Art. 7, Art. 8, Art. 11, Art. 15 und Art. 20 der Charta der Grundrechte der Europäischen Union. Sie nutzen als Rechtsanwälte, Ärzte, Journalisten und Mitglieder des Deutschen Bundestages sowie des Abgeordnetenhauses von Berlin privat und dienstlich bzw. geschäftlich verschiedene Telekommunikationsdienste wie insbesondere Telefondienste und Internet, und machen geltend, durch die Speicherung ihrer Verbindungsdaten vor allem in ihrem Grundrecht auf Wahrung des Telekommunikationsgeheimnisses, auf Pressefreiheit, freie Meinungsäußerung und ihrer Berufsfreiheit verletzt zu sein. Da insbesondere Art 10 Abs. 1 GG auch die Vertraulichkeit der Umstände von Telekommunikationsvor-

[17] EuGH, Urt. v. 8.4.2014 – C 293/12 und C 594/12.

gängen schützt,[18] ist eine solche Verletzung durch die angegriffenen Vorschriften möglich. Selbiges gilt für das in Art. 7 der Charta verankerte Recht auf Privatleben und das in Art. 8 der Charta verankerte Recht auf Schutz personenbezogener Daten. Darüber hinaus rügen die Antragsteller als Berufsgeheimnisträger insbesondere eine Verletzung des Gleichheitssatzes gemäß Art. 3 Abs. 1 GG und Art. 20 der Charta, soweit sie nicht – anders als die Anschlüsse der sozialen und kirchlichen Telefonberatung – von der umfassenden Speicherpflicht ausgenommen werden.

c) Antragsteller selbst, gegenwärtig und unmittelbar betroffen

Nach der Rechtsprechung des Bundesverfassungsgerichts ist Zulässigkeitsvoraussetzung, dass der Antragsteller durch die angegriffene Norm selbst, gegenwärtig und unmittelbar in einem Grundrecht betroffen ist.[19]

Gemäß dem in § 90 Abs. 2 Satz 1 BVerfGG zum Ausdruck kommenden allgemeinen Grundsatz der Subsidiarität der Verfassungsbeschwerde ist die Verfassungsbeschwerde unzulässig, soweit der Antragsteller vor Anrufung des Bundesverfassungsgerichts in zumutbarer Weise Rechtsschutz durch die allgemein zuständigen Gerichte erlangen kann.[20] Damit solle neben der Entlastung des Bundesverfassungsgerichts erreicht werden, dass das Bundesverfassungsgericht nicht auf ungesicherter Tatsachen- und Rechtsgrundlage entscheiden muss[21]. Die Verpflichtung, vor einer Anrufung des Bundesverfassungsgerichts Rechtsschutz vor den Fachgerichten zu suchen, bestehe jedoch nicht, wenn der mit dem Subsidiaritätsgrundsatz verfolgte Zweck, eine fachgerichtliche Vorklärung der verfassungsrechtlich relevanten Sach- und Rechtsfragen herbeizuführen, nicht erreicht werden kann[22]. Dies sei auch der Fall, wenn die Frage der Verfassungsmäßigkeit der angegriffenen Norm allein von der Beurteilung verfassungsrechtlicher Fragen abhängt[23]. Das Bundesverfassungsgericht habe im Einzelfall die für und wider eine Entscheidung vor Erschöpfung des Rechtswegs sprechenden Umstände

---

[18] BVerfG, Urt. v. 2.3.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08; vgl. auch BVerfG, Beschl. v. 20.6.1984 – 1 BvR 1494/78; BVerfG, Beschl. v. 25.3.1992 – 1 BvR 1430/88; BVerfG, Urt. v. 27.2.2008 – 1 BvR 370/07.

[19] BVerfG, Beschl. v. 21.12.2004 - 2 BvR 2197/04; vgl. auch BVerfG, Urt. v. 19.7.2000 – 1 BvR 539/96; vgl. auch BVerfG, Beschl. v. 19.12.1951 – 1 BvR 220/51.

[20] Vgl. BVerfG, Beschl. v. 14.1.1998 – 1 BvR 1995/94; BVerfG, Urt. v. 19. 7.2000 – 1 BvR 539/96.

[21] Vgl. BVerfG, Beschl. v. 11.10.1988 – 1 BvR 777/85; BVerfG, Beschl. v. 14.1.1998 – 1 BvR 1995/94; BVerfG, Urt. v. 19.7.2000 – 1 BvR 539/96.

[22] Vgl. BVerfG, Beschl. v. 11.10.1988 – 1 BvR 777/85; BVerfG, Beschl. v. 9.3.1994 – 1 BvR 1369/90.

[23] Vgl. BVerfG, Beschl. v. 12.12.1984 – 1 BvR 1249/83.

pflichtgemäß gegeneinander abzuwägen.[24] Diese Abwägung muss hier auch in Anbetracht der Verpflichtung zur Wahrung des effektiven Vollzugs des Unionsrechts, wozu neben den hier betroffenen Unionsgrundrechten aus Art. 7, 8, 11, 15 und 20 der Charta insbesondere auch das in Art. 47 der Charta garantierte Recht auf effektiven Rechtsschutz gehört, zur Zulässigkeit der verfahrensgegenständlichen Verfassungsbeschwerde führen.

Die angegriffenen Vorschriften betreffen die Antragsteller unmittelbar, selbst und gegenwärtig. Zwar richtet sich die Speicherungspflicht des § 113b TKG nicht an die als Nutzer betroffenen Antragsteller, sondern an die Diensteanbieter. Jedoch sind diese ohne jeden Entscheidungsfreiraum[25] unbedingt zur Speicherung der Daten der Antragsteller verpflichtet. § 113b TKG führt damit unmittelbar und gegenwärtig zu einer Speicherung von Daten der Antragsteller für die in § 113c Abs. 1 TKG vorgesehenen Zwecke. Die Antragsteller werden durch das Gesetz somit bereits durch sein bloßes Inkrafttreten in ihren (Unions-)Grundrechten unmittelbar beeinträchtigt. Insbesondere stellt es von vornherein keinerlei zumutbare oder effektive Alternative dar, die Antragsteller darauf zu verweisen, vor den Fachgerichten gegen die Telekommunikationsunternehmen zu klagen.

Soweit vorgesehen ist, dass die Telekommunikationsanbieter die Speicherverpflichtung und die damit verbundenen Verpflichtungen spätestens ab dem am ersten Tag des 19. auf die Verkündung des Gesetzes folgenden Kalendermonats erfüllen müssen, ändert dies nichts daran, dass sämtliche Verpflichtungen – insbesondere § 113b TKG – bereits vom ersten Tag an gelten.

Denn die mit Inkrafttreten des Gesetzes einhergehende Speicherpflicht gilt unmittelbar und unbedingt. Soweit diesbezüglich eine Implementierungsphase vorgesehen ist, stellt deren Ende den spätestmöglichen Zeitpunkt der Erfüllung dieser Speicherpflicht durch die Telekommunikationsunternehmen dar. Gleichwohl gilt die Verpflichtung zur Speicherung vom ersten Tage an. Diese Verpflichtung korrespondiert zudem mit einer ebenfalls unmittelbar mit Inkrafttreten des Gesetzes einsetzenden Berechtigung zur Speicherung durch die Telekommunikationsunternehmen, die somit ab diesem Zeitpunkt ohne weiteres jederzeit mit der Speicherung beginnen müssen und können. Insbesondere müssen die Telekommunikationsunternehmen nicht abwarten, bis die Bun-

[24] Vgl. BVerfG, Beschl. v. 23.10.1958 – 1 BvR 458/58; BVerfG, Beschl. v. 23.7.1987 – 1 BvR 825/87.

[25] BVerfG, Urt. v. 2.3.2010 – 1 BvR 256/08; vgl. BVerfG, Urt. v. 12.3.2003 – 1 BvR 330/96.

desnetzagentur den Anforderungskatalog gemäß § 113f TKG veröffentlicht hat, da diese Vorschrift lediglich eine Vermutungsregel im Hinblick auf die Einhaltung des zu gewährleistenden Standards der Datensicherheit und Datenqualität darstellt. Die Antragsteller werden daher bereits ungeachtet der vorgesehenen Implementierungsphase durch das bloße Inkrafttreten des Gesetzes, nämlich dadurch beeinträchtigt, dass sie die Speicherung der Daten dann jederzeit zu gewärtigen haben.

Diese Implementierungsphase wurde vom Gesetzgeber im Übrigen mit denselben Erwägungen begründet, die ihn auch schon bei der Vorgängerregelung dazu veranlassten, die Anwendung der Bußgeldvorschriften hinsichtlich der Verletzung der Verpflichtungen seitens der Diensteanbieter ein Jahr aufzuschieben, nämlich um den Telekommunikationsunternehmen ausreichend Zeit für die Umsetzung zu geben.[26] Im verfahrensgegenständlichen Gesetz wurde lediglich eine andere gesetzestechnische Gestaltung gewählt. Soweit sich diese Gestaltung – dies sei nur der Vollständigkeit halber angemerkt – insofern von der Vorgängerregelung unterscheidet, als vorliegend anders als dort während der Umsetzungsphase auch die frühere Durchsetzung der Speicherpflicht mit Zwangsmitteln von vornherein nicht in Betracht kommt, sei nur auf die damalige Gegenäußerung der Bundesregierung im Gesetzgebungsverfahren verwiesen, wonach es sich bei § 115 TKG um eine Ermessensvorschrift handele und erforderlichenfalls das Bundesministerium für Wirtschaft und Technologie zu prüfen haben werde, ob der Erlass einer allgemeinen ermessensleitenden Verfügung, von der Befugnis zur Festsetzung von Zwangsgeldern nach § 115 TKG unter bestimmten Voraussetzungen einstweilen keinen Gebrauch zu machen, angezeigt ist.[27] Damit handelte es sich hierbei eher um eine theoretische Option, so dass auch dieser Aspekt vorliegend keinen maßgeblichen Unterschied darstellen kann.

Dennoch ist das Bundesverfassungsgericht in seinen Entscheidungen zur Vorgängerregelung[28] ohne weiteres von einer gegenwärtigen und unmittelbaren Betroffenheit der dortigen Antragsteller vom ersten Tag des Inkrafttretens des Gesetzes an ausgegangen.

Entsprechendes muss somit im vorliegenden Fall gelten.

---

[26] Vgl. BT-Drucks. 18/5088, Seite 44 sowie zur Vorgängerregelung BT-Drucks. 16/5846, Seite 74.

[27] BT-Drucks. 16/5846, Seite 97.

[28] BVerfG, Urt. v. 2.3.2010 – 1 BvR 256/08.

Schließlich ist vorliegend auch das Erfordernis der Unmittelbarkeit erfüllt. Eine unmittelbare Beschwerde gegen Rechtsnormen wie hier ist nur ausnahmsweise zulässig, und zwar dann, wenn es keines konkretisierenden Vollzugsaktes mehr bedarf und sich weder einfach-rechtliche noch tatsächliche Fragen stellen, sondern allein die Verfassungsmäßigkeit einer in ihrer Auslegung unzweifelhaften Rechtsnorm in Frage steht.[29] Auch dies ist vorliegend gegeben. Zweifelhaft ist – angesichts des eindeutigen und einer (verfassungskonformen wie auch unionsrechtskonformen) Auslegung nicht zugänglichen Wortlauts der angegriffenen Normen und der klar auf der Hand liegenden erheblichen Betroffenheit der Antragsteller – allein die verfassungsrechtliche Zulässigkeit der Einführung der Vorratsdatenspeicherung in der in dem angegriffenen Gesetz geregelten Form und damit die grundsätzliche Frage, ob die Antragsteller hierdurch in ihren (Unions-)Grundrechten verletzt sind.

Alternativ hierzu ist eine unmittelbare Verfassungsbeschwerde auch dann zulässig, wenn ein Abwarten für den Antragsteller unzumutbar ist. Hierzu ist anerkannt, dass Antragsteller nicht darauf verwiesen werden können, unnötige Vollzugsakte zu provozieren oder gar das Risiko eines Bußgeldes oder Strafverfahrens einzugehen.[30]

Ein Abwarten etwa bis zu dem Zeitpunkt, bis das erste Telekommunikationsunternehmen die vorgesehene Speicherpflicht konkret erfüllt, ist schon allein deswegen nicht zumutbar, weil dieser Zeitpunkt völlig unbestimmt ist, insoweit auch keine Verpflichtung zur öffentlichen Bekanntmachung besteht und somit für die Antragsteller gänzlich im Ungewissen liegt, wann die einzelnen verpflichteten Diensteanbieter konkret mit der Speicherung der Daten beginnen.

Es ist auch nicht ersichtlich, dass das Bundesverfassungsgericht in seinen Entscheidungen zur Vorgängerregelung (1 BvR 256/08) in einer insoweit vergleichbaren Konstellation darauf abgestellt hätte, ob in Erfüllung der gesetzlichen Verpflichtungen bereits Daten auf Vorrat gespeichert und Abrufe der gespeicherten Daten getätigt wurden.

d) Gebot effektiven Vollzugs des Unionsrechts und effektiven Rechtsschutzes

Käme man trotz der vorstehenden Darlegungen zu dem Ergebnis, die Zulässigkeit der vorliegenden Verfassungsbeschwerde zu verneinen, so versagte man dem von

---

[29] Vgl. Sperlich, in: Umbach,/Clemens/Dollinger, BVerfGG, 2. Aufl. 2005, § 90 Rn. 134.

[30] Vgl. BVerfG, Beschl. v. 25.10.1977 – 1 BvR 173/75; BVerfG, Beschl. v. 14.11.1989 – 1 BvL 14/85.

§ 93 Abs. 3 BVerfGG vorausgesetzten Institut der Rechtssatzverfassungsbeschwerde zumindest in Konstellationen wie der vorliegenden grundsätzlich die Anerkennung. Dies wäre weder mit dem Gebot des effektiven Vollzugs des Unionsrechts noch in Ansehung der ständigen Rechtsprechung des Bundesverfassungsgerichts mit dem Gebot effektiven Rechtsschutzes zu vereinbaren. Denn ansonsten wäre dem Gesetzgeber generell die Möglichkeit in die Hand gegeben, sich einer Rechtssatzverfassungsbeschwerde bei entsprechenden Vorhaben zu entziehen, indem er gesetzliche Regelungen sofort in Kraft setzt, gleichzeitig aber vorsieht, sie erst nach Ablauf der Jahresfrist zwingend anzuwenden und ihre Anwendung auch erst dann tatsächlich erfolgt.

2.) Begründetheit der Verfassungsbeschwerde

Die Verfassungsbeschwerde ist zudem nicht nur nicht offensichtlich unbegründet, sondern vielmehr sogar offensichtlich begründet. Dies gilt nicht zuletzt mit Blick auf die Entscheidung des Gerichtshofs der Europäischen Union vom 08.04.2014.[31]

a) Vorgaben des Bundesverfassungsgerichts nicht erfüllt

Soweit das Bundesverfassungsgericht in seiner Entscheidung vom 02.03.2010 eine sechsmonatige, vorsorglich anlasslose Speicherung von Telekommunikationsverkehrsdaten durch private Diensteanbieter unter sehr engen Voraussetzungen als mit Art. 10 GG nicht schlechthin unvereinbar angesehen hat,[32] sind zum einen wesentliche dieser und anderer verfassungsrechtlicher Vorgaben nicht oder nicht hinreichend erfüllt.

(a) Speicherung von SMS-Inhalten

Dies gilt etwa für die mit der Umsetzung der durch die angegriffenen Normen angeordneten Speicherpflicht von Seiten der Telekommunikationsanbieter zu besorgende offenbar technisch bedingte Vorratsspeicherung von SMS-Inhalten und damit von Kommunikationsinhalten, die nach der Rechtsprechung des Senats von vornherein offensichtlich verfassungswidrig ist.[33] Auch nach der Rechtsprechung des Europäischen Gerichtshofs stellt eine Vorratsspeicherung des Inhalts elektronischer Kommunikation

---

[31] EuGH, Urt. v. 8.4.2014 – C 293/12 und C 594/12.

[32] BVerfG, Urt. v. 2.3.2010 – 1 BvR 256/08, Rz. 209.

[33] Vgl. BVerfG, Urt. v. 2.3.2010 – 1 BvR 256/08, Rz. 218.

nicht nur einen besonders schwerwiegenden Eingriff in das Grundrecht auf Achtung des Privatlebens und die übrigen in Art. 7 der Charta verankerten Rechte dar, sondern wäre geeignet, deren Wesensgehalt anzutasten, und damit ein Verstoß gegen Unionsrecht bzw. eine Verletzung von Unionsgrundrechten.[34] Bereits mit Blick auf diesen Aspekt ist die Zuverlässigkeit und Geeignetheit der Diensteanbieter, die Wahrung der Grundrechte der Nutzer der Dienste zu gewährleisten, was eine wesentliche Erwägung des Senats in Bezug auf die von ihm vorgegebene dezentrale Speicherung der Daten war, als höchst fraglich anzusehen.

(b) Richtervorbehalt

Selbiges gilt für den im angegriffenen Gesetz vorgesehenen Richtervorbehalt. Dieser entspricht nicht den Vorgaben des Bundesverfassungsgerichts zu der in diesen Fällen erforderlichen Ausgestaltung, wonach die Effektivität des Richtervorbehalts durch eine entsprechend hinreichende Justizorganisation zu sichern ist.[35] Gerade in Anbetracht der seither gewonnenen tatsächlichen Erkenntnisse über die Anwendung des Richtervorbehalts in der Praxis (siehe unten) wäre es von Seiten des Gesetzgebers geboten gewesen, entsprechende Vorkehrungen zu treffen, um die Wahrung der Grundrechte der betroffenen Nutzer effektiv zu gewährleisten und die entsprechende Maßgabe des Bundesverfassungsgerichts zu erfüllen.[36]

Denn selbst das Bundesverfassungsgericht äußert Zweifel, ob der Richtervorbehalt ein geeignetes Kontrollinstrument ist. Mit Urteil vom 20.02.2001 führt es hierzu aus:

> *„In der Literatur werden die Neigung zu exzessiver und zum Teil missbräuchlicher Anwendung der Eilkompetenz durch die Strafverfolgungsbehörden, insbesondere durch die Polizei beklagt (vgl. etwa Nelles, Kompetenzen und Ausnahmekompetenzen in der Strafprozessordnung, 1980, S. 247 f.; Schäfer in: Löwe-Rosenberg, StPO, 24. Aufl., § 98, Rn. 35; Schnäbele in: Gefahr im Verzug, Tagung der Neuen Richtervereinigung, 1989, S. 12; Dubbers, ebenda, S. 36 f.; Werkentin, ebenda, S. 26) und die Mangelhaftigkeit der richterlichen Kontrolle beanstandet. Die Mängel werden unter anderem darauf zurückgeführt, dass der Ermittlungsrichter, auch aus Gründen unzureichender personeller Ausstattung der Amtsgerichte, unter zu starkem Zeitdruck*

[34] EuGH, Urt. v. 6.10.2015 – C-362/14, Safe Harbor, Rz. 94. EuGH, Urt. v. 8.4.2014 – C 293/12 und C 594/12, Rz. 39.

[35] BVerfG, Urt. v. 20.2.2001, 2 BvR 1444/00.

[36] vgl. BVerfG, Urt. v. 2.3.2010 – 1 BvR 256/08, Rz. 247 ff.

stehe, dass er gerade bei umfangreichen Verfahren keine vollständige Kenntnis des Sachstands erlangen könne und dass ihm oft das notwendige Fachwissen in Spezialgebieten fehle (vgl. etwa Lilie, ZStW 111 <1999>, S. 808, 817 f.; Asbrock, ZRP 1998, S. 17, 19; Geppert, DRiZ 1992, S. 405, 410; Müller, AnwBl 1992, S. 349, 351; Weber, DRiZ 1991, S. 116, 117).“[37]

Daher hat das Bundesverfassungsgericht die Vorgabe gemacht, die Effektivität des Richtervorbehalts durch eine entsprechend hinreichende Justizorganisation zu sichern. Es führt insofern aus:

„Diese Mängel können nicht allein durch den jeweils zuständigen Richter behoben werden. Seine verfassungsrechtlich begründete Pflicht, sich die notwendige Zeit für die Prüfung eines Durchsuchungsantrags zu nehmen und sich Kenntnis von der Sache sowie das erforderliche Fachwissen zu verschaffen, kann er nur bei einer entsprechenden Geschäftsverteilung, ausreichender personeller und sächlicher Ausstattung seines Gerichts, durch Aus- und Fortbildungsmöglichkeiten sowie vollständige Information seitens der Strafverfolgungsbehörden über den Sachstand erfüllen.“[38]

Zu einer wirksamen Kontrolle gehört die Kontrolle der Kontrolle. Mit anderen Worten muss die vom Bundesverfassungsgericht geforderte entsprechend hinreichende Justizorganisation Instrumente vorsehen, die eine entsprechende Kontrolle gewährleisten. Hierzu gehören neben einer ausreichenden personellen und sächlichen Ausstattung des Gerichts und Aus- und Fortbildungsmöglichkeiten der Richter auch statistische Erhebungen, deren Auswertungen Rückschlüsse auf die Effektivität des Kontrollinstruments „Richtervorbehalt“ zulassen.

Zwar ist nach § 101b Nr. 1 StPO eine statistische Erfassung der angeordneten Erhebungen von Verkehrsdaten vorgesehen, indem hierüber jährlich eine Übersicht zu erstellen ist. Diese Übersichten betreffen allerdings nur die Anzahl der Verfahren, in denen diese Maßnahmen nach § 100g Abs. 1, 2 und 3 StPO durchgeführt wurden, des Weiteren die Anzahl der Erstanordnungen, sowie die Anzahl der Verlängerungsanordnungen. Diese Angaben alleine sind jedoch nicht aussagekräftig. Es fehlt eine Übersicht zu der Anzahl der Anträge auf Anordnung entsprechender Erhebungen und – dies vor al-

[37] BVerfG, Urt. v. 20.2.2001, 2 BvR 1444/00, Rz. 29.

[38] BVerfG, a. a. O.

lem – eine Übersicht zu der Frage, wie oft den Anträgen entsprochen wurde und wie oft diese abgelehnt wurden. Denn die Frage, wie viele der Anträge auf Anordnung von Überwachungsmaßnahmen stattgegeben oder aber abgelehnt wurden, sagt auch etwas über die Wirksamkeit des Kontrollinstruments Richtervorbehalt aus. Denn auch ein Kontrollinstrument bedarf der Kontrolle, um sicherzustellen, dass es seine Funktion wirksam ausübt. Denn würde allen Anträgen auf Erhebung stattgegeben, stünde zu vermuten, dass eine effektive Kontrolle tatsächlich nicht stattfindet. In diesem Zusammenhang sei auf den Transparenzbericht des Berliner E-Mail-Providers Posteo verwiesen. Das Unternehmen hatte die Justizministerien der Länder um Auskunft gebeten, wie viele der beantragten Telekommunikations-Überwachungsmaßnahmen von Richtern negativ beschieden wurden. Dem Transparenzbericht zu Folge erfasst lediglich die Berliner Justiz die Anzahl der abgelehnten Anträge. Demnach wurden in Berlin zwischen 2008 und 2014 in Berlin 14.621 Anschlüsse überwacht, wobei die Anzahl der angeordneten Überwachungen über die Jahre hinweg deutlich anstieg. Kein einziger nach dem Jahr 2007 in Berlin gestellter Antrag auf Telekommunikationsüberwachung nach §§ 100a, 100b StPO wurde mehr abgelehnt.[39] Der Transparenzbericht führt hierzu aus:

> *„Dass zwischen 2008 und 2014 bei 14.621 überwachten Anschlüssen (Festnetz, Mobilfunk und Internet) in Berlin kein einziger Antrag auf Überwachung abgelehnt wurde, verdeutlicht unserer Auffassung nach eindrücklich, dass Zweifel an der Wirksamkeit des Kontrollinstrumentes des Richtervorbehaltes nicht nur berechtigt sind, sondern dass auch Klärungsbedarf besteht. Wie kann es möglich sein, dass Richter über viele Jahre hinweg jedem einzelnen Antrag auf Überwachung einer Bürgerin oder eines Bürgers stattgeben? Was sagen diese Zahlen über den Zustand unseres Rechtsstaates aus? Die Zahlen aus Berlin geben einen breiten Überblick über einen großen Zeitraum. Sie belegen unserer Auffassung nach deutlich, dass das Instrument seiner zugedachten Kontrollaufgabe dort tatsächlich schon lange nicht mehr mit ausreichender Qualität nachkommt und eine Debatte notwendig ist."*[40]

Das angegriffene Gesetz trifft insofern also keinerlei Vorkehrungen im Hinblick auf eine entsprechend Organisation der Justiz, die die Wahrung der Grundrechte gewährleisten können. Dies wäre jedoch zwingend erforderlich gewesen, um den hohen verfassungsrechtlichen Vorgaben in diesem Zusammenhang gerecht zu werden. Der Gesetzgeber

---

[39] http://pardok.parlament-berlin.de/starweb/adis/citat/VT/17/DruckSachen/d17-2401.pdf, zuletzt abgerufen am 4.11.2015.

[40] Posteo, Transparenzbericht 2014, a.a.O., Seite 18, f.

verkennt in diesem Zusammenhang, dass der bestehende Rahmen wie dargelegt ganz offensichtlich nicht ausreicht, die Grundrechtsträger trotz des mit der angeordneten Massenspeicherung verbundenen drastisch höheren personellen und sachlichen Aufwands hinreichend vor Rechtsverletzungen zu schützen. Somit kommt weder dem vom Gesetz vorgesehenen Richtervorbehalt ohne entsprechende Justizorgansiation eine Wächterfunktion zu, die die Schwere der mit der Datenspeicherung verbundenen Grundrechtseingriffe hinreichend kompensieren könnte. Damit entspricht der in dem mit der Verfassungsbeschwerde angegriffenen Gesetz vorgesehene Richtervorbehalt nicht den Vorgaben des Bundesverfassungsgerichts zu der in diesen Fällen erforderlichen Ausgestaltung, wonach die Effektivität des Richtervorbehalts durch eine entsprechend hinreichende Justizorganisation zu sichern ist.[41] Es fehlt schlicht an einer Kontrolle der Kontrolle.

b) Neue Erkenntnisse und Vorgänge:
Snowden-Enthüllungen, NSA-Affäre und Redtube-Skandal

Zum anderen greift die Verfassungsbeschwerde sowohl die erheblichen Erkenntnisse und Vorgänge tatsächlicher Art, die seit der Entscheidung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung vom 02.03.2010 an die Öffentlichkeit gelangt sind bzw. stattgefunden haben, als auch die maßgeblichen rechtlichen Entwicklungen, die sich seither vollzogen haben, auf. Schon allein diese im Rahmen der verfassungsrechtlichen Prüfung maßgeblich zu berücksichtigenden Aspekte stellen Anlass genug dar, die Verfassungsmäßigkeit einer solchen anlasslosen Vorratsspeicherung von Daten jedenfalls in der vom angegriffenen Gesetz konkret vorgesehenen Form mit weitergehenden Erwägungen zu hinterfragen und die entsprechenden Normen mit der Verfassungsbeschwerde anzugreifen.

Dies gilt etwa in Bezug auf die Enthüllungen durch Herrn Edward Snowden in Bezug auf das Agieren nationaler und internationaler Nachrichtendienste auch in Deutschland, was auch bereits Niederschlag in der Rechtsprechung des Gerichtshofs der Europäischen Union gefunden hat,[42] wie auch die rechtswidrige Kooperation der Telekommunikationsunternehmen mit diesen Diensten. In Anbetracht der von Herrn Snowden enthüllten Überwachungstätigkeiten von Nachrichtendiensten und anderen Behörden insbesondere der USA, die im Rahmen der von ihnen praktizierten massenhaften und

[41] BVerfG, Urt. v. 20.2.2001, 2 BvR 1444/00.

[42] EuGH, Urt. v. 6.10.2015 – C-362/14, Safe Harbor.

wahllosen Überwachung und Erfassung weltweit, in der Europäischen Union und auch in der Bundesrepublik Deutschland auf Daten und Inhalte der elektronischen Kommunikation zugreifen, ohne dass die betroffenen Grundrechtsträger insoweit einen wirksamen Anspruch auf rechtliches Gehör haben oder in irgendeiner Form benachrichtigt werden, und deren Zugriff auf die aufgrund der vorgeschriebenen Vorratsspeicherung gespeicherten Daten der elektronischen Kommunikation nicht ausgeschlossen werden kann, ist in keiner Weise ersichtlich, wie dies etwa mit der Vorgabe des Bundesverfassungsgerichts, dass der Staat insbesondere keinen direkten Zugriff auf die Daten haben darf, was durch entsprechende Regelungen und technische Vorkehrungen sicherzustellen ist.[43]

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit stellt zur NSA-Affäre fest: [44]

> *„Dass es sich hierbei um ein realistisches Szenario handelt, belegt auch die aktuelle Diskussion zum Thema „NSA", in der unzweifelhaft offen gelegt wurde, dass eine umfassende Überwachung des Internetverkehrs für Nachrichtendienste heute nicht nur kein Problem mehr darstellt, sondern auch tatsächlich praktiziert wird."*

Graulich führt hierzu aus:[45]

> *„Der in einer anlasslosen Speicherung von Telekommunikationsverkehrsdaten liegende Eingriff ist nach dem Bundesverfassungsgericht nur dann verhältnismäßig i.e.S., wenn er besonderen Anforderungen an die Datensicherheit, an den Umfang der Datenverwendung, an die Transparenz und an den Rechtsschutz genügt. Die katastrophalen Erkenntnisse über die Ausspähung von Datenbeständen durch ausländische Nachrichtendienste sowie nichtstaatliche Hacker begründen Zweifel, ob die nunmehr durch Gesetz unternommene Anlegung einer riesigen Menge von Telekommunikationsdaten überhaupt wirksam vor unbefugten Zugriffen geschützt werden können."*

---

[43] BVerfG, Urt. v. 2.3.2010, 1 BvR 256/08, Rz. 214.

[44] Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten v. 9.6.2015, S. 8.

[45] Vgl. Graulich, vorgänge Nr. 209 (Heft 1/2015), S. 85-98.

Im Zusammenhang mit der Tätigkeit der Nachrichtendienste hat etwa auch der irische High Court festgestellt, dass der massenhafte und undifferenzierte Zugriff auf personenbezogene Daten offenkundig gegen den Grundsatz der Verhältnismäßigkeit und die durch die irische Verfassung geschützten Grundwerte verstoße.[46]

Ebenso sind hier weitere Erkenntnisse über den höchst fragwürdigen Umgang gerade auch von deutschen Telekommunikationsunternehmen mit den grundrechtsrelevanten Daten ihrer Kunden im Inland sowie über die Anwendung des Richtervorbehalts in der Praxis, wie sie sich insbesondere im Zuge eines als skandalös zu bezeichnenden Vorgangs im Jahre 2013/2014 in Bezug auf das Portal Redtube darstellte, zu nennen.[47]

c) Neue rechtliche Entwicklungen: Weitere anlasslose Datensammlungen

Darüber hinaus sind auch die zwischenzeitlichen rechtlichen Entwicklungen insbesondere in Form anderer und weiterer vorsorglich anlassloser Datensammlungen über den Weg der Europäischen Union bzw. auf internationaler Ebene zu berücksichtigen. Auch insoweit erweist sich die Verfassungsbeschwerde mit Blick auf die Vorgaben des Bundesverfassungsgerichts aus dem Urteil vom 02.03.2010 als offensichtlich begründet. So dürfte angesichts diverser umgesetzter oder geplanter Datensammlungsvorhaben (Speicherung von Fluggastdaten, Zahlungsverkehrsdaten etc.) wie auch der oben genannten rechtswidrigen Tätigkeit von Nachrichtendiensten in Deutschland der Spielraum des Gesetzgebers heute mit Blick auf die Einführung einer Vorratsspeicherung von Telekommunikationsverkehrsdaten im Zuge der vorzunehmenden Überwachungsgesamtrechnung[48] jedenfalls erheblich weiter eingeschränkt sein, als dies bereits im Jahre 2010 der Fall war.[49] Dabei spricht – nicht zuletzt in Verbindung mit den infolge der Snowden-Enthüllungen bekannt gewordenen Tätigkeiten von Nachrichtendiensten in Deutschland, allen voran der National Security Agency (NSA) der USA, und deren Kooperation mit Telekommunikationsunternehmen – viel dafür, dass sich diese Rechnung entscheidend dahingehend verändert hat, dass der Spielraum des Gesetzgebers im Ergebnis auf Null reduziert ist.

---

[46] EuGH, Urt. v. 6.10.2015 – C-362/14, Rz. 33, Safe Harbor.

[47] Vgl. hierzu ausführlich Müller/Rößner, K&R 2014, S. 136; Müller, Abmahnwelle gegen Redtube-Nutzer: Vom Leerlaufen des Richtervorbehalts. In: Legal Tribune Online, 12.12.2013, abrufbar unter: http://www.lto.de/persistent/a_id/10344/

[48] Bezeichnung nach Roßnagel in NJW 2010, 1238 ff.

[49] BVerfG, Urt. v. 2.3.2010, 1 BvR 256/08, Rz. 218.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit stellt in diesem Zusammenhang zutreffend fest: [50]

„So wird im Entwurf nicht berücksichtigt, dass das BVerfG für „die verfassungsrechtliche Unbedenklichkeit einer vorsorglich anlasslosen Speicherung der Telekommunikationsverkehrsdaten […] voraus[setzt], dass diese eine Ausnahme bleibt" und „sie […] auch nicht im Zusammenspiel mit anderen vorhandenen Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger führen [darf]" (BVerfG, NJW 2010, S. 833 (839), Absatz Nr. 218). Diese „Überwachungs-Gesamtrechnung" (Bezeichnung nach Roßnagel in NJW 2010, S. 1238 ff.) wird jedenfalls im Bereich der Überwachung der Internetnutzung außer Acht gelassen. Aufgrund der weitreichenden Verpflichtung zur Speicherung von IP-Adressen (siehe III.1.a) unten) wird bereits nur aufgrund der Vorgaben des vorliegenden Gesetzentwurfes ein äußerst umfangreicher Datenpool geschaffen."

Daneben wurden in den letzten Jahren in immer mehr Gesetzen die Rechtsgrundlagen zur Speicherung und Verarbeitung von IP-Adressen erweitert. Insbesondere im Bereich der Sicherheitsbehörden gibt es z.B. im Bundesverfassungsschutzgesetz weitreichende Zugriffsmöglichkeiten auf entsprechende Daten. Ebenfalls erlaubt etwa § 7 Absatz 4 BKAG die Auskunft über den Inhaber einer IP-Adresse. Die Vorschrift ist nur an die unbestimmte Voraussetzung geknüpft, dass dies für die „Zentralstellenfunktion" des Bundeskriminalamtes erforderlich sein muss. Mit dem sich aktuell in der parlamentarischen Debatte befindlichen „Entwurfs eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)" werden den TK-Anbietern weitere Verwendungs- und in diesem Zusammenhang auch indirekt längere Speichermöglichkeiten eingeräumt.

Dabei sind die IP-Adressen nicht nur als Verkehrsdaten im Sinne des TKG, sondern auch als Nutzungsdaten im Sinne des Telemediengesetzes betroffen. Gerade letztere vermitteln aber detaillierte Informationen über die im Internet genutzten Inhalte. Anhand der bei den Telemediendiensten erhobenen Nutzungsdaten können Sicherheitsbehörden im Zusammenspiel mit der Zuordnungsmöglichkeit der IP-Adressen der Vorratsdatenspeicherung (…) somit zumindest über mehrere Wochen das Surfverhalten der Internetnutzer äußerst detailliert überwachen. Dass es sich hierbei

[50] Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten v. 9.6.2015, S. 7 f.

um ein realistisches Szenario handelt, belegt auch die aktuelle Diskussion zum Thema „NSA", in der unzweifelhaft offen gelegt wurde, dass eine umfassende Überwachung des Internetverkehrs für Nachrichtendienste heute nicht nur kein Problem mehr darstellt, sondern auch tatsächlich praktiziert wird. Durch die in § 113c Absatz 1 Nummer 3 TKG-E geschaffene Verknüpfung mit § 113 TKG können diese auch die in den Vorratsdaten gespeicherten IP-Adressen zumindest mittelbar nutzen (...) unten)."

d) Zwingende Vorgaben des EuGH nicht erfüllt

Schließlich ist die Verfassungsbeschwerde auch in Ansehung der Rechtsprechung des Gerichtshofs der Europäischen Union offensichtlich begründet.

(a) Gesetzgeber an Grundrechtecharta gebunden

Denn bei der verfassungsrechtlichen Beurteilung der angegriffenen Normen sind neben den Vorgaben des Grundgesetzes auch die Vorgaben der Grundrechtecharta, wie sie der Gerichtshof der Europäischen Union in seinem Urteil vom 08.04.2014 zur Richtlinie 2006/24/EG präzisiert hat, zu beachten, worauf der Gesetzgeber – freilich ohne diese Vorgaben zu erfüllen – selbst zutreffend hinweist:

„Nach Artikel 51 Absatz 1 der Grundrechtecharta sind die Mitgliedstaaten bei der Durchführung des Rechts der Union an die Grundrechtecharta gebunden. Das ist der Fall, wenn eine nationale Regelung in den Anwendungsbereich des Unionsrechts fällt. Die grundsätzliche Anwendbarkeit der Grundrechtecharta für nationale Regelungen zur Vorratsdatenspeicherung folgt aus 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): Nachdem der Gerichtshof der Europäischen Union die Richtlinie 2006/24/EG für ungültig erklärt hat, ist für nationale Regelungen zur Speicherung von Telekommunikationsdaten der Anwendungsbereich des Artikels 15 Absatz 1 der Richtlinie 2002/58/EG wieder eröffnet. Danach sind nationale Regelungen zur Vorratsdatenspeicherung zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten zulässig, wenn sie den Anforderungen des Artikels 6 Absatz 1 und 2 des Vertrags über die Europäische Union genügen. Aus Artikel 15 Absatz 1 folgt demnach die Bindung etwaiger nationaler Regelungen an die Charta. Darüber hinaus bewirkt die Anwendbarkeit des Ar-

tikels 15, dass nationale Regelungen in den Geltungsbereich des Unionsrechts fallen."[51]

(b) Nichtigkeit unionsrechtswidriger Normen

Dies wird auch bestätigt durch die ständige Rechtsprechung des Europäischen Gerichtshofs zu der Frage, welche Konsequenzen das nationale Gericht aus einem Widerspruch zwischen Bestimmungen seines innerstaatlichen Rechts und den durch die Grundrechtecharta verbürgten Rechten zu ziehen hat. Danach ist das nationale Gericht, das im Rahmen seiner Zuständigkeit die Bestimmungen des Unionsrechts anzuwenden hat, gehalten, für die volle Wirksamkeit dieser Normen Sorge zu tragen, indem es erforderlichenfalls jede – auch spätere – entgegenstehende Bestimmung des nationalen Rechts aus eigener Entscheidungsbefugnis unangewandt lässt, ohne dass es die vorherige Beseitigung dieser Bestimmung auf gesetzgeberischem Wege oder durch irgendein anderes verfassungsrechtliches Verfahren beantragen oder abwarten müsste.[52] Handelt es sich bei dem zur Entscheidung berufenen nationalen Gericht wie hier um ein Verfassungsgericht mit Normverwerfungskompetenz, das in einem Verfassungsbeschwerdeverfahren zu entscheiden hat, muss dies zwingend zur Nichtigerklärung der angegriffenen dem Unionsrecht entgegenstehenden und die Unionsgrundrechte verletzenden nationalen Normen und – in einem Verfassungsbeschwerdeverfahren wie hier – mithin zum Erfolg der Verfassungsbeschwerde führen.

(c) Keine Beschränkung auf das absolut Notwendige – insbesondere keine umfassende Ausnahme von Berufsgeheimnisträgern

Nach der somit hier maßgeblichen Entscheidung des Europäischen Gerichtshofs ist die Speicherpflicht auf das absolut Notwendige zu beschränken.[53] Gegen diese Grundbedingung wird verstoßen, wenn ausnahmslos (Speicherung sämtlicher Verkehrsdaten al-

---

[51] Vgl. BT-Drucks 18/5088. S. 22 f.

[52] EuGH, Urt. v. 26.2.2013 – C-617/10 mit Hinweis auf EuGH, Urteile vom 9.3.1978, Simmenthal, 106/77, Slg. 1978, 629, Rn. 21 und 24, vom 19.11.2009, Filipiak, C-314/08, Slg. 2009, I-11049, Rn. 81, sowie vom 22.6.2010, Melki und Abdeli, C-188/10 und C-189/10, Slg. 2010, I-5667, Rn. 43.

[53] EuGH, Urt. v. 8.4.2014 – C 293/12 und C 594/12, Rz. 58 f.

ler Kommunikationsmittel in Bezug auf alle Personen), anlasslos (keine auch nur mittelbare Veranlassung durch die betroffenen Personen) und zusammenhanglos (kein auch nur mittelbarer oder entfernter Bezug zwischen Datenspeicherung und der Bekämpfung schwerer Straftaten) gespeichert wird.[54] In diesem Falle liegt ein unverhältnismäßiger Eingriff in Art. 7 (Recht auf Privatheit) und Art. 8 (Schutz personenbezogener Daten) der EU-Grundrechtecharta vor.[55]

Nach dem angegriffenen Gesetz soll die Speicherung weiterhin anlass- und zusammenhanglos erfolgen. Ein irgendwie gearteter Bezug zwischen betroffenen Personen und Daten einerseits und der Bekämpfung schwerer Straftaten bzw. der Abwehr von Gefahren andererseits wird nicht verlangt. Lediglich ein Kommunikationsmittel – nämlich die elektronische Post, wobei auch insoweit unter Verstoß gegen das vom Bundesverfassungsgericht ausdrücklich postulierte Gebot der Normenklarheit offen bleibt, wie weit diese Ausnahme angesichts der Speicherpflicht für Kurz-, Multimedia- „oder ähnlichen Nachrichten" im Ergebnis tatsächlich reicht – und einige wenige Anschlüsse der sozialen und kirchlichen Telefonberatung sollen von der umfassenden Speicherpflicht ausgenommen werden. Insgesamt ist darin eine allenfalls marginale Einschränkung des Kriteriums „ausnahmslos" zu sehen, die den EuGH-Vorgaben schwerlich genügen dürfte.[56]

Die Beschwerdeführer sind zudem, soweit sie in der Ausübung ihrer beruflichen Tätigkeit Geheimnisträger sind und besonderen Verschwiegenheitsverpflichtungen unterliegen, was für die hier klagenden Rechtsanwälte, Journalisten, Ärzte und Abgeordneten gleichermaßen gilt (§ 53 StPO), darüber hinaus in ihrer beruflichen Tätigkeit in besonderem Maße von der anlasslosen, zusammenhanglosen und ausnahmslosen Speicherung der Telekommunikationsverbindungsdaten betroffen.

Als Berufsgeheimnisträger werden sie – zum Leidwesen ihrer Mandanten, Patienten, Informanten und Gesprächspartner – in ihren Rechten völlig schutzlos gestellt. Nicht nur, dass ohne Weiteres von den Verbindungsdaten der Telefonate und der sonstigen von der Vorratsdatenspeicherung betroffenen elektronischen Kommunikation auf deren Inhalte geschlossen werden kann. Oftmals ist bereits der Umstand der Kontaktaufnahme sensibel und fällt unter die besondere Geheimsphäre. Ferner liegt insbesondere in

---

[54] Nachbaur, ZRP 2015, 215, 216.

[55] EuGH, a.a.O., Rz. 58 f.

[56] Nachbaur, ZRP 2015, 215, 216.

der Weite der Datenspeicherungsverpflichtung und der nicht hinreichenden Bestimmtheit ihrer Verwendung die Gefahr für Mandanten, Patienten, Informanten und Gesprächspartner, zu Unrecht in den Fokus von Ermittlungen zu geraten.

Zudem stellt eine anlasslose Speicherung der Telekommunikationsverbindungsdaten wegen der damit verbundenen Möglichkeit einer einschüchternden Wirkung eine Beeinträchtigung der Medienfreiheiten dar. Insbesondere können potentielle Informanten durch die begründete Befürchtung, durch die Speicherung und Erhebung der Daten könnte ihre Identität festgestellt werden, davon abgehalten werden, Informationen zu liefern, die sie nur im Vertrauen auf die Wahrung ihrer Anonymität herauszugeben bereit sind. Überdies liegt in der Verschaffung staatlichen Wissens über die im Bereich journalistischer Recherche hergestellten Kontakte ein Eingriff in das Redaktionsgeheimnis, dem neben dem Vertrauensverhältnis der Medien zu ihren Informanten eigenständige Bedeutung zukommt.[57]

Soweit die Beschwerdeführer in ihrer Eigenschaft als Berufsgeheimnisträger betroffen sind, wird sogar in der Gesetzesbegründung darauf hingewiesen, dass nach Entscheidungen sowohl des Bundesverfassungsgerichts[58] als auch des Gerichtshofs der Europäischen Union[59] die Verhältnismäßigkeit einer Speicherung von Verkehrsdaten besondere Regelungen zum Schutz von Personen voraussetzt, die beruflichen Verschwiegenheitspflichten unterliegen.[60] Damit räumt der Gesetzgeber selbst ein, dass die Grundrechte und die Vertraulichkeit der Kommunikation gerade von Berufsgeheimnisträgern bereits durch die Speicherung der Daten– und nicht erst durch deren Abruf – in besonderem Maße beeinträchtigt werden.

Dem entspricht, dass es der Gesetzgeber in diesem Zusammenhang für notwendig hält, Ausnahmen in Bezug auf die Speicherpflicht dahingehend vorzusehen, dass Daten, die den Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen zugrunde liegen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit besonderen Verschwiegenheitsver-

[57] BVerfG, Urteil v. 27.2.2007 – 1 BvR 538/06, Cicero.

[58] BVerfG, Urt. v. 2.3.2010 – 1 BvR 256/08.

[59] EuGH, Urt. v. 8.4.2014 – C-293/12 und C-594/12, Rz. 58.

[60] BT-Drucks. 18/5088, S. 33.

pflichtungen unterliegen, nicht gespeichert werden dürfen (§ 113b Abs. 6 TKG)[61] – und zwar „zum Schutz des besonderen Vertrauensverhältnisses", wie in der Gesetzesbegründung ausdrücklich betont wird.[62]

Nicht ausgenommen von der vorsorglich anlasslosen Speicherung von Telekommunikationsverkehrsdaten werden dagegen insbesondere Berufsgeheimnisträger wie Rechtsanwälte, Journalisten, Ärzte, Abgeordnete oder Pfarrer – und dies nicht etwa, weil der Gesetzgeber deren Kommunikationsvorgänge als weniger sensibel als die von Einrichtungen der sozialen und kirchlichen Telefonberatung ansieht, sondern lediglich aus Praktikabilitätserwägungen.[63] Schon allein dies verstößt gegen die klaren Vorgaben des Europäischen Gerichtshofs.[64] In der Gesetzesbegründung wird hierzu ausgeführt:

> *„Die Berufsgeheimnisträger in ihrer Gesamtheit schon von der Speicherung ihrer Verkehrsdaten auszunehmen, ist nicht möglich. Dazu müsste sämtlichen Telekommunikationsanbietern, von denen es in Deutschland ca. 1 000 gibt, mitgeteilt werden, wer Berufsgeheimnisträger im Sinne des § 53 StPO ist; diese Liste müsste dauernd aktualisiert werden. Ihre Erstellung, Übermittlung und Aktualisierung birgt auch im Falle des Einverständnisses der Betroffenen ein erhebliches Missbrauchsrisiko. Hinzu kommt, dass Berufsgeheimnisträger in vielen Fällen nicht über statische, sondern über dynamische IP-Adressen verfügen, so dass eine Liste der verwendeten Adressen gar nicht erstellt werden könnte. Der bessere Schutz ergibt sich daher bei einer Regelung, die die Verwendung der gespeicherten Daten ausschließt. Dieser Schutzmechanismus hat sich in der StPO auch an anderer Stelle bewährt."*[65]

Das kann aber in rechtlicher Hinsicht nicht überzeugen. Ein derart schwerwiegender Grundrechtseingriff ist nicht mit Praktikabilitätserwägungen oder technischen Hürden in der Lebenswirklichkeit zu rechtfertigen. Dies insbesondere dann nicht, wenn mit dieser auf nahezu alle Berufsgeheimnisträger in der Bundesrepublik Deutschland abzielenden Maßnahme in ihre Telekommunikationsfreiheiten derart massiv und radikal eingegriffen wird, statt die Vertraulichkeit ihrer Kommunikationsvorgänge als zwingend

---

[61] BT-Drucks. 18/5088, S. 23 f., 33, 39 f.

[62] BT-Drucks. 18/5088, S. 23.

[63] Vgl. BT-Drucks. 18/5088, S 39.

[64] EuGH, Urt. v. 8.4.2014 – C 293/12 und C 594/12, Rz. 58.

[65] BT-Drucks., 15-5088, Seite 33.

notwendige Kernvoraussetzung ihrer Tätigkeit wirksam zu schützen. Denn der Eingriff betrifft ja nicht nur die Berufsgeheimnisträger sondern reflektiert unmittelbar auf deren Kommunikationspartner, die sich in der Gewissheit überwacht zu werden, nicht mehr ohne weiteres und zwanglos den hier betroffenen Grundrechtsträgern anvertrauen werden. Der besondere Schutz, dem die Kommunikation und insofern auch die Telekommunikation zwischen Geheimnisträger und Kommunikationspartner unterliegt, ist kein Selbstzweck und auch kein in Zeiten terroristischer Bedrohungslagen zu vernachlässigender Belang, der ja ohnehin nur die betrifft, die etwas zu verbergen haben. Vielmehr wird hier in für das Gemeinwesen notwendige und in einer von der Geheimsphäre geschützte Kommunikation in nicht hinnehmbarer Weise eingegriffen. Die hier betroffene Kommunikation der Berufsgeheimnisträger dient einem gesamtgesellschaftlichen Interesse.

Der Rechtsanwalt ist Organ der Rechtspflege und hat als solcher eine gesellschaftliche Aufgabe zu erfüllen. Er ist dazu berufen, das Interesse seiner Mandanten zu vertreten.[66] Dem Rechtsanwalt als berufenem unabhängigen Berater und Beistand obliegt es, im Rahmen seiner freien und von Art. 12 Abs. 1 Satz 1 GG geschützten Berufsausübung seinen Mandanten umfassend beizustehen. Voraussetzung für die Erfüllung dieser Aufgabe ist ein Vertrauensverhältnis zwischen Rechtsanwalt und Mandant. In dieses Vertrauensverhältnis wird unmittelbar eingegriffen, wenn der Mandant befürchten muss, dass bereits die Kontaktaufnahme oder die Ansprache eines Anwaltes registriert und gegebenenfalls ausgewertet wird.

Diese Erwägungen gelten in ähnlicher Weise für das Vertrauensverhältnis zwischen einem Arzt und seinem Mandanten. Auch der Arzt nimmt im Bereich der Gesundheitssorge eine gesellschaftlich tragende Rolle ein. Auch hier ist das Vertrauensverhältnis zwischen Arzt und Patient wesentlich, zudem hier, je nach Fachrichtung des konsultierten Arztes, bereits in der Kontaktaufnahme die Intimsphäre betroffen sein kann – denn nach wie vor ist gilt es nicht in allen Teilen der Gesellschaft als sozialadäquat anerkannt, beispielsweise einen Psychiater oder Psychotherapeuten aufzusuchen.

In besonders schwerem Maße wiegt der Grundrechtseingriff auch bei den Journalisten. Der Schutz des Art. 10 Abs. 1 GG wird hier flankiert von den Medienfreiheiten, die wiederum nach der Rechtsprechung des Bundesverfassungsgericht Wesenselement des

[66] BVerfG, 17.11.1959 – 1 BvL 80/53.

freiheitlichen Staates und der Demokratie ist.[67] Die Medien beschaffen die Informationen, nehmen selbst dazu Stellung und wirken damit als orientierende Kraft in der öffentlichen Auseinandersetzung. In der repräsentativen Demokratie stehen die Medien zugleich als ständiges Verbindungs- und Kontrollorgan zwischen dem Volk und seinen gewählten Vertretern in Parlament und Regierung. Sie fassen die in der Gesellschaft und ihren Gruppen unaufhörlich sich neu bildenden Meinungen und Forderungen kritisch zusammen, stellen sie zur Erörterung und tragen sie an die politisch handelnden Staatsorgane heran, die auf diese Weise ihre Entscheidungen auch in Einzelfragen der Tagespolitik ständig am Maßstab der im Volk tatsächlich vertretenen Auffassungen messen können.[68] Zur Pressefreiheit gehört auch der Schutz des Vertrauensverhältnisses zwischen Medien und privaten Informanten. Er ist unentbehrlich, da die Presse auf private Mitteilungen nicht verzichten kann, diese Informationsquelle aber nur dann ergiebig fließt, wenn sich der Informant grundsätzlich darauf verlassen kann, dass das „Redaktionsgeheimnis" gewahrt bleibt. Anderenfalls würde sich kaum ein Informant vertraulich an Journalisten wenden. Dies wäre geeignet, die Pressefreiheit nicht nur beeinträchtigen, sondern sogar akut zu gefährden.

Auch die Kommunikationsvorgänge von Abgeordneten sind in besonderem Maße geschützt. Gemäß Art. 47 GG sind die Abgeordneten des Deutschen Bundestages berechtigt, über Personen, die ihnen in ihrer Eigenschaft als Abgeordnete oder denen sie in dieser Eigenschaft Tatsachen anvertraut haben, sowie über diese Tatsachen selbst das Zeugnis zu verweigern. Die Abgeordneten des Abgeordnetenhauses von Berlin haben gemäß Art. 51 Abs. 2 der Verfassung von Berlin das Recht, Angaben über Personen, die ihnen in ihrer Eigenschaft als Abgeordnete Mitteilung gemacht haben, und die Herausgabe von Schriftstücken zu verweigern, die ihnen in ihrer Eigenschaft als Abgeordnete übergeben wurden. In diesem Zusammenhang handelt es sich ebenfalls um geschützte Rechtsgüter von Verfassungsrang und um Grundvoraussetzungen zur Gewährleistung einer funktionierenden parlamentarischen Demokratie, die durch eine umfassende Vorratsdatenspeicherung konkret beeinträchtigt und damit in Frage gestellt wird.

Eine Abwägung der drohenden Beeinträchtigung des freien Meinungs- und Informationsaustausches auf der einen Seite und des graduellen Nutzens, den eine anlasslose, zusammenhangslos und nahezu ausnahmslose Vorratsspeicherung von Telekommunikationsverbindungsdaten allenfalls bewirken kann, muss auch an dieser Stelle zu dem

---

[67] BVerfG, Urt. v. 5.8.1966 – 1 BvR 586/62, Spiegel.

[68] Vgl. BVerfG, a.a.O.

Ergebnis kommen, dass die demokratiegewährleistenden Grundrechte der Meinungsfreiheit und Informationsfreiheit Vorrang beanspruchen. Insbesondere kann der mit einer solchen Datenspeicherung verbundene Effekt des gefühlten Überwachtseins nicht durch Möglichkeiten anonymer Telekommunikationsnutzung aufgefangen werden, weil die Nutzung dieser Möglichkeiten zusätzliche Kosten, jedenfalls aber zusätzliche Mühen und anderweitige Einschränkungen verursachen kann. Zudem bedarf es zu deren Nutzung eines Maßes an technischem Grundverständnis, über das nicht jeder verfügt. Der Wert eines freien und ungehinderten Austausches von Informationen über Telekommunikationsnetze ist im digitalen Zeitalter von allerhöchster Bedeutung. Gerade im Internet werden in besonderem Maße öffentliche Missstände aufgedeckt, ansonsten unzugängliche öffentliche Dokumente veröffentlicht und politische Fragen kontrovers diskutiert. Längst haben hier Portale wie netzpolitik.org die vom Bundesverfassungsgericht der Presse zugeschriebenen Aufgabe des öffentlichen Wachhundes[69] mitübernommen, wie die Affäre um den vermeintlichen Landesverrat wegen der Veröffentlichung von vermeintlichen Staatsgeheimnissen gezeigt hat.

Dies gilt umso mehr, als die Vorgabe, bei der Speicherverpflichtung zu Standortdaten auch die bei Beginn einer mobilen Internetverbindung genutzte Funkzelle zu erfassen, zu einer sehr umfangreichen Speicherung führen und insbesondere Daten erzeugen werden, die die Erstellung engmaschiger Bewegungsprofile ermöglichen.

Wäre die Datenspeicherung für sich genommen grundsätzlich unbedenklich, bedürfte es auch der vom Gesetzgeber getroffenen Ausnahmeregelung von vornherein nicht. Mit Blick darauf, dass der Gesetzgeber hierdurch selbst zugesteht, dass bereits die Datenspeicherung einen schwerwiegenden Eingriff in sensible Kommunikationsvorgänge von Berufsgeheimnisträgern und mithin eine entsprechend schwerwiegende Beeinträchtigung ihrer Vertraulichkeit darstellt, können reine Praktikabilitätserwägungen, wie sie vom Gesetzgeber angeführt werden,[70] zur Rechtfertigung der Datenspeicherung ersichtlich nicht in Betracht kommen.

Sämtliche betroffenen Berufsgeheimnisträger stehen in „besonderen Vertrauensverhältnissen“ im Sinne der Gesetzesbegründung, die durch eine Ausnahme von der Speicherpflicht zwingend zu schützen sind. Auch insoweit muss sich der Gesetzgeber an den von ihm selbst getroffenen Regelungen messen lassen. Zudem kann nur durch den Schutz al-

[69] Vgl. BVerfG, Beschl. v. 13.6.2006 – 1 BvR 565/06, Rz. 15.

[70] BT-Drucks. 18/5088, Seite 33.

ler Personen, die beruflichen Verschwiegenheitspflichten unterliegen, diese vom Gesetzgeber selbst herangezogene nach der Rechtsprechung des Bundesverfassungsgerichts und Europäischen Gerichtshofs[71] zwingende Voraussetzung für die Verhältnismäßigkeit einer Speicherung von Verkehrsdaten überhaupt erfüllt werden.

Indem trotz der vom Gesetzgeber mit der Regelung des § 113b Abs. 6 TKG nebst zugehöriger Begründung selbst anerkannten erheblichen Eingriffsqualität gleichwohl Daten zu sensiblen Kommunikationsvorgängen der Beschwerdeführer als Berufsgeheimnisträger von der Speicherung erfasst und nur einige wenige Einrichtungen und Personen hiervon ausgenommen werden sollen, sind die betroffenen Beschwerdeführer wie auch alle anderen Berufsgeheimnisträger insbesondere in ihrem Grundrecht aus Art. 3 Abs. 1 GG und Art. 20 der Charta verletzt. Auch insofern verkennt der Gesetzgeber, dass wenn das unionsrechtlich vorgegebene Speicherverbot zum Schutz von Berufsgeheimnisträgern faktisch nicht zu machen ist, dies nicht für ein bloßes Verwendungsverbot, sondern gegen die Verfassungs- und Unionrechtmäßigkeit der Vorratsdatenspeicherung spricht.[72]

(d) Speicherpflicht generell unzulässig

Schließlich ist aus der Entscheidung des Gerichtshofs der Europäischen Gerichtshof zur Vorratsdatenspeicherung sogar zu folgern, dass in Anbetracht der von Herrn Edward Snowden enthüllten Überwachungstätigkeiten von Nachrichtendiensten und anderen Behörden insbesondere der USA, die im Rahmen der von ihnen praktizierten massenhaften und wahllosen Überwachung und Erfassung weltweit und auch in der Europäischen Union auf Daten und Inhalte der elektronischen Kommunikation zugreifen, ohne dass die Unionsbürger insoweit einen wirksamen Anspruch auf rechtliches Gehör haben oder in irgendeiner Form benachrichtigt werden, und deren Zugriff auf die aufgrund einer in einem Mitgliedsstaat der Europäischen Union vorgeschriebenen Vorratsspeicherung gespeicherten Daten der elektronischen Kommunikation nicht ausgeschlossen werden kann, jedenfalls derzeit jegliche nationale Regelung, die die vorsorgliche Vorratsspeicherung von Telekommunikationsverkehrsdaten vorschreibt, prinzipiell weder mit den Art. 7, 8, 11 und 15 der Charta noch mit dem in Art. 47 der Charta verankerten Recht auf effektiven Rechtsschutz vereinbar sein kann.

---

[71] EuGH, Urt. v. 8.4.2014 – C-293/12 und C-594/12, Rz. 58.

[72] Vgl. Nachbaur, ZRP 2015, 215, 216.

Vor diesem Hintergrund erweist sich die Verfassungsbeschwerde als offensichtlich begründet, so dass die Aussetzung der Vorratsdatenspeicherung im Wege des Erlasses der beantragten einstweiligen Anordnung nicht nur möglich, sondern insbesondere mit Blick auf den Grundsatz des effektiven Vollzugs des Gemeinschaftsrechts auch zwingend geboten ist.

e) Gleichheitswidrige Ungleichbehandlung von Berufsgeheimnisträgern

Soweit die Beschwerdeführer in ihrer Eigenschaft als Berufsgeheimnisträger betroffen sind, wird in der Gesetzesbegründung darauf hingewiesen, dass nach Entscheidungen sowohl des Bundesverfassungsgerichts[73] als auch des Gerichtshofs der Europäischen Union[74] die Verhältnismäßigkeit einer Speicherung von Verkehrsdaten besondere Regelungen zum Schutz von Personen voraussetzt, die beruflichen Verschwiegenheitspflichten unterliegen.[75] Damit räumt der Gesetzgeber selbst ein, dass die Grundrechte und die Vertraulichkeit der Kommunikation gerade von Berufsgeheimnisträgern bereits durch die Speicherung der Daten– und nicht erst durch deren Abruf – in besonderem Maße beeinträchtigt werden.

Dem entspricht, dass es der Gesetzgeber in diesem Zusammenhang für notwendig hält, Ausnahmen in Bezug auf die Speicherpflicht dahingehend vorzusehen, dass Daten, die den Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen zugrunde liegen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit besonderen Verschwiegenheitsverpflichtungen unterliegen, nicht gespeichert werden dürfen (§ 113b Abs. 6 TKG)[76] – und zwar „zum Schutz des besonderen Vertrauensverhältnisses", wie in der Gesetzesbegründung ausdrücklich betont wird.[77]

Nicht ausgenommen von der vorsorglich anlasslosen Speicherung von Telekommunikationsverkehrsdaten werden dagegen insbesondere Berufsgeheimnisträger wie Rechtsanwälte, Journalisten, Ärzte, Parlamentsabgeordnete oder Pfarrer – und dies nicht etwa, weil

---

[73] BVerfG, Urt. v. 2.3.2010 – 1 BvR 256/08.

[74] EuGH, Urt. v. 8.4.2014 – C-293/12 und C-594/12, Rz. 58.

[75] BT-Drucks. 18/5088, S. 33.

[76] BT-Drucks. 18/5088, S. 23 f., 33, 39 f.

[77] BT-Drucks. 18/5088, S. 23.

der Gesetzgeber deren Kommunikationsvorgänge als weniger sensibel als die von Einrichtungen der sozialen und kirchlichen Telefonberatung ansieht, sondern lediglich aus Praktikabilitätserwägungen.[78] Dies verstößt nicht nur gegen die klaren Vorgaben des Europäischen Gerichtshofs, sondern auch gegen allgemeinen Gleichheitssatz gemäß Art. 3 Abs. 1 GG sowie Art. 20 der Charta.

Der Grundsatz, dass alle Menschen vor dem Gesetz gleich sind, soll in erster Linie eine ungerechtfertigte Bevorzugung oder Benachteiligung von Personen verhindern. Deshalb unterliegt der Gesetzgeber bei einer Ungleichbehandlung von Personengruppen regelmäßig einer strengen Bindung. Überdies sind dem Gestaltungsspielraum des Gesetzgebers umso engere Grenzen gesetzt, je stärker sich die Ungleichbehandlung von Personen oder Sachverhalten auf die Ausübung grundrechtlich geschützter Freiheiten nachteilig auswirken kann.[79] In diesen Fällen prüft das Bundesverfassungsgericht im Einzelnen nach, ob für die vorgesehene Differenzierung Gründe von solcher Art und solchem Gewicht bestehen, dass sie die ungleichen Rechtsfolgen rechtfertigen können.[80]

Bei der Anwendung des Gleichheitsgebotes ist der jeweilige Lebens- und Sachbereich zu berücksichtigen.[81] So hat das Bundesverfassungsgericht ausgeführt, dass dem gesetzgeberischen Gestaltungsraum dort enge Grenzen gezogen sind, wo es sich um Regelungen handelt, die Auswirkungen auf die durch Art. 12 Abs. 1 GG geschützte Freiheit der beruflichen Tätigkeit haben.[82]

Nach der neueren Rechtsprechung des Bundesverfassungsgerichts begründet der Gleichheitssatz des Art. 3 Abs. 1 GG im Ergebnis eine enge Selbstbindung des Gesetzgebers, die es diesem zwar grundsätzlich nicht verwehrt, sachgerechte Differenzierungen vorzunehmen, die ihn aber dazu verpflichtet, die von ihm erlassenen Regelungen derart aufeinander abzustimmen, dass Widersprüchlichkeiten vermieden werden und somit eine Folgerichtigkeit der Gesamtregelung gewahrt bleibt.[83]

---

[78] BT-Drucks. 18/5088, S. 33.

[79] vgl. BVerfGE 98, 365; BVerfGE 60, 123, 134; 82, 126, 146.

[80] Vgl. BVerfGE 98, 365, Rz. 74, BVerfGE 88, 87, 96 f.

[81] Vgl. BVerfGE 60, 123, Rz. 41; BVerfGE 25, 269, 292; 35, 348, 357.

[82] Vgl. BVerfGE 60, 123, Rz. 41; BVerfGE 37, 342, 353 f.

[83] S. zum Bereich des Steuerrechts Kirchhof, StuW 2000, 316, 322; Schön, FR 2001, 381, 384, Drüen, StuW 2008, 3, 8; Musil/Volmering DB 2008, 12, 14.

Dies muss im Bereich von gravierenden Grundrechtseingriffen wie hier umso mehr gelten. Wäre die Datenspeicherung für sich genommen grundsätzlich unbedenklich, bedürfte es auch der vom Gesetzgeber getroffenen Ausnahmeregelung von vornherein nicht. Insofern müsste der Gesetzgeber hinreichend gewichtige Sachgründe dartun, die eine Ungleichbehandlung rechtfertigen könnten. Mit Blick darauf, dass der Gesetzgeber durch die von ihm getroffene Ausnahmeregelung selbst zugesteht, dass bereits die Datenspeicherung einen schwerwiegenden Eingriff in sensible Kommunikationsvorgänge von Berufsgeheimnisträgern und mithin eine entsprechend schwerwiegende Beeinträchtigung ihrer Vertraulichkeit darstellt, können reine Praktikabilitätserwägungen, wie sie vom Gesetzgeber angeführt werden,[84] zur Rechtfertigung der Datenspeicherung ersichtlich nicht in Betracht kommen. Diese Erwägungen bestätigen vielmehr, dass sich die in diesem Zusammenhang zu betrachtenden Personengruppen und Sachverhalte – Berufsgeheimnisträger im Bereich von Einrichtungen der sozialen und kirchlichen Telefonberatung sowie alle sonstigen Berufsgeheimnisträger –, was ihre Schutzwürdigkeit und –bedürftigkeit in Bezug auf den Kern der betroffenen Tätigkeiten bzw. Grundrechtsausübungen betrifft, in keiner Weise dahingehend unterscheiden, dass eine Ungleichbehandlung gerechtfertigt sein könnte.

Sämtliche betroffenen Berufsgeheimnisträger stehen in „besonderen Vertrauensverhältnissen“ im Sinne der Gesetzesbegründung, die durch eine Ausnahme von der Speicherpflicht zwingend zu schützen sind. Auch und gerade mit Blick auf Art. 3 Abs. 1 GG muss sich der Gesetzgeber an den von ihm selbst getroffenen Regelungen messen lassen. Zudem kann nur durch den Schutz aller Personen, die beruflichen Verschwiegenheitspflichten unterlie¬gen, diese vom Gesetzgeber selbst herangezogene nach der Rechtsprechung des Bundesverfassungsgerichts und Europäischen Gerichtshofs[85] zwingende Voraussetzung für die Verhältnismä¬ßigkeit einer Speicherung von Verkehrsdaten überhaupt erfüllt werden.

Indem trotz der vom Gesetzgeber mit der Regelung des § 113b Abs. 6 TKG nebst zugehöriger Begründung selbst anerkannten erheblichen Eingriffsqualität gleichwohl Daten zu sensiblen Kommunikationsvorgängen der Beschwerdeführer als Berufsgeheimnisträger von der Speicherung erfasst wer¬den sollen und nur einige wenige Einrichtungen und Personen hiervon ausnimmt, sind die betroffenen Beschwerdeführer alle anderen Berufsgeheimnisträger insbesondere in ihrem Grundrecht aus Art. 3 Abs. 1 GG und Art. 20 der Charta verletzt. Auch insofern verkennt der Gesetzgeber, dass wenn das unionsrechtlich

[84] BT-Drucks. 18/5088, Seite 33.

[85] EuGH, Urt. v. 8.4.2014 – C-293/12 und C-594/12, Rz. 58.

vorgegebene Speicherverbot zum Schutz von Berufsgeheimnisträgern faktisch nicht zu machen ist, dies nicht für ein bloßes Verwendungsverbot, sondern gegen die Verfassungs- und Unionrechtsmäßigkeit der Vorratsdatenspeicherung spricht.[86]

III. Aussetzung der Vorratsdatenspeicherung zur Wahrung des Unionsrechts zwingend geboten

Unabhängig von den vorstehenden Erwägungen ist die Vorratsdatenspeicherung schon allein wegen der Verpflichtung der Bundesrepublik Deutschland zur Wahrung des effektiven Vollzugs des Unionsrechts einstweilen auszusetzen.

1.) Zwingende Vorgaben des EuGH nicht erfüllt

a) Anlasslose, zusammenhanglose und fast ausnahmslose Speicherung

Aus der Entscheidung des Gerichtshofs der Europäischen Gerichtshof zur Vorratsdatenspeicherung[87] ergibt sich, dass eine nationale Regelung, die wie das angegriffene Gesetz die vorsorgliche Vorratsspeicherung von Telekommunikationsverkehrsdaten vorschreibt und

- die in umfassender Weise alle Personen betrifft, die elektronische Kommunikationsdienste nutzen, ohne dass sich jedoch die Personen, deren Daten auf Vorrat gespeichert werden, auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte, und also auch für Personen gilt, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte,[88]

- die zwar zur Bekämpfung schwerer Kriminalität beitragen soll, aber keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit verlangt und insbesondere die Vorratsspeicherung weder auf die Daten eines bestimmten Zeitraums und/oder eines bestimmten geografischen Gebiets und/oder eines bestimmten Personenkreises be-

[86] Vgl. Nachbaur, ZRP 2015, 215, 216.

[87] EuGH, Urt. v. 8.4.2014 – C 293/12 und C 594/12.

[88] EuGH, a.a.O., Rz. 58, ff.

schränkt, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnten[89]

- die lediglich Ausnahmen dahingehend vorsieht, dass Daten von Diensten der elektronischen Post sowie Daten, die den Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen zugrunde liegen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit besonderen Verschwiegenheitsverpflichtungen unterliegen, nicht gespeichert werden dürfen, aber darüber hinaus keinerlei Ausnahme vorsieht, so dass sie auch für sämtliche sonstigen Personen gilt, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen[90]

mit dem in Art. 7 der Charta verankerten Recht auf Privatleben, mit dem in Art. 8 der Charta verankerten Recht auf Schutz personenbezogener Daten und mit dem in Art. 11 der Charta verankerten Recht auf Freiheit der Meinungsäußerung nicht vereinbar ist.

In Ansehung der betroffenen Berufsgeheimnisträger kommt hinzu, dass eine solche Regelung auch gegen die in Art. 15 der Charta verankerten Berufsfreiheit sowie den in Art. 20 der Charta verankerten allgemeinen Gleichheitssatz verstößt.

b) Speicherpflicht generell unzulässig

In Anbetracht der von Herrn Edward Snowden enthüllten Überwachungstätigkeiten von Nachrichtendiensten und anderen Behörden vor allem der USA, insbesondere der National Security Agency (NSA), die im Rahmen der von ihnen praktizierten massenhaften und wahllosen Überwachung und Erfassung weltweit und auch in der Europäischen Union auf Daten und Inhalte der elektronischen Kommunikation zugreifen, ohne dass die Unionsbürger insoweit einen wirksamen Anspruch auf rechtliches Gehör haben oder in irgendeiner Form benachrichtigt werden, und deren Zugriff auf die aufgrund einer in einem Mitgliedsstaat der Europäischen Union vorgeschriebenen Vorratsspeicherung gespeicherten Daten der elektronischen Kommunikation nicht ausge-

[89] EuGH, a.a.O.

[90] EuGH, a.a.O.

schlossen werden kann, ist aus der Entscheidung des Gerichtshofs der Europäischen Gerichtshof vom 08.04.2014[91] sogar zu folgern, dass jedenfalls derzeit jede nationale Regelung, die die vorsorgliche Vorratsspeicherung von Telekommunikationsverkehrsdaten vorschreibt, generell weder mit den Art. 7, 8, 11 und 15 der Charta noch mit dem in Art. 47 der Charta verankerten Recht auf effektiven Rechtsschutz vereinbar sein kann.

In diesem Zusammenhang ist etwa auf die Entscheidung des Europäischen Gerichtshofs vom 06.10.2015 zum Safe-Harbor-Abkommen zu verweisen,[92] in der diese auch vorliegend zu berücksichtigenden tatsächlichen Umstände – nämlich die durch die Enthüllungen von Herrn Edward Snowden bekannt gewordenen Tätigkeiten nationaler und internationaler Nachrichtendienste auch in Deutschland in Bezug auf die massenhafte Überwachung und Erfassung von Daten und Inhalten der elektronischen Telekommunikation einschließlich rechtswidrigen Kooperation der in Deutschland tätigen Telekommunikationsunternehmen mit diesen Diensten – bereits ihren Niederschlag gefunden haben:[93]

> *„Herr Schrems erhob gegen die im Ausgangsverfahren in Rede stehende Entscheidung Klage beim High Court. Dieser stellte nach Prüfung der von den Parteien des Ausgangsverfahrens vorgelegten Beweise fest, dass die elektronische Überwachung und Erfassung der aus der Union in die Vereinigten Staaten übermittelten personenbezogenen Daten notwendigen und unerlässlichen Zielen von öffentlichem Interesse diene. Die Enthüllungen von Herrn Snowden hätten jedoch gezeigt, dass die NSA und andere Bundesbehörden „erhebliche Exzesse" begangen hätten.*
>
> *Der High Court fügte hinzu, die Unionsbürger hätten keinen wirksamen Anspruch auf rechtliches Gehör. Die Überwachung der Handlungen der Nachrichtendienste finde ex parte und unter Geheimhaltung statt. Sobald die personenbezogenen Daten in die Vereinigten Staaten übermittelt worden seien, könnten die NSA und andere Bundesbehörden wie das Federal Bureau of Investigation (FBI) darauf im Rahmen der von ihnen praktizierten massenhaften und wahllosen Überwachung und Erfassung zugreifen."*

---

[91] EuGH, Urt. v. 8.4.2014 – C-293/12 und C-594/12.

[92] EuGH, Urt. v. 6.10.2015 – C-362/14, Safe Harbor.

[93] EuGH, Urt. v. 6.10.2015 – C-362/14, Rz. 28 ff. insb. 30 f., Safe Harbor.

Vor diesem Hintergrund kann keine Rede davon sein, dass die zentrale und unbedingte Vorgabe des Europäischen Gerichtshofs in seiner Entscheidung vom 08.04.2014, nämlich dass

> *in Bezug auf die Sicherheit und zum Schutz der von den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder den Betreibern eines öffentlichen Kommunikationsnetzes auf Vorrat gespeicherten Daten den Personen, deren Daten auf Vorrat gespeichert werden, ausreichende Garantien dafür geboten werden müssen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen, weil das Erfordernis, über solche Garantien zur verfügen, umso bedeutsamer ist, wenn die personenbezogenen Daten automatisch verarbeitet werden und eine erhebliche Gefahr des unberechtigten Zugangs zu diesen Daten besteht (EuGH Rz. 54 f., 66; vgl. entsprechend, zu Art. 8 EMRK, Urteile des EGMR Liberty u. a./Vereinigtes Königreich vom 1. Juli 2008, Nr. 58243/00, §§ 62 und 63, Rotaru/Rumänien, §§ 57 bis 59, sowie S und Marper/Vereinigtes Königreich, § 99),*

zumindest derzeit auch nur ansatzweise erfüllt wird. Vielmehr kann ein umfassender Zugriff insbesondere der Nachrichtendienste auf die Daten, deren Vorratsspeicherung die angegriffenen Normen vorschreiben, gerade nicht ausgeschlossen werden.

Vielmehr ist gerade vor diesem Hintergrund der mit der Datenspeicherung verbundene Eingriff in die in Art. 7, Art. 8, Art. 11 und Art. 15 der Charta verankerten Grundrechte, wie auch der Generalanwalt insbesondere in den Nrn. 77 und 80 seiner Schlussanträge ausgeführt hat, von großem Ausmaß und als besonders schwerwiegend anzusehen. Außerdem ist der Umstand, dass Speicherung und Nutzung der Daten von Seiten der Nachrichtendienste erfolgen, ohne dass der Betroffene darüber informiert wird, geeignet, bei den Betroffenen – wie der Generalanwalt in den Nrn. 52 und 72 seiner Schlussanträge ausgeführt hat – das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist.[94]

Daher ist der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit uneingeschränkt beizupflichten, wenn sie in ihrer Stellungnahme zum Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten wie folgt dezidiert kritisiert:

---

[94] EuGH, Urt. v. 6.10.2015 – C-362/14, Rz. 37, Safe Harbor.

„Dabei sind die IP-Adressen nicht nur als Verkehrsdaten im Sinne des TKG, sondern auch als Nutzungsdaten im Sinne des Telemediengesetzes betroffen. Gerade letztere vermitteln aber detaillierte Informationen über die im Internet genutzten Inhalte. Anhand der bei den Telemediendiensten erhobenen Nutzungsdaten können Sicherheitsbehörden im Zusammenspiel mit der Zuordnungsmöglichkeit der IP-Adressen der Vorratsdatenspeicherung (...) somit zumindest über mehrere Wochen das Surfverhalten der Internetnutzer äußerst detailliert überwachen. Dass es sich hierbei um ein realistisches Szenario handelt, belegt auch die aktuelle Diskussion zum Thema „NSA", in der unzweifelhaft offen gelegt wurde, dass eine umfassende Überwachung des Internetverkehrs für Nachrichtendienste heute nicht nur kein Problem mehr darstellt, sondern auch tatsächlich praktiziert wird. Durch die in § 113c Absatz 1 Nummer 3 TKG-E geschaffene Verknüpfung mit § 113 TKG können diese auch die in den Vorratsdaten gespeicherten IP-Adressen zumindest mittelbar nutzen (...)."[95]

Aus diesem offenkundigen Verstoß gegen Unionsrecht und der Verletzung von Unionsgrundrechten folgt, dass die durch die angegriffenen Normen angeordnete Vorratsdatenspeicherung zwingend auszusetzen ist.

2.) BVerfG zur einstweiligen Aussetzung unionsrechtlich verpflichtet

Die Rechtsprechung des Europäischen Gerichtshofs hat geklärt, dass nationales Recht Instrumente bereitzustellen hat, die dem Unionsrecht zur vollen Wirksamkeit verhelfen, und nationale Gerichte gegebenenfalls von nationalen Normen abweichen müssen, wenn dies zur Durchsetzung von Unionsrecht erforderlich ist.[96]

In diesem Zusammenhang sind grundlegend die vom Europäischen Gerichtshof herausgearbeiteten allgemeinen Pflichten zu berücksichtigen, die alle Staatsfunktionen, also Legislative, Exekutive, Judikative, gesamtstaatlich und funktionsübergreifend betreffen, ungeachtet der funktionsspezifischen Erfüllung dieser Pflichten durch die einzelnen Staatsorgane.

---

[95] Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten v. 9.6.2015, S. 8.

[96] Vgl. Steindorff, EuZW 1997, 7, 10.

Der Europäische Gerichtshof hat mit dem Vorrang des Unionsrechts und der unmittelbaren Geltung und Wirkung von Normen des Primärrechts einschließlich der Unionsgrundrechte als allgemeine Rechtsgrundsätze die dafür erforderlichen Prinzipien zur Sicherung des Unionsrechts entwickelt. In der praktischen Anwendung obliegt die Wahrung dieser Prinzipien den Mitgliedsstaaten und dabei zunächst den Verwaltungsbehörden, sodann den Gerichten. Gerichte und Behörden der Mitgliedsstaaten haben den Vorrang des Unionsrechts, insbesondere der Unionsgrundrechte, beim Vollzug des Unionsrechts und allen Tätigkeiten im Anwendungsbereich der Verträge von Amts wegen zu berücksichtigen. Sie müssen nationales Recht unionsrechtskonform auslegen und entgegenstehendes Recht außer Anwendung lassen.[97]

Zur Sicherung der Einheitlichkeit und der Effektivität des Vollzugs des Unionsrechts hat der Europäische Gerichtshof die Grundsätze des Effektivitätsgebots und des Äquivalenzgrundsatzes entwickelt, die insoweit unmittelbare Wirkung entfalten.[98] Dabei fordert das Effektivitätsgebot, dass die im nationalen Recht vorgesehenen Modalitäten die Tragweite und Wirksamkeit des Unionsrechts nicht beeinträchtigen, insbesondere die Herstellung des gemeinschaftsrechtlich gebotenen Zustands nicht praktisch unmöglich machen dürfen.[99]

Die Wahrung des Unionsrechts obliegt im erheblichen Umfang den Gerichten der Mitgliedsstaaten. Dem Unionsrecht, insbesondere dem unmittelbar anwendbaren Primärrecht einschließlich der Unionsgrundrechte muss in jedem Fall der Vorrang vor entgegenstehendem nationalem Recht eingeräumt werden. Dieser Aufgabe müssen die Gerichte der Mitgliedstaaten unter Beachtung des Effektivitäts- und Äquivalenzgrundsatzes als funktionelle Unionsrechtsgerichte nachkommen. Der effektive und einheitliche Vollzug als Existenzbedingung dieser Rechtsordnung und die Wahrung der durch diese Rechtsordnung begründeten Gewährleistungen, insbesondere Individualrechte und unmittelbar anwendbare Grundfreiheiten, erfordern entsprechenden Rechtsschutz im nationalen Recht, das insoweit europäisiert wird. Dies hat erhebliche Folgen für den primären wie den sekundären Rechtsschutz im Recht der Mitgliedsstaaten. Dabei sind die Grundsätze des Vorrangs und der wirksamen Durchsetzung des Gemeinschaftsrechts auch im Rahmen der Abwägung der Interessen der an einem gerichtlichen Verfahren beteiligten Parteien zu beachten.

---

[97] Zur verfassungsrechtlichen Rechtfertigung vgl.: BVerfG, Beschl. v. 9.6.1971 – 2 BvR 225/69.

[98] Grundlegend: EuGH, Rs. 804/79, Kommission/Vereinigtes Königreich, Slg. 1981, 1042, Rz. 28.

[99] EuGH, verb. RS 205-215/82, Deutsches Milchkontor, Slg. 1983, 2633 Rn. 23.

Anknüpfungspunkt für den – auch einstweiligen – Rechtschutz ist Art. 47 der Charta, wonach effektiver Rechtsschutz gerade auch gemeinschaftsrechtlich garantiert wird.[100] Demnach hat jede Person, deren durch das Recht der Union garantierte Rechte oder Freiheiten verletzt worden sind, das Recht, bei einem Gericht einen wirksamen Rechtsbehelf einzulegen. Diese Möglichkeit eines effektiven gerichtlichen Rechtsschutzes ist zugleich Ausfluss des in Art. 2 EUV statuierten europäischen Grundsatzes der Rechtsstaatlichkeit.[101] Zur Wirksamkeit eines gerichtlichen Rechtsbehelfs gehört insbesondere auch die Möglichkeit, erforderlichenfalls einstweiligen Rechtsschutz zu erlangen.[102]

Zur Gewährleistung und Reichweite von einstweiligem Rechtsschutz im Unionsrecht hat sich der EuGH in mehreren Entscheidungen geäußert.[103] So ist Unionsrecht insbesondere dahin auszulegen, dass ein nationales Gericht, das in einem bei ihm anhängigen, das Unionsrecht betreffenden Rechtsstreit zu der Auffassung gelangt, dem Erlass einstweiliger Anordnungen stehe nur eine Vorschrift des nationalen Rechts entgegen, diese Vorschrift nicht anwenden darf.[104]

Nach der ständigen Rechtsprechung des Europäischen Gerichtshofs zu der Frage, welche Konsequenzen das nationale Gericht aus einem Widerspruch zwischen Bestimmungen seines innerstaatlichen Rechts und den durch die Grundrechtecharta verbürgten Rechten zu ziehen hat, ist das nationale Gericht, das im Rahmen seiner Zuständigkeit die Bestimmungen des Unionsrechts anzuwenden hat, gehalten, für die volle Wirksamkeit dieser Normen Sorge zu tragen, indem es erforderlichenfalls jede – auch spätere – entgegenstehende Bestimmung des nationalen Rechts aus eigener Entscheidungsbefugnis unangewandt lässt, ohne dass es die vorherige Beseitigung dieser

---

[100] Siehe auch Art. 13 EMRK; vgl. auch Schoch, in: Schoch/Schmidt-Aßmann/Pietzner, VwGO, Vorb. § 80 Rdnr. 18.

[101] Vgl. dazu: EuGH, Rs. 222/86 (Unectef/Heylens), Slg. 1987, 4097; Rs. 222/84 (Johnsten), Slg. 1986, 1651, 1681, Rn. 18f.

[102] EuGH; Rs. C-213/89, Slg. 1990, I-2433, Rn. 10 (Factortame) Alber, in: Tettinger/Stern, Europäische Grundrechtecharta, Art. 47, Rn. 44, Blanke, in: Calliess/Ruffert, Art. 47 Rn. 1.

[103] (Vgl. dazu EuGH, Rs. C-213/89 (Facortame), Slg. 1990, 2433 ff; Rs. C 217/88 (Tafelwein), Slg. 1990, 2879 ff; Rs. C-143/88 (Süderdithmarschen), Slg. 1991, 415 ff; Rs. C-465/93 (Altlanta), Slg. 1996, I-3761 ff; Rs. 68/95 (T. Port), Slg. 1996, I-6065 ff.

[104] EuGH, Rs. C-213/89 (Facortame), Slg. 1990, 2433, 2466.

Bestimmung auf gesetzgeberischem Wege oder durch irgendein anderes verfassungsrechtliches Verfahren beantragen oder abwarten müsste.[105]

Mit den in der Natur des Unionsrechts liegenden Erfordernissen ist nämlich jede Bestimmung einer nationalen Rechtsordnung oder jede Gesetzgebungs-, Verwaltungs- oder Gerichtspraxis unvereinbar, die dadurch zu einer Schwächung der Wirksamkeit des Unionsrechts führt, dass dem für die Anwendung dieses Rechts zuständigen Gericht die Befugnis abgesprochen wird, bereits zum Zeitpunkt dieser Anwendung alles Erforderliche zu tun, um diejenigen innerstaatlichen Rechtsvorschriften auszuschalten, die unter Umständen ein Hindernis für die volle Wirksamkeit der Unionsnormen bilden.[106]

Handelt es sich bei dem zur Entscheidung berufenen nationalen Gericht wie hier um ein Verfassungsgericht mit Normverwerfungskompetenz, das in einem Verfassungsbeschwerdeverfahren zu entscheiden hat, muss dies zwingend zur Nichtigerklärung der angegriffenen dem Unionsrecht entgegenstehenden und die Unionsgrundrechte verletzenden nationalen Normen und – in einem Verfassungsbeschwerdeverfahren wie hier – mithin zum Erfolg der Verfassungsbeschwerde führen. Geht es um eine Entscheidung in einem Verfahren auf Erlass einer einstweiligen Anordnung, führen diese Erwägungen zu dem Ergebnis, dass eine Aussetzung der dem Unionsrecht entgegenstehenden und die Unionsgrundrechte verletzenden Vorschriften des nationalen Rechts zwingend geboten ist. Dies schließt insbesondere ein, dass nationales Recht, das dem Erlass einer solchen einstweiligen Anordnung entgegenstehen könnte, unionsrechtkonform auszulegen oder – falls dies nicht möglich ist – unangewandt zu bleiben hat.

Dies ist im Übrigen auch mit Blick auf Art. 4 Abs. 3 EUV geboten. Die sich hierauf beziehende Vorlagefrage des irischen High Court, ob die nationalen Gerichte aufgrund der Pflicht zur loyalen Zusammenarbeit die Vereinbarkeit der nationalen Vorschriften zur Umsetzung der Richtlinie 2006/24 mit den Bestimmungen der Charta zu prüfen und festzustellen haben, wurde vom Generalanwalt jedenfalls u.a. mit Hinweis auf die Entscheidung des EuGH (Åkerberg Fransson)[107], eindeutig bejaht.[108] Dies gilt gerade auch

---

[105] EuGH, Urt. v. 26.2.2013 – C-617/10 mit Hinweis auf EuGH, Urteile vom 9. 3.1978, Simmenthal, 106/77, Slg. 1978, 629, Randnrn. 21 und 24, vom 19.11.2009, Filipiak, C-314/08, Slg. 2009, I-11049, Randnr. 81, sowie vom 22.6.2010, Melki und Abdeli, C-188/10 und C-189/10, Slg. 2010, I-5667, Randnr. 43.

[106] Urteil Melki und Abdeli, Randnr. 44 und die dort angeführte Rechtsprechung.

[107] EuGH, Urt. v. 26.2.2013 – C-617/10.

dann, wenn der Grundrechtsschutz nach innerstaatlichem Verfassungsrecht im Vergleich zum unionsrechtlichen Primärrecht weniger weitgehend sein sollte; diese Divergenz ist zwingend so aufzulösen, dass das Unionsrecht Vorrang hat und gewährleistet wird, dass die Unionsgrundrechte ihre volle Wirkung entfalten.

Der Aussetzung der Vorratsdatenspeicherung ist insbesondere deswegen ohne Alternative, weil die Verpflichtung der Bundesrepublik Deutschland zur Wahrung des effektiven Vollzugs des Unionsrechts vorliegend auf andere Weise nicht erfüllt werden kann. Denn da das Gesetz bereits durch sein bloßes Inkrafttreten die Antragsteller in ihren Unionsgrundrechten unmittelbar und irreversibel beeinträchtigt, bedarf es, um dies effektiv zu vermeiden, einer Aussetzung des Gesetzes durch das Bundesverfassungsgericht. Insbesondere stellt es von vornherein keinerlei zumutbare oder effektive Alternative dar, die Antragsteller darauf zu verweisen, vor den Fachgerichten gegen die Telekommunikationsunternehmen zu klagen.

3.) Inkrafttreten des Gesetzes steht unmittelbar bevor

Die Wahrung des effektiven Vollzugs des Unionsrechts gebietet es darüber hinaus, die einstweilige Anordnung bereits jetzt mit Wirkung vom Inkrafttreten der angegriffenen Normen an zu erlassen.

Bei dem verfahrensgegenständlichen vom Bundestag am 16.10.2015 beschlossenen Gesetz handelt es sich um ein Einspruchsgesetz, das nicht der Zustimmung des Bundesrats bedarf. Dadurch, dass der Bundesrat heute den Antrag gemäß Art. 77 Abs. 2 GG bezüglich dieses Gesetzes nicht gestellt hat, ist es zustande gekommen. Aufgrund dessen droht nunmehr dessen kurzfristiges Inkrafttreten. Denn gemäß seinem Artikel 7 wird das angegriffene Gesetz schon unmittelbar am Tag nach seiner ab sofort jederzeit möglichen Verkündung in Kraft treten. Ein Inkrafttreten des Gesetzes kann jedoch insbesondere wegen der Verpflichtung der Bundesrepublik Deutschland zur Wahrung des effektiven Vollzugs des Unionsrechts und insbesondere der Gewährleistung der durch das Gesetz unmittelbar verletzten Unionsgrundrechte keinesfalls hingenommen werden. Insbesondere ist vor diesem Hintergrund und angesichts der dargelegten Nachteile zwingend zu vermeiden, dass das Gesetz zunächst – wenn auch nur vorübergehend für die Dauer des Verfahrens auf Erlass einer einstweiligen Anordnung – in Kraft tritt,

---

[108] Vgl. Schlussantr. d. Generalanwalts v. 12.12.2013 – C-293/12, C-594/12, Rdnrn. 28, 153; s. hierzu auch Rößner, EuZW 2014, 134.

wie dies etwa in Bezug auf später teilweise ausgesetzte Vorschriften der Vorgängerregelung im Verfahren 1 BvR 256/08 über einen Zeitraum von mehr als zwei Monaten – nämlich vom Inkrafttreten am 01.08.2008 bis zur Entscheidung des Bundesverfassungsgerichts am 11.03.2008 – geschehen ist.

Sollte sich das Bundesverfassungsgericht zum Erlass einer einstweiligen Anordnung vor Verkündung des angegriffenen Gesetzes nicht in der Lage sehen, ist über das Begehren der Antragsteller entsprechend des hilfsweise gestellten Antrags erst nach der Verkündung des angegriffenen Gesetzes zu entscheiden.

IV. Folgenabwägung führte zum selben Ergebnis

Eine aus Sicht des nationalen Rechts nach den Maßstäben des Bundesverfassungsgerichts[109] vorgenommene Folgenabwägung würde im Übrigen zu keinem anderen Ergebnis führen, als es in Ansehung der Wahrung des effektiven Vollzugs des Unionsrechts geboten ist.

Denn die Nachteile, die eintreten würden, wenn die einstweilige Anordnung nicht erginge, die Verfassungsbeschwerde später aber Erfolg hätte, würden die Nachteile in Ausmaß und Schwere deutlich überwiegen, die entstünden, wenn die begehrte einstweilige Anordnung erlassen würde, der Verfassungsbeschwerde aber der Erfolg zu versagen wäre.

1.) Maßstäbe in Anbetracht zwingenden Unionsrechts

Wird die Aussetzung des Vollzugs eines Gesetzes begehrt, ist bei der Folgenabwägung nach der Rechtsprechung des Senats ein besonders strenger Maßstab anzulegen.[110] Das Bundesverfassungsgericht darf von seiner Befugnis, das Inkrafttreten eines Gesetzes zu verzögern, nur mit größter Zurückhaltung Gebrauch machen, da der Erlass einer solchen einstweiligen Anordnung stets ein erheblicher Eingriff in die Gestaltungsfreiheit des Gesetzgebers ist. Ein Gesetz darf deshalb nur dann vorläufig am Inkrafttreten gehindert werden, wenn die Nachteile, die mit seinem Inkrafttreten nach späterer Feststellung seiner Verfassungswidrigkeit verbunden wären, in Ausmaß und Schwere die Nachteile deutlich überwiegen, die im Falle der vorläufigen Verhinderung eines sich als verfassungsgemäß

---

[109] BVerfG, Beschl. v. 11.3.2008 – 1 BvR 256/08; vgl. auch BVerfG, Beschl. v. 22.3.2005 – 1 BvR 2357/04.

[110] BVerfG, Beschl. v. 11.3.2008 – 1 BvR 256/08; vgl. BVerfG, Urt. v. 18.7.2001 – 1 BvQ 23/01; BVerfG, Beschl. v. 22.3.2005 – 1 BvR 2357/04; stRspr.

erweisenden Gesetzes einträten.[111] Bei dieser Folgenabwägung sind die Auswirkungen auf alle von dem Gesetz Betroffenen zu berücksichtigen, nicht nur Folgen, die sich für den Antragsteller ergeben.[112]

Soweit das Bundesverfassungsgericht darüber hinaus davon ausgeht, dass dieser Maßstab noch weiter zu verschärfen ist, wenn eine einstweilige Anordnung begehrt wird, durch die der Vollzug einer Rechtsnorm ausgesetzt wird, soweit sie zwingende Vorgaben des Gemeinschaftsrechts in das deutsche Recht umsetzt,[113] ist im vorliegenden Fall umgekehrt zu berücksichtigen, dass die Aussetzung einer Norm begehrt wird, die gegen zwingende Vorgaben des Gemeinschaftsrechts verstößt bzw. Unionsgrundrechte verletzt.

Das Bundesverfassungsgericht betont in diesem Zusammenhang ausdrücklich, dass angesichts der Integrationsoffenheit des Grundgesetzes[114] im Rahmen der Folgenabwägung die Auswirkungen für die Gemeinschaftsrechtsordnung zu berücksichtigen sind. Wenn demnach in dem Erlass einer einstweiligen Anordnung eine Störung des Gemeinschaftsinteresses an einem effektiven Vollzug des Gemeinschaftsrechts liegt, weil einem Gemeinschaftsrechtsakt die Wirkung in der Bundesrepublik Deutschland genommen wird, der sich letztlich als für den deutschen Gesetzgeber verbindlich erweist, gilt dies ebenso für die Ablehnung der gemeinschaftsrechtlich zwingend gebotenen Aussetzung einer gemeinschaftsrechtswidrigen Norm des nationalen Rechts. Der Senat bestätigt hierbei unter Hinweis auf die Rechtsprechung des Europäischen Gerichtshofs, dass das Interesse der Gemeinschaft am Vollzug des Gemeinschaftsrechts angemessen zu berücksichtigen ist.[115]

2.) Nachteile durch Normvollzug überwiegen Nachteile durch Aussetzung

Auch nach diesen Maßstäben ist dem Antrag auf Erlass einer einstweiligen Anordnung stattzugeben. Denn die Folgenabwägung ergibt, dass das öffentliche Interesse am Vollzug

---

[111] BVerfG, Beschl. v. 11.3.2008 – 1 BvR 256/08; vgl. BVerfG, Beschl. v. 22.5.2001 – 2 BvQ 48/00; BVerfG, Beschl. v. 5.12.2006 – 1 BvR 2186/06; stRspr.

[112] BVerfG, Beschl. v. 11.3.2008 – 1 BvR 256/08; vgl. BVerfG, Beschl. v. 22.3.2005 – 1 BvR 2357/04.

[113] BVerfG, Beschl. v. 11.3.2008 – 1 BvR 256/08.

[114] BVerfG Beschl. v. 11.3.2008 – 1 BvR 256/08; vgl. BVerfG, Urt. v. 12.10.1993 – 2 BvR 2134/92.

[115] BVerfG Beschl. v. 11.3.2008 – 1 BvR 256/08; vgl. EuGH, Urteil vom 21.2.1991 - C-143/88, C-92/89 - Zuckerfabrik Süderdithmarschen und Zuckerfabrik Soest, Slg. 1991, I-415, Rn. 22 ff.; Urteil vom 9.11.1995 - C-465/93 - Atlanta Fruchthandelsgesellschaft mbH u.a., Slg. 1995, I-3761, Rn. 31 ff.; Urteil vom 17.7.1997 - C-334/95 - Krüger GmbH&Co. KG, Slg. 1997, I-4517, Rn. 43 ff.; Urteil vom 6.12.2005 - C-461/03 - Gaston Schul, Slg. 2005, I-10513, Rn. 17 ff.

der angegriffenen Normen hinter den Nachteilen, die durch den Normvollzug drohen, zurückstehen muss.

a) Irreparable und besonders schwerwiegende Nachteile durch Speicherpflicht

Erginge keine einstweilige Anordnung, erwiese sich die Verfassungsbeschwerde aber später als begründet, so drohten Einzelnen und der Allgemeinheit in der Zwischenzeit Nachteile von ganz erheblichem Gewicht.[116]

Der Speicherung der Telekommunikations-Verkehrsdaten bewirkt für die Betroffenen gewichtige Nachteile, die sich durch eine spätere Nichtigerklärung der Vorschriften über die Datenbevorratung nicht mehr beheben ließen. Neben der Verpflichtung zur Wahrung des effektiven Vollzugs des Unionsrechts ist hierbei zu berücksichtigen, dass das Bundesverfassungsgericht bereits in seiner Entscheidung vom 11.03.2008 mit Blick auf die Datenspeicherung davon ausgegangen ist, dass die anlasslose Bevorratung sensibler Daten einen nicht rückgängig zu machenden erheblichen Einschüchterungseffekt bewirken kann.[117] Dieser Effekt ließe sich für die Zeit zwischen dem Inkrafttreten der Norm und der Entscheidung des Bundesverfassungsgerichts selbst dann nicht rückgängig machen, wenn die Verfassungsbeschwerde in der Hauptsache Erfolg haben sollte.[118]

Soweit die Antragsteller in ihrer Eigenschaft als Berufsgeheimnisträger betroffen sind, weist der Gesetzgeber darauf hin, dass nach Entscheidungen sowohl des Bundesverfassungsgerichts[119] als auch des Gerichtshofs der Europäischen Union[120] die Verhältnismäßigkeit einer Speicherung von Verkehrsdaten besondere Regelungen zum Schutz von Personen voraussetzt, die beruflichen Verschwiegenheitspflichten unterliegen.[121] Damit räumt der Gesetzgeber selbst ein, dass die Grundrechte und die Vertraulichkeit der Kommunikation gerade von Berufsgeheimnisträgern bereits durch die Speicherung der Daten– und nicht erst durch deren Abruf – in besonderem Maße beeinträchtigt werden.

---

[116] BVerfG, Beschl. v. 11.3.2008 – 1 BvR 256/08, Rz. 152 f.

[117] Vgl. zum grundrechtlichen Gewicht solcher Effekte: BVerfG, Beschl. v. 12.4.2005 – 2 BvR 1027/02, 46.

[118] Vgl. BVerfG, Beschl. v. 11.3.2008 – 1 BvR 256/08, Rz. 148; s. hierzu auch Rößner, EuZW 2014, 134.

[119] BVerfG, Urt. v. 2.3.2010 – 1 BvR 256/08.

[120] EuGH, Urt. v. 8.4.2014 – C-293/12 und C-594/12, Rz. 58.

[121] BT-Drucks. 18/5088, S. 33.

Dem entspricht, dass es der Gesetzgeber in diesem Zusammenhang für notwendig hält, Ausnahmen in Bezug auf die Speicherpflicht dahingehend vorzusehen, dass Daten, die den Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen zugrunde liegen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit besonderen Verschwiegenheitsverpflichtungen unterliegen, nicht gespeichert werden dürfen (§ 113b Abs. 6 TKG).

Wäre die Datenspeicherung für sich genommen grundsätzlich unbedenklich und im Rahmen der Folgenabwägung unbeachtlich, bedürfte es auch dieser Ausnahmeregelung von vornherein nicht. Indem der Gesetzgeber eine solche Ausnahmeregelung trifft, gesteht er also zu, dass Berufsgeheimnisträger schon durch die Speicherung in besonders schwerwiegendem Maße irreparabel betroffen werden.

Diese Einschätzung des Gesetzgebers im Hinblick auf die bereits mit der Vollziehung des Gesetzes verbundenen irreparablen Beeinträchtigungen der Betroffenen ist auch im Rahmen der Folgenabwägung maßgeblich zu berücksichtigen. Auch insoweit muss sich der Gesetzgeber mit Blick auf das Interesse an dem Vollzug eines Gesetzes an den von ihm selbst getroffenen Regelungen messen lassen. Indem trotz der vom Gesetzgeber selbst anerkannten Eingriffsqualität Daten zu sensiblen Kommunikationsvorgängen der Antragsteller als Berufsgeheimnisträger – zumal unter Verstoß gegen den Gleichheitssatz des Art. 3 Abs. 1 GG sowie Art. 20 der Charta – von der Speicherung erfasst werden, ist mit dem Vollzug des Gesetzes ein derart schwerwiegender und irreparabler Nachteil verbunden, der bereits für sich genommen die Aussetzung der angegriffenen Normen rechtfertigt.

Dies gilt mit Blick auf das Gebot des effektiven Vollzugs des Unionsrechts umso mehr, als die Antragsteller durch die angegriffene Speicherung besonders schwerwiegend und irreparabel auch in ihren Unionsgrundrechten verletzt werden, weil der damit verbundene Eingriff in die in Art. 7, 8, 11, 15 und 20 der Charta verankerten Grundrechte die meisten elektronischen Kommunikationsmittel, deren Nutzung stark verbreitet und im täglichen Leben jedes Einzelnen von wachsender Bedeutung ist, und zusammenhanglos, anlasslos und nahezu ausnahmslos[122]die gesamte deutsche Bevölkerung betrifft.[123] Er ist damit, wie

[122] Vgl. hierzu Nachbaur, ZRP 2015, 215, 216.

[123] Vgl. EuGH, Urt. v. 8.4.2014 – C-293/12 und C-594/12, Rz. 56.

auch der Generalanwalt insbesondere in den Nrn. 77 und 80 seiner Schlussanträge ausgeführt hat,

> *„von großem Ausmaß und als besonders schwerwiegend"*

anzusehen.[124] Diese Wertung des Europäischen Gerichtshofs ist auch im Rahmen der Folgenabwägung verbindlich und ihr zwingend zugrunde zu legen.

Angesichts des nicht auszuschließenden umfassenden und dauerhaften sowie massenhaften und wahllosen Zugriffs der Nachrichtendienste auf sämtliche Daten der elektronischen Kommunikation einschließlich der vorsorglich anlasslos gespeicherten Daten ist darüber hinaus von einer umfassenden und dauerhaften Beeinträchtigung auszugehen.

Auch in diesem Zusammenhang muss nochmals auf die deutliche Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit hingewiesen werden:

> *„Dabei sind die IP-Adressen nicht nur als Verkehrsdaten im Sinne des TKG, sondern auch als Nutzungsdaten im Sinne des Telemediengesetzes betroffen. Gerade letztere vermitteln aber detaillierte Informationen über die im Internet genutzten Inhalte. Anhand der bei den Telemediendiensten erhobenen Nutzungsdaten können Sicherheitsbehörden im Zusammenspiel mit der Zuordnungsmöglichkeit der IP-Adressen der Vorratsdatenspeicherung (...) somit zumindest über mehrere Wochen das Surfverhalten der Internetnutzer äußerst detailliert überwachen. Dass es sich hierbei um ein realistisches Szenario handelt, belegt auch die aktuelle Diskussion zum Thema „NSA", in der unzweifelhaft offen gelegt wurde, dass eine umfassende Überwachung des Internetverkehrs für Nachrichtendienste heute nicht nur kein Problem mehr darstellt, sondern auch tatsächlich praktiziert wird. Durch die in § 113c Absatz 1 Nummer 3 TKG-E geschaffene Verknüpfung mit § 113 TKG können diese auch die in den Vorratsdaten gespeicherten IP-Adressen zumindest mittelbar nutzen (...)."*[125]

---

[124] EuGH, Urt. v. 8.4.2014 – C-293/12 und C-594/12, Rz. 37.

[125] Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten v. 9.6.2015, Seite 8.

Dass insbesondere von Seiten ausländischer Nachrichtendienste entsprechende Gefahren im Sinne schweren Missbrauchs der Daten drohen, räumt der Gesetzgeber indirekt ein, wenn er in diesem Zusammenhang diffus auf „jüngere Erfahrungen" verweist, angesichts derer ein entgegen der Verwendungsbeschränkung in § 113c TKG-E erfolgender Zugriff auf gespeicherte „nicht nur als theoretische Gefahr erscheint". In geradezu naiver Verkennung der tatsächlichen Bedrohungslage meint der Gesetzgeber jedoch, dass bei einer Speicherung im Inland die in den §§ 113c ff. TKG-E enthaltenen Anforderungen insbesondere an die Verwendung und die Sicherheit der Daten umfassend gewährleistet und überprüft werden könnten.[126]

Diese nicht nur theoretische Gefahr schweren massenhaften Datenmissbrauchs schlägt sich auch in einem tiefgehenden Einschüchterungseffekt der gesamten Bevölkerung nieder. So gab etwa nach einer repräsentativen Studie aus dem Jahre 2013 zum Thema „Datensicherheit im Internet: Einfluss der „Snowden-Affäre" auf die Datensicherheit im Netz aus Sicht der Internet-Nutzer"[127] ein Großteil der 1.093 befragten Internetnutzer ab 18 Jahre an, ihr Vertrauen in die Sicherheit ihrer persönlichen Daten im Internet sei erschüttert. Dies sei vor allem auf das Bekanntwerden der Überwachungstätigkeiten der Nachrichtendienste aufgrund der Snowden-Enthüllungen zurückführen. Mehr als die Hälfte der Nutzer gab an, seit seither an der Datensicherheit in Deutschland zu zweifeln. Als direkte Konsequenz der Snowden-Enthüllungen haben 70 Prozent der Internet-Nutzer ihre Sicherheitssoftware auf den neuesten Stand gebracht. Für ebenso viele Nutzer sind Datenschutzthemen nun wichtiger als zuvor. Vor allem Nutzer aus den östlichen Bundesländern geben an, dass die Affäre ihr Online-Nutzungsverhalten beeinflusst habe.[128]

Gerade angesichts dieses Einschüchterungseffekts ist eine Vorratsspeicherung von Telekommunikationsverkehrsdaten besonders problematisch und auch nicht auch nur vorübergehend hinnehmbar. Denn durch Schaffung weiterer Datenpools, wie sie im Zuge der Vollziehung des Gesetzes entstünden, würden die Möglichkeiten einer unkontrollierten Datenverwendung und missbräuchlichen Ausspähung sensibler persönlicher Daten jedenfalls

---

[126] BT-Drucks. 18/5088, Seite 38.

[127] „Datensicherheit im Internet: Einfluss der „Snowden-Affäre" auf die Datensicherheit im Netz aus Sicht der Internet-Nutzer", Fittkau & Maaß Consulting, Studie im Auftrag der Internet World Messe, Internetrepräsentative Panelbefragung im Juli/August 2013, abrufbar unter: www.internetworld-messe.de/content/download/1466/14914/file/Studie_F&M_IW_Datenschutz und Datensicherheit im Internet.pdf

[128] „Datensicherheit im Internet: Einfluss der „Snowden-Affäre" auf die Datensicherheit im Netz aus Sicht der Internet-Nutzer", a.a.O., S. 6.

erheblich erweitert, ohne dass sich die hiervon Betroffenen den damit verbundenen rechtlichen und tatsächlichen Zugriffs- und Überwachungsmöglichkeiten entziehen könnten.

Die Antragsteller werden wie oben dargelegt auch insbesondere bereits durch das bloße Inkrafttreten des Gesetzes, nämlich dadurch beeinträchtigt, dass sie die Speicherung der Daten dann jederzeit zu gewärtigen haben.

Denn die mit dem Inkrafttreten des angegriffenen Gesetzes einhergehende Speicherpflicht gilt unmittelbar und unbedingt. Soweit diesbezüglich eine Implementierungsphase vorgesehen ist, stellt deren Ende den spätestmöglichen Zeitpunkt der Erfüllung dieser Speicherpflicht durch die Telekommunikationsunternehmen dar. Gleichwohl – dies sei nochmals betont – gilt die Verpflichtung zur Speicherung vom ersten Tage an. Diese Verpflichtung korrespondiert zudem mit einer ebenfalls unmittelbar mit Inkrafttreten des Gesetzes einsetzenden Berechtigung zur Speicherung durch die Telekommunikationsunternehmen, die somit ab diesem Zeitpunkt ohne weiteres jederzeit mit der Speicherung beginnen müssen und können. Insbesondere müssen die Telekommunikationsunternehmen nicht abwarten, bis die Bundesnetzagentur den Anforderungskatalog gemäß § 113f TKG veröffentlicht hat, da diese Vorschrift lediglich eine Vermutungsregel im Hinblick auf die Einhaltung des zu gewährleistenden Standards der Datensicherheit und Datenqualität darstellt.

Ein Abwarten mit der einstweiligen Außervollzugsetzung der angegriffenen Normen etwa bis zu dem Zeitpunkt, bis das erste Telekommunikationsunternehmen die kommende Speicherpflicht konkret erfüllt, ist schon allein deswegen nicht zumutbar, weil dieser Zeitpunkt völlig unbestimmt ist, insoweit auch keine Verpflichtung zur öffentlichen Bekanntmachung besteht und somit für die Antragsteller wie auch das Bundesverfassungsgericht gänzlich im Ungewissen liegt, wann die einzelnen verpflichteten Diensteanbieter konkret mit der Speicherung der Daten beginnen.

Im Übrigen hat das Bundesverfassungsgericht in einer insoweit vergleichbaren Konstellation in Bezug auf die Vorgängerregelung (Verfahren 1 BvR 256/08) im Jahre 2008 kein Hindernis gesehen, den Gesetzesvollzug im Wege der einstweiligen Anordnung zumindest teilweise bereits kurz nach Inkrafttreten der dort angegriffenen Normen auszusetzen, obwohl zu diesem Zeitpunkt die damals vorgesehene Umsetzungsphase von einem Jahr weder abgelaufen war, noch deren Ablauf kurz bevor stand, sondern das Gesetz gerade erst etwas mehr als zwei Monate in Kraft war. Es ist auch nicht ersichtlich, dass das Bundesverfassungsgericht seinerzeit darauf abgestellt hätte, ob in Erfüllung der gesetzlichen

Verpflichtungen bereits Daten auf Vorrat gespeichert und Abrufe der gespeicherten Daten getätigt wurden.

b) Nachteile durch Aussetzung der Speicherpflicht vernachlässigbar

Erginge eine auf die Speicherung der Daten bezogene einstweilige Anordnung, erwiesen sich die angegriffenen Normen jedoch später als verfassungs- und unionsrechtsgemäß, so könnten sich demgegenüber allenfalls überschaubare Nachteile für das öffentliche Interesse an einer effektiven Strafverfolgung und Gefahrenabwehr ergeben, die deutlich weniger schwer wiegen und angesichts des oben dargestellten Gewichts der dem Einzelnen und der Allgemeinheit durch den Vollzug der angegriffenen Normen drohenden Folgen und insbesondere der Verletzung der Verpflichtung zur Wahrung des effektiven Vollzugs des Unionsrecht einschließlich der Unionsgrundrechte hinzunehmen sind.

Diese Nachteile wiegen deutlich weniger schwer und sind angesichts des Gewichts der dem Einzelnen und der Allgemeinheit durch den Vollzug der angegriffenen Normen drohenden Nachteile hinzunehmen.

So ist von vornherein äußerst fraglich, ob das verfahrensgegenständliche Gesetz überhaupt einen nennenswerten Beitrag in Richtung einer effektiven Strafverfolgung oder Gefahrenabwehr leisten kann. Belastbare Angaben dazu, in wie vielen Fällen Abrufe von Verkehrsdaten seit dem 02.03.2010 erfolglos blieben, weil die Verkehrsdaten nicht über das Verbindungsende hinaus gespeichert oder zwischenzeitlich gelöscht worden waren, sind – soweit ersichtlich – nicht vorhanden. Dies gilt auch dafür, wie viele Straftaten und Gefahren im Zeitraum bis zum 02.03.2010 ausschließlich aufgrund der Möglichkeit der Erhebung von auf Vorrat gespeicherten Telekommunikationsverkehrsdaten aufgeklärt bzw. abgewehrt werden konnten und bei wie vielen Straftaten und Gefahren eine Aufklärung bzw. Abwehr wegen der bereits erfolgten Löschung dieser Daten nicht möglich war.

Belastbares Zahlenmaterial existiert auch nicht in Bezug auf die Frage nach dem Nutzen des angegriffenen Gesetzes. Eine seriöse Studie hierzu gibt es nicht.[129] Ob allerdings mit einer Speicherung der Telekommunikationsdaten der gesamten Bevölkerung der Bundesrepublik Deutschland tatsächlich schwere Kriminalität, insbesondere der internationale Terrorismus, wirksam bekämpft werden kann, darf mit guten Gründen bezweifelt werden. Nach einem Gutachten des wissenschaftlichen Dienstes des Deutschen Bundestages, das

[129] Vgl. Nachbaur, ZRP 2015, 215, 216.

sich auf Zahlen des Bundeskriminalamtes beruft, hat die Vorratsdatenspeicherung auf die Aufklärungsquoten in den EU- Mitgliedsstaaten „praktisch keine Auswirkungen". Die Aufklärungsquote steige mit der Vorratsdatenspeicherung nur marginal, nämlich um 0,006 %.[130] Umgekehrt liegen zu der Frage, welche Auswirkungen mit dem Wegfallen der Vorratsdatenspeicherung seit dem Urteil des Bundesverfassungsgerichts verbunden sind, insbesondere zu der Frage, ob die Aufklärungsquote signifikant gesunken ist, ebenfalls keine belastbaren Erkenntnisse vor.[131] Der Deutsche Anwaltverein führt hierzu in einer Stellungnahme zu dem Gesetzesentwurf aus wie folgt:

> *„Obwohl also keine gesicherten empirischen Erkenntnisse darüber vorliegen, ob mit der flächendeckenden Vorratsdatenspeicherung das Ziel der Gefahrenabwehr und der Strafverfolgung überhaupt erreicht werden kann, soll in das Grundrecht aus Art. 10 GG von 80 Millionen Bundesbürgerinnen und Bundesbürgern eingegriffen und die eine Demokratie ausmachende freie und offene Kommunikation gefährdet sowie das Risiko eines Datenmissbrauchs angelegt werden."*[132]

Während mit der Speicherung ein massenhafter und schwerwiegender Eingriff in die von den Antragstellern gerügten (Unions-)Grundrechte einhergeht, wird der konkrete Nutzen des angegriffenen Gesetzes gerade auch von Seiten der Strafverfolgungs- und Gefahrenabwehrbehörden in Zweifel gezogen. So heißt es in einem Medienartikel hierzu etwa wie folgt:[133]

---

[130] Wissenschaftlicher Dienst des Deutschen Bundestages, Sachstandsbericht v. 18. 3.2011, WD 7-3000-036/11, zitiert nach Stellungnahme des Deutschen Anwaltvereins durch die Ausschüsse Gefahrenabwehrrecht, Informationsrecht und Strafrecht zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz für ein Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (Stand: 15.5.2015).

[131] Vgl. Gutachten Max-Planck-Institut (zweite erweiterte Fassung) Juli 2011, S. 218, abrufbar unter: https://www.mpg.de/5000721/vorratsdatenspeicherung.pdf, zuletzt abgerufen am 3.11.2015.

[132] Stellungnahme des Deutschen Anwaltvereins durch die Ausschüsse Gefahrenabwehrrecht, Informationsrecht und Strafrecht zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz für ein Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (Stand: 15.05.2015), Seite 11.

[133] SPIEGEL ONLINE v. 26.6.2015, abrufbar unter: http://www.spiegel.de/netzwelt/netzpolitik/vorratsdatenspeicherung-ermittler-halten-gesetzentwurf-fuer-untauglich-a-1040779.html

„Die geplante Vorratsdatenspeicherung empört nicht nur Datenschützer. Auch Ermittler, denen das Gesetz eigentlich helfen soll, sind unzufrieden: Sie fürchten, teilweise schlechter gestellt zu werden als bisher.

(...)

Der vorgelegte Gesetzentwurf, der die Sicherheitslage in Deutschland verbessern soll, sorgt für erhebliche Ernüchterung in den Sicherheitsbehörden.

Es handele sich um Strafverfolgung vom Schreibtisch aus, sagt ein Kriminalbeamter aus dem Bereich der organisierten Kriminalität. Es werde deutlich, dass nur „wenig Fachwissen zur praktischen Arbeit von Ermittlungsbehörden" abgefragt worden sei.

Der Bund Deutscher Kriminalbeamter (BDK) erkennt sogar „erhebliche Schwachstellen" in dem Gesetzentwurf. Er sei praxisfern und bedürfe „dringend der Nachbesserung", heißt es in einer Stellungnahme für den Rechtsausschuss des Bundestages.

(...)

Als problematisch erachten Fahnder auch die geplante Länge der Speicherfrist. Während Datenschützer zehn Wochen als viel zu lang ansehen, halten die Ermittler das für entschieden zu kurz. Drei bis sechs Monate seien nötig, so der BDK. "Die kurze Speicherfrist von zehn Wochen für Verkehrs- und vier Wochen für Standortdaten ist weder verfassungsrechtlich geboten noch ermittlungstechnisch ausreichend. Möglicherweise entspringt sie vielmehr reinen rechtspolitischen Ängsten", schreibt der Richterbund. Ein Staatsschützer sagt: "In der Realität erfahren wir von vielen Delikten erst sehr viel später."

Nachbaur führt in diesem Zusammenhang aus:[134]

„Die Frage nach dem Nutzen der geplanten VDS-„light"-Version ist in Ermangelung belastbaren Zahlenmaterials nicht abschließend zu beantworten. Eine seriöse Studie hierzu gibt es nicht (...). Für den Bereich der Gefahrenabwehr lässt sich mutmaßen, dass die VDS infolge der hohen Tatbestandshürde – der Datenabruf erfordert eine bereits konkrete Gefahr (BVerfG, NJW 2010, 833 [841 f.] – ein weitgehend untaugliches Mittel

[134] Vgl. Nachbaur, ZRP 2015, 215, 216 f.

bleibt. Von polizeilichem Interesse wäre in erster Linie die Datennutzung im Vorfeld konkreter Gefahren („Verhinderungsvorsorge"); genau für diesen Zweck aber wurde dem Datenabruf durch das BVerfG aus Gründen der Verhältnismäßigkeit ein strikter Riegel vorgeschoben. Auch die typischerweise im Vorfeld konkreter Gefahren operierenden Geheimdienste kommen deshalb als abrufberechtigte Stellen so gut wie nicht in Betracht (BVerfG, NJW 2010, 833 [842]).

Auf dem Gebiet der Strafverfolgung könnte sich die Regelung mit Blick auf vielfältige Umgehungsmöglichkeiten ebenfalls als nur bedingt tauglich erweisen. Schon weil nicht alle Kommunikationsmittel erfasst werden dürfen (E-Mail) bzw. technisch (noch) gar nicht zu erfassen sind (Messenger-Dienste wie „WhatsApp"), können sich Straftäter der staatlichen Überwachung leicht entziehen, von der Nutzung legal zu erwerbender Anonymisierungssoftware ganz zu schweigen. Es wäre erstaunlich, wenn ausgerechnet Terroristen und andere Schwerkriminelle – nur um deren Bekämpfung soll und darf es im Kontext der VDS gehen – diese Möglichkeiten ungenutzt ließen.

So ist denn der praktische Nutzen der VDS-Regelungen eher ungewiss. Sicher dagegen ist der mit der Speicherung der Verkehrsdaten und ihrer Nutzung einhergehende Eingriff in die Freiheitsrechte nahezu der gesamten Bevölkerung, der keineswegs als grundrechtliche Marginalie abgetan werden kann. Das BVerfG führte in seinem Urteil zur VDS aus, dass der damit verbundene Eingriff „grundsätzlich nicht geringer wiegt als die inhaltsbezogene Telekommunikationsüberwachung" (NJW 2010, 833 [841])."

Was den geringen Nutzen der vorgesehenen Vorratsdatenspeicherung für die Strafverfolgung und Gefahrenabwehr betrifft, ist schließlich auch insoweit auf die Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu verweisen. Da die diesbezüglichen Ausführungen in ihrer Prägnanz und Deutlichkeit für sich sprechen, werden sie nachfolgend im Volltext zitiert: [135]

„a) Geeignetheit

Erhebliche Zweifel bestehen bereits hinsichtlich der Geeignetheit der Maßnahme. Der Gesetzentwurf begründet die Notwendigkeit der Regelung mit „der zunehmenden Be-

[135] Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten v. 9.6.2015, Seite 4 ff.

deutung der Telekommunikation für die Vorbereitung und Begehung von Straftaten"[136]*, benennt aber gleichzeitig explizit Umgehungsmöglichkeiten, die dazu führen, nicht von der Speicherung erfasst zu werden. Er zeigt somit selbst die Wege auf, wie Telekommunikation auch nach Einführung des Gesetzes hervorragend für die Vorbereitung und Begehung von Straftaten genutzt werden kann.*

Durch die in der Begründung zu § 113a TKG-E nunmehr offiziell bestätigte Ausnahme von Callshops, Internet-Cafés und öffentlich zugänglichen Telefon- oder W-LAN-Angeboten in Restaurants oder Hotels[137] *können sämtliche Kommunikationswege genutzt werden, ohne Spuren in den auf Vorrat gespeicherten Daten zu hinterlassen. Außerdem sollen ebenfalls E-Mail Verkehrsdaten nicht zu den zu speichernden Daten gehören.*

Unterstellt man den Kriminellen (insbesondere denjenigen, die schwerste Straftaten verüben und die mit der Vorratsdatenspeicherung bekämpft werden sollen) nicht eine überwiegend ausgeprägt fehlende Intelligenz, dürfte sich ein Großteil der für die Strafverfolgung relevanten Korrespondenz in Zukunft auf die oben dargestellten Kommunikationswege verlagern. Die mit der Vorratsdatenspeicherung erfassten Daten werden daher zu einem noch größeren Prozentsatz solche von unbescholtenen Bürgerinnen und Bürgern sein, die keinerlei Anlass für eine strafrechtliche Verfolgung geben, als dies schon ohnehin der Fall ist.

Zwar hat das Bundesverfassungsgericht (BVerfG) in diesem Zusammenhang ausgeführt, die Möglichkeit des Unterlaufens der Speicherung im Einzelfall führe nicht zwingend zur Ungeeignetheit der Maßnahme, solange die Zweckerreichung generell gefördert wird.[138] *Hierbei legte das Gericht aber noch nicht eine Speicherpraxis zu Grunde, in der mit der E-Mail eines der meistgenutzten Telekommunikationsmittel aus der Erfassung ausgeschlossen wurde. Gegenwärtig werden pro Jahr über 500 Milliarden E-Mails (ohne Spam) verschickt.*[139] *Zudem sind möglicherweise auch Messengerdienste wie das zu Facebook gehörende WhatsApp nicht von der Speicherpflicht umfasst und können somit nicht zur Auskunftserteilung herangezogen werden (...). Gerade letzterer wird aber in Deutschland von fast 60% aller mobilen Internetnutzer verwendet.*[140] *Bereits im*

---

136 BT-Drucks. 18/5088, S. 23.

137 BT-Drucks. 18/5088, S. 42.

138 BVerfG, Urt. v. 02.03.2010 – 1 BvR 256/08.

139 http://de.statista.com/statistik/daten/studie/392576/umfrage/anzahl-der-versendeten-e-mailsin-deutschland-pro-jahr/ (zuletzt aufgerufen am 29.5.2015).

140 http://de.statista.com/statistik/daten/studie/299740/umfrage/anteil-der-whatsapp-nutzer-anallen-

Jahr 2012 hatte die Anzahl der mit Messengerdiensten verschickten Nachrichten die Anzahl der verschickten SMS überholt, Ende 2013 war die Zahl sogar doppelt so groß.[141]

Anders als vom BVerfG zu Grunde gelegt, geht es vorliegend also nicht mehr bloß um Einzelfälle, die durch das Raster fallen. Zudem muss auch kein erhöhter Aufwand wie die Beschaffung ausländischer SIM-Karten mehr betrieben werden, um der Speicherung zu entgehen. Die Nutzung der nicht von der Vorratsdatenspeicherung erfassten E-Mail ist auch bequem von der heimischen Couch aus möglich. Im Ergebnis wird bei einem dermaßen großen selbstgeschaffenen „Blindspot" auch unter der Maßgabe des BVerfG das Vorliegen einer geeigneten Maßnahme äußerst fraglich.

b) Erforderlichkeit

Die im Rahmen der Erwägung zur Geeignetheit (siehe a) oben) geäußerten Bedenken, der gewünschte Effekt einer Verbesserung der Strafverfolgung und Gefahrenabwehr werde durch den vorliegenden Gesetzentwurf nicht erreicht, verstärken sich noch, da auch die Erforderlichkeit der Maßnahme nicht hinreichend belegt wird. In der Begründung wird lediglich darauf hingewiesen, die aus betrieblichen Gründen bei den TK-Anbietern vorhandenen Daten würden in Verbindung mit den bestehenden Auskunftsrechten zu Unzulänglichkeiten bei der Strafverfolgungsvorsorge und Gefahrenabwehr führen.[142] *Grund wäre der Umstand, dass „[...] die Speicherpraxis der Erbringer öffentlich zugänglicher Telekommunikationsdienste sehr unterschiedlich ist", so dass es „[...] derzeit vom Zufall abhängig [ist], welche Daten bei einer Abfrage nach § 100g StPO abgerufen werden können"*[143]*.*

Diese Aussage ist nach meinen umfangreichen und jahrelangen Prüferfahrungen bei den TK-Anbietern nicht nachvollziehbar. So werden beispielsweise Verkehrsdaten von Telefonverbindungen zu betrieblichen Zwecken regelmäßig zwischen drei und sechs Monaten vorgehalten (siehe hierzu auch die in Anlage 3 aufgeführten Speicherfristen der einzelnen Datenverarbeitungen). Diese Notwendigkeit ergibt sich schon aus dem den Kunden zustehenden, in § 45i Absatz 1 TKG gesetzlich normierten Einspruchszeitraum von acht Wochen nach Rechnungsversand. Somit kann davon ausgegangen wer-

---

mobilen-internetnutzern-weltweit/ (zuletzt aufgerufen am 29.5.2015).

[141] http://www.heise.de/newsticker/meldung/Marktforscher-Messenger-wie-WhatsAppueberholen-die-SMS-1852549.html (zuletzt aufgerufen am 29.5.2015).

[142] BT-Drucks. 18/5088, S. 22.

[143] a.a.O.

den, dass der überwiegende Teil der zu speichernden Daten bei den TK-Anbietern – jedenfalls in dem vom Gesetzesentwurf festgelegten Zeitraum von zehn Wochen – ohnehin vorhanden ist und somit auch nach Maßgabe des geltenden Rechts für Auskünfte an die Sicherheitsbehörden zur Verfügung steht.

Eine Ausnahme hiervon bilden lediglich die den Teilnehmern zugewiesenen IP-Adressen – die grundsätzlich nur bis zu sieben Tage gespeichert werden –, Standortdaten in Form der Funkzellen sowie unter eine sogenannte Flatrate fallende netzinterne Verbindungen, die jeweils je nach System des TK-Anbieters üblicherweise zwischen 7 und 30 Tage abrufbar sind. Im Gesamtvolumen der zu speichernden Daten dürften diese aber einen eher geringen Anteil ausmachen. Im Ergebnis ist die hier angeordnete Doppelspeicherung von unzähligen Daten daher absolut unnötig.

(...)

Weitere Ausführungen zur Erforderlichkeit finden sich im Gesetzentwurf im Übrigen nicht. Dabei wäre es nicht nur wünschenswert, sondern verfassungsrechtlich geboten, dass der Gesetzgeber die Erforderlichkeit des massiven Grundrechtseingriffs belegt.[144] Dieser Darlegungslast kann vorliegend auch nicht mit dem Argument entgangen werden, das Gesetz sei noch nicht in Kraft, so dass dementsprechend auch noch keine Ergebnisse über die Auswirkungen der Vorratsdatenspeicherung vorlägen."

Dies gilt umso mehr, als der Gesetzgeber gerade nach fünf Jahren ohne Vorratsdatenspeicherung konkret dartun müsste, welche Schutzlücken nach der Aufhebungsentscheidung durch das Bundesverfassungsgericht im Jahr 2010 überhaupt entstanden sind. Außer einer Bezugnahme auf das aus der Rechtsprechung des Bundesverfassungsgerichts abgeleitete „verfassungsrechtliche Gebot einer effektiven Strafverfolgung" finden sich im Referentenentwurf dazu keine Angaben.[145]

Im Ergebnis droht aus der begehrten einstweiligen Aussetzung der angegriffenen Normen ersichtlich kein Schaden, der auch nur ansatzweise von solchem Gewicht wäre, dass er die oben dargestellten Folgen eines ungehinderten Inkrafttretens des Gesetzes einschließlich der Verletzung der Verpflichtung zur Wahrung des effektiven Vollzugs des Unionsrechts einschließlich der Unionsgrundrechte überwiegen könnte.

---

[144] BVerfG, Beschl. v. 6.6.2007 – 1 BvR 1423/07.

[145] Vgl. Graulich, vorgänge Nr. 209 (Heft 1/2015), S. 85-98.

c) Langjähriges Zuwarten des Gesetzgebers widerlegt jede Dringlichkeit

Ungeachtet der vorstehenden Folgenabwägung scheidet ein überwiegendes Interesse am Vollzug der angegriffenen Normen schon allein deswegen von vornherein aus, weil der Gesetzgeber durch sein eigenes Verhalten jegliche Dringlichkeit in Bezug auf eine vorsorglich anlasslose Speicherung von Telekommunikationsverkehrsdaten widerlegt hat. Der Gesetzgeber hat, seit das Bundesverfassungsgericht §§ 113a und 113b des Telekommunikationsgesetzes in der Fassung des Artikel 2 Nummer 6 des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21.12.2007[146] mit Urteil vom 02.03.2010 für nichtig erklärt hat, mehr als fünfeinhalb Jahre, nämlich bis zum 16.10.2015, zugewartet, bis vom Deutschen Bundestag ein neues Gesetz zur Vorratsdatenspeicherung beschlossen wurde. Zudem ist in dem neuen § 150 Abs. 13 TKG vorgesehen, dass die Speicherverpflichtung und die damit verbundenen Verpflichtungen nach den §§ 113b bis 113e und 113g TKG erst mehr als 18 Monate nach Inkrafttreten des Gesetzes zu erfüllen sind.

Nach mehr als fünfeinhalb Jahren ohne Vorratsdatenspeicherung müsste der Gesetzgeber in diesem Zusammenhang konkret dartun, welche Schutzlücken nach der Aufhebungsentscheidung durch das Bundesverfassungsgericht im Jahr 2010 überhaupt entstanden sind und weshalb deren Wiedereinführung nunmehr in irgendeiner Weise dringlich sein sollte. Außer einer Bezugnahme auf das aus der Rechtsprechung des Bundesverfassungsgerichts abgeleitete „verfassungsrechtliche Gebot einer effektiven Strafverfolgung“ finden sich im Referentenentwurf dazu jedoch keine Angaben.[147]

Der Gesetzgeber hat also aus freien Stücken darauf verzichtet, über einen Zeitraum von insgesamt mehr als sieben Jahren eine Vorratsspeicherung von Telekommunikationsverkehrsdaten vorzuschreiben und begründet weder deren Wiedereinführung noch eine Dringlichkeit derselben; vielmehr widerlegt er letztere durch sein langjähriges Zuwarten. Dies ist umso beachtlicher, als der Gesetzgeber hierbei über einen Zeitraum von mehr als vier Jahren – nämlich von der Entscheidung des Bundesverfassungsgerichts am 02.03.2010 bis zur Entscheidung des Europäischen Gerichtshofs am 08.04.2014 – sogar ein Umsetzungsdefizit in Bezug auf die Richtlinie 2006/24/EG in Kauf genommen hat.[148]

---

[146] Bundesgesetzblatt Teil I, Seite 3198.

[147] Vgl. Graulich, vorgänge Nr. 209 (Heft 1/2015), S. 85-98.

[148] Vgl. hierzu ausführlich Rößner, EuZW 2014, 134.

Vor dem Hintergrund dieses Verhaltens des Gesetzgebers, der sich auch insoweit und im vorliegenden Zusammenhang an seinem eigenen Verhalten – also nicht nur an seinem Handeln, etwa an den von ihm getroffenen Regelungen (wie vorliegend den Ausnahmen in Bezug auf die Speicherung von Daten der Verbindungen der Telefonseelsorge), sondern auch an seinem Unterlassen (wie hier dem langjährigen Zuwarten mit einer Neuregelung) – messen und festhalten lassen muss und aus dessen Sicht die Wiedereinführung der Vorratsspeicherung von Telekommunikationsverkehrsdaten offenkundig nicht eilbedürftig war, kann keinerlei Dringlichkeit in Richtung eines kurzfristigen Inkrafttretens des angegriffenen Gesetzes angenommen werden. Angesichts dieses langjährigen Zuwartens des Gesetzgebers kann daher die Aussetzung der angegriffenen Normen selbst dann, wenn sich das Hauptsacheverfahren wie dasjenige hinsichtlich der Vorgängerregelung (1 BvR 256/08) über einen Zeitraum von mehr als zwei Jahren erstrecken sollte, aus Sicht des nationalen Rechts keinerlei Bedenken begegnen. Dies gilt umso mehr, wenn die Aussetzung aus unionsrechtlicher Sicht zwingend geboten ist.

3.) Entscheidung des Senats vom 06.10.2015 zum Tarifvertragsgesetz

Die vorstehenden Erwägungen und Umstände, insbesondere die unionsrechtliche Dimension sowie das langjährige Zuwarten des Gesetzgebers, wodurch dem Gesetzesvollzug nicht nur von vornherein jegliche Dringlichkeit fehlt, sondern dieser zur Wahrung des effektiven Vollzugs des Unionsrechts zwingend zu unterbleiben hat, unterscheiden die vorliegende Konstellation auch von vornherein grundlegend von dem Fall, der der Entscheidung des Senats vom 06.10.2015 im Hinblick auf den Erlass einer einstweiligen Anordnung in Bezug auf das Tarifvertragsgesetz zugrunde lag.[149]

Anders als dort verstößt die Bundesrepublik Deutschland mit Inkrafttreten des angegriffenen Gesetzes offensichtlich und unmittelbar gegen zwingende Vorgaben des Unionsrechts.

Anders als dort ist hier maßgeblich zu berücksichtigen, dass das bloße Inkrafttreten des angegriffenen Gesetzes eine irreparable und besonders schwerwiegende Verletzung von Grundrechten der Antragsteller darstellt – und zwar nicht nur von deutschen Grundrechten, sondern insbesondere auch von Unionsgrundrechten.

[149] BVerfG, Beschl. v. 6.10.2015 – 1 BvR 1571/15.

Anders als dort – und auch das ist vorliegend von maßgeblicher Bedeutung – hat der Gesetzgeber sogar unter Inkaufnahme eines Umsetzungsdefizits in Bezug auf die Richtlinie 2006/24/EG von mehr als vier Jahren über einen Zeitraum von mehr als fünfeinhalb Jahren mit seinem Gesetzesvorhaben zugewartet.[150]

Anders als dort ist gegenwärtig bereits eindeutig erkennbar, dass die Antragsteller wie auch die gesamte Bevölkerung der Bundesrepublik Deutschland im Zeitraum bis zur Entscheidung in der Hauptsache gravierende, kaum revidierbare und irreversible Nachteile erleiden werden, weil sie bereits durch das bloße Inkrafttreten des Gesetzes, nämlich dadurch beeinträchtigt werden, dass sie die Speicherung der Daten dann jederzeit zu gewärtigen haben.

Denn die mit dem Inkrafttreten des angegriffenen Gesetzes einhergehende Speicherpflicht gilt unmittelbar und unbedingt. Soweit diesbezüglich eine Implementierungsphase vorgesehen ist, stellt deren Ende den spätestmöglichen Zeitpunkt der Erfüllung dieser Speicherpflicht durch die Telekommunikationsunternehmen dar. Gleichwohl – dies sei nochmals betont – gilt die Verpflichtung zur Speicherung vom ersten Tage an. Diese Verpflichtung korrespondiert zudem mit einer ebenfalls unmittelbar mit Inkrafttreten des Gesetzes einsetzenden Berechtigung zur Speicherung durch die Telekommunikationsunternehmen, die somit ab diesem Zeitpunkt ohne weiteres jederzeit mit der Speicherung beginnen müssen und können. Insbesondere müssen die Telekommunikationsunternehmen nicht abwarten, bis die Bundesnetzagentur den Anforderungskatalog gemäß § 113f TKG veröffentlicht hat, da diese Vorschrift lediglich eine Vermutungsregel im Hinblick auf die Einhaltung des zu gewährleistenden Standards der Datensicherheit und Datenqualität darstellt.

Ein Abwarten mit der einstweiligen Außervollzugsetzung der angegriffenen Normen etwa bis zu dem Zeitpunkt, bis das erste Telekommunikationsunternehmen die kommende Speicherpflicht konkret erfüllt, ist schon allein deswegen nicht zumutbar, weil dieser Zeitpunkt völlig unbestimmt ist, insoweit auch keine Verpflichtung zur öffentlichen Bekanntmachung besteht und somit für die Antragsteller wie auch das Bundesverfassungsgericht gänzlich im Ungewissen liegt, wann die einzelnen verpflichteten Diensteanbieter konkret mit der Speicherung der Daten beginnen.

Im Übrigen hat – hierauf sei in diesem Zusammenhang nochmals hingewiesen – das Bundesverfassungsgericht in einer insoweit vergleichbaren Konstellation in Bezug auf die Vor-

[150] Vgl. hierzu ausführlich Rößner, EuZW 2014, 134.

gängerregelung (Verfahren 1 BvR 256/08) im Jahre 2008 kein Hindernis gesehen, den Gesetzesvollzug schon in einem frühen Stadium der Umsetzungsphase kurz nach Inkrafttreten des Gesetzes (teilweise) auszusetzen. Es ist nicht ersichtlich, dass das Bundesverfassungsgericht hierbei darauf abgestellt hätte, ob bereits Daten auf Vorrat gespeichert und Abrufe der gespeicherten Daten getätigt wurden.

V. Vorlage an den Gerichtshof der Europäischen Union

1.) Vorlagepflicht

Sollte das Bundesverfassungsgericht der Auffassung sein, dass sich aus der Entscheidung des Europäischen Gerichtshofs vom 08.04.2014[151] nicht mit hinreichender Klarheit ergibt, dass die angegriffenen Vorschriften gegen Unionsrecht verstoßen, namentlich mit Art. 7, 8, 11, 15 und 20 der Grundrechtecharta unvereinbar sind, und sie daher schon allein aus diesem Grunde einstweilen auszusetzen sind und sich darüber hinaus aufgrund des nationalen Rechts daran gehindert sehen, die begehrte einstweilige Anordnung zu erlassen, wäre es zur Wahrung des effektiven Vollzugs des Unionsrechts mit Blick auf die genannte Rechtsprechung des Europäischen Gerichtshofs[152] jedenfalls dazu verpflichtet, das Verfahren auf Erlass einer einstweiligen Anordnung auszusetzen und ein Vorabentscheidungsverfahren vor dem Europäischen Gerichtshof durchzuführen.

Denn gemäß Art. 267 AEUV hat ein innerstaatliches Gericht, bei dem ein Rechtsstreit über das Unionsrecht anhängig ist und dem dessen Sinn oder Reichweite nicht klar ist, die Pflicht, dem Gerichtshof Fragen nach der Auslegung der fraglichen Bestimmung des Unionsrechts vorzulegen, wenn dessen Entscheidungen selbst nicht mehr mit Rechtsmitteln des innerstaatlichen Rechts angefochten werden können.[153]

---

[151] EuGH, Urt. v. 8.4.2014 – C-293/12 und C-594/12.

[152] EuGH, Urt. v. 26.2.2013 – C-617/10.

[153] EuGH a.a.O., mit Hinweis auf EuGH, Urt. v. 6.10.1982, Cilfit u. a., 283/81, Slg. 1982, 3415.

Nach der Rechtsprechung des Europäischen Gerichtshofs steht das Unionsrecht einer Gerichtspraxis entgegen, die die Verpflichtung des nationalen Gerichts, Vorschriften, die gegen ein durch die Charta der Grundrechte der Europäischen Union garantiertes Grundrecht verstoßen, unangewendet zu lassen, davon abhängig macht, dass sich dieser Verstoß klar aus den betreffenden Rechtsvorschriften oder der entsprechenden Rechtsprechung ergibt, da sie dem nationalen Gericht die Befugnis abspricht – gegebenenfalls in Zusammenarbeit mit dem Gerichtshof der Europäischen Union – die Vereinbarkeit dieser Bestimmung mit der Charta umfassend zu beurteilen.[154]

2.) Vorlagefragen

Konkret wären dem Europäischen Gerichtshof hierbei folgende Fragen vorzulegen:

1. Ist eine nationale Regelung, die die Vorratsspeicherung von Daten der elektronischen Kommunikation vorschreibt und

   - die in umfassender Weise alle Personen betrifft, die elektronische Kommunikationsdienste nutzen, ohne dass sich jedoch die Personen, deren Daten auf Vorrat gespeichert werden, auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte, und also auch für Personen gilt, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte,

   - die zwar zur Bekämpfung schwerer Kriminalität beitragen soll, aber keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit verlangt und insbesondere die Vorratsspeicherung weder auf die Daten eines bestimmten Zeitraums und/oder eines bestimmten geografischen Gebiets und/oder eines bestimmten Personenkreises beschränkt, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnten;

[154] EuGH a.a.O.

- die lediglich Ausnahmen dahingehend vorsieht, dass Daten von Diensten der elektronischen Post sowie Daten, die den Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen zugrunde liegen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit besonderen Verschwiegenheitsverpflichtungen unterliegen, nicht gespeichert werden dürfen, aber darüber hinaus keinerlei Ausnahme vorsieht, so dass sie auch für sämtliche sonstigen Personen gilt, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen,

mit dem in Art. 7 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta) verankerten Recht auf Privatleben, mit dem in Art. 8 der Charta verankerten Recht auf Schutz personenbezogener Daten, mit dem in Art. 11 der Charta verankerten Recht auf Freiheit der Meinungsäußerung, mit der in Art. 15 der Charta verankerten Berufsfreiheit sowie mit dem in Art. 20 der Charta verankerten allgemeinen Gleichheitssatz vereinbar?

2. Ist eine nationale Regelung, die die Vorratsspeicherung von Daten der elektronischen Kommunikation vorschreibt, in Anbetracht der von Herrn Edward Snowden enthüllten Überwachungstätigkeiten von Nachrichtendiensten und anderen Behörden insbesondere der USA, die im Rahmen der von ihnen praktizierten massenhaften und wahllosen Überwachung und Erfassung weltweit und auch in der Europäischen Union auf Daten und Inhalte der elektronischen Kommunikation zugreifen, ohne dass die Unionsbürger insoweit einen wirksamen Anspruch auf rechtliches Gehör haben oder in irgendeiner Form benachrichtigt werden, und deren Zugriff auf die aufgrund der vorgeschriebenen Vorratsspeicherung gespeicherten Daten der elektronischen Kommunikation nicht ausgeschlossen werden kann,

derzeit mit dem in Art. 7 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta) verankerten Recht auf Privatleben, mit dem in Art. 8 der Charta verankerten Recht auf Schutz personenbezogener Daten, mit dem in Art. 11 der Charta verankerten Recht auf Freiheit der Meinungsäußerung, mit der in Art. 15 der Charta verankerten Berufsfreiheit sowie dem in Art. 47 der Charta verankerten Recht auf effektiven Rechtsschutz vereinbar?

Carl Christian Müller, LL.M.
Rechtsanwalt
Fachanwalt für Urheber- und Medienrecht

Sören Rößner, LL.M.
Rechtsanwalt