BUNDESRECHTSANWALTSKAMMER

Stellungnahme Nr. 32/2015
September 2015

Zum Gesetzentwurf der Fraktionen der CDU/CSU und SPD, Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (BT-Drucks. 18/5088)

Mitglieder des Verfassungsrechtsauschusses

RA Prof. Dr. Christian Kirchberg, Vorsitzender
RA Dr. Christian-Dietrich Bracher
RAuN Prof. Dr. Wolfgang Kuhla
RA Prof. Dr. Christofer Lenz
RA Dr. Michael Moeskes
RA Prof. Dr. Michael Quaas
RA Dr. iur. h.c. Gerhard Strate
RA und Notar Prof. Dr. Bernhard Stüer
RA Prof. Dr. Michael Uechtritz (Berichterstatter)

Mitglieder des Strafrechtsausschusses

RA Prof. Dr. Dr. Alexander Ignor, Vorsitzender
RA Dr. Jan Bockemühl (Mitberichterstatter)
RA Prof. Dr. Alfred Dierlamm
RA Thomas C. Knierim (Berichterstatter)
RA Dr. Daniel M. Krause
RA Prof. Dr. Holger Matt
RAin Anke Müller-Jacobsen
RA Prof. Dr. Tido Park
RA Prof. Dr. Reinhold Schlothauer
RA Dr. Jens Schmidt
RAin Dr. Anne Wehnert
RAin Dr. Annette von Stetten

RA Prof. Dr. Ralf Neuhaus

RA Frank Johnigk, Bundesrechtsanwaltskammer

Verteiler: Bundesministerium der Justiz
Rechtsausschuss des Deutschen Bundestages
Arbeitskreise Recht der Bundestagsfraktionen
Landesjustizminister/Justizsenatoren der Länder
Rechtsanwaltskammern
Bundesverband der Freien Berufe
Bundesnotarkammer
Bundessteuerberaterkammer
Deutscher Steuerberaterverband
Wirtschaftsprüferkammer
Institut der Wirtschaftsprüfer
Deutscher Anwaltverein
Deutscher Notarverein
Deutscher Richterbund
Deutscher Juristinnenbund
Bundesvorstand Neue Richtervereinigung
Redaktionen der NJW, Strafverteidiger, Neue Zeitschrift für Strafrecht, ZAP Verlag, Zeitschrift für höchstrichterliche Rechtsprechung im Strafrecht, Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht, wistra - Zeitschrift für Wirtschafts- und Steuerstrafrecht

Inhaltsverzeichnis

Die Bundesrechtsanwaltskammer ist die Dachorganisation der anwaltlichen Selbstverwaltung. Sie vertritt die Interessen der 28 Rechtsanwaltskammern und damit der gesamten Anwaltschaft der Bundesrepublik Deutschland mit etwa 163.000 Rechtsanwältinnen und Rechtsanwälten gegenüber Behörden, Gerichten und Organisationen – auf nationaler, europäischer und internationaler Ebene.

A. Sachverhalt

Der Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten („Vorratsdatenspeicherung“) geht davon aus, dass Verkehrsdaten ein wichtiges Hilfsmittel für die staatlichen Behörden für eine effektive Strafverfolgung ist. Art. 2 des Entwurfs sieht daher die Einfügung der §§ 113a bis 113g in das TKG vor. Art. 1 des Entwurfs enthält Änderungen der Strafprozessordnung, mit denen die Erhebung der bei den Telekommunikationsdienstleistungsanbietern gespeicherter Daten geregelt wird. Durch Art. 5 wird eine Änderung des Strafgesetzbuches herbeigefügt. Mit § 202d StGB soll ein neuer Straftatbestand der Datenhehlerei eingeführt werden. Im Einzelnen:

- § 113b TKG-E stellt die Kernregelung des Entwurfs dar. Nach dessen Absatz 2 werden die Erbringer öffentlich zugänglicher Telefondienste verpflichtet, die bei der Telekommunikation anfallenden Verkehrsdaten (Rufnummern oder eine andere Kennzeichnung der beteiligten Anschlüsse, Zeitpunkt und Dauer des Anrufs, Angaben zu dem genutzten Dienst, wenn im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden, für den Bereich der Mobiltelefonie die internationalen Kennzeichnungen der beteiligten mobilen Teilnehmer und der beteiligten Endgeräte, im Bereich der Internettelefonie die Internetprotokoll-Adressen des Anrufenden und des angerufenen Anschlusses sowie die zugewiesenen Benutzerkennungen) zu speichern. Nach § 113b Abs. 4 TKG-E sind bei Mobilfunk auch die Standortdaten des Anrufenden und des angerufenen Anschlusses bei Beginn der Verbindung zu speichern. Die Erbringer öffentlich zugänglicher Internetzugangsdienste sollen zur Speicherung von IP-Adressen einschließlich Zeitpunkt und Dauer der Vergabe einer IP verpflichtet werden (§ 113b Abs. 3 TKG-E). Nicht zulässig ist die Speicherung des Inhalts der Kommunikation. Gemäß § 113b Abs. 1 TKG-E muss die Speicherung im Inland erfolgen.

- Hinsichtlich der Speicherfrist differenziert § 113b TKG-E: Diese beträgt für Standortdaten vier Wochen, für die Verkehrsdaten 10 Wochen. Nach § 113b TKG-E hat der zur Datenspeicherung Verpflichtete sicherzustellen, dass die aufgrund der Speicherpflicht gespeicherten Daten durch technische und organisatorische Maßnahmen nach dem Stand der Technik gegen unbefugte Kenntnisnahme und Verwendung geschützt werden. Hierzu macht § 113g TKG-E Vorgaben für zusätzliche Aufnahmen in das Sicherheitskonzept nach § 109 Abs. 4 TKG.

- Ein Speicherungsverbot gilt nach § 113b Abs. 6 TKG-E i.V.m. § 99 Abs. 2 TKG nur für Verkehrsdaten, die sich auf Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen beziehen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten. Verkehrsdaten, die sich auf nach § 53 StPO zeugnisverweigerungsberechtigten Personen, also auch auf Rechtsanwälte, beziehen, sind nicht von der Speicherpflicht ausgenommen. Sie dürfen von den Behörden aber nicht erhoben werden und unterliegen darüber hinaus einem Verwendungsverbot (§ 100g Abs. 4 StPO-E).

- Art. 1 enthält Änderungen der Strafprozessordnung, mit denen die Erhebung der gespeicherten Daten geregelt wird. Nach § 100g Abs. 2 StPO-E dürfen die gespeicherten Verkehrsdaten nur erhoben werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine der im Gesetzentwurf enumerativ aufgeführten besonders schweren Straftaten begangen hat. Der Abruf von Verkehrsdaten bedarf richterlicher Zulassung. Eine Eilkompetenz der Staatsanwaltschaft besteht nicht (§ 101a Abs. 1 Satz 2 StPO-E i.V.m. § 100b Abs. 1 Satz 2 und 3 StPO). Die Beteiligten der Telekommunikation sind – soweit kein Geheimhaltungsgebot besteht – von der Erhebung zu unterrichten.

- Durch Art. 1 Ziff. 6 soll der neue Straftatbestand der Datenhehlerei in § 160a Abs. 4 StPO als Ausnahmegrund von der grundsätzlichen Unverwertbarkeit der Informationen von Seelsorgern, Berufsgeheimnisträgern, Ärzten und Medienvertretern eingeführt werden. Weiter soll gem. Art. 1 Nr. 8 der Schutz dieses Personenkreises vor strafprozessualen Maßnahmen aufgehoben werden, wenn der Verdacht einer Täterschaft oder Teilnahme an der Datenhehlerei besteht. Strafverfolgungsbehörden sollen deswegen bei einem einfachen Verdacht von der Vereidigung absehen (§ 60 Nr. 2 StPO), Zeugenbeistände zurückweisen (§ 68b Abs. 1 S. 4 StPO), schriftliche und elektronische Mandats- und Patienteninformationen bei Seelsorgern, Berufsgeheimnisträgern, Ärzten und Medienvertretern beschlagnahmen (§ 97 Abs. 2 S. 3 StPO), bei jedermann eine richterlich anzuordnende Durchsuchung durchführen (§ 102 StPO) sowie Strafverteidiger von der Verteidigung ausschließen (§ 138a Abs. 1 Nr. 3 StPO) können.

- Der Straftatbestand der Datenhehlerei (§ 202a StGB-E) soll die Strafbarkeit aller Arten von Hehlereihandlungen mit rechtswidrig aus einer Vortat erlangten geschützten Daten zur eigenen Bereicherung, zur Bereicherung Dritter oder zur Schädigung Anderer einführen. Die Verfolgung soll als relatives, nicht vererbliches Antragsdelikt ermöglicht werden (§ 205 Abs. 1 S. 2, Abs. 2 S. 1 StGB-E). Von der Strafbarkeit sollen gem. § 202b Abs. 3 StGB-E nur Handlungen ausgenommen worden, die „*ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten*“ dienen. Als einzigen Anwendungsfall nennt der Referentenentwurf den behördlichen Einsatz solcher Daten für Besteuerungszwecke, für ein Strafverfahren oder ein Bußgeldverfahren. Eine „*berufliche Pflicht*“ soll nach der Entwurfsbegründung die Vorbereitung einer journalistischen Veröffentlichung sein. Im Übrigen sollen Ausnahmen parallel zu der Regelung bei der Verbreitung kinderpornographischer Schriften (§ 184b Abs. 5 StGB) auf wenige Anwendungsfälle beschränkt bleiben.[1]

  Ausweislich des allgemeinen Teils der Begründung soll mit dem jetzt vorgelegten Entwurf den Anforderungen des Bundesverfassungsgerichts aus dem Urteil vom 2. März 2010[2] an die Sicherheit der Daten sowie an deren Übermittlung ebenso Rechnung getragen, wie den Anforderungen, die der EuGH in seinen Urteilen vom 8. April 2014[3] aus Art. 7 und 8 GRCh abgeleitet hatte. Den Ausführungen in der Gesetzesbegründung kann entnommen werden, dass nach Einschätzung der Verfasser des Entwurfs dieser nicht nur an den verfassungsrechtlichen Maßgaben des GG sondern auch an den grundrechtlichen Garantien der GRCh zu würdigen ist.

[1] BT-Drs. 18/5088, S. 52 f.
[2] BVerfGE 125, 260
[3] C-293/12 und C-594/12, DVBl 2014, 708

B. Rechtliche Würdigung

Vorbemerkung:

Die nachfolgende Stellungnahme beschränkt sich auf die rechtliche Würdigung des vorgelegten Entwurfs. Es geht also um die Beurteilung der Verfassungskonformität und im Hinblick auf die gleichfalls zu wahrenden Vorgaben aus Art. 7 und 8 der GRCh (dazu sogleich näher unten II.) um die Vereinbarkeit mit europäischem Primärrecht. Dabei werden für die verfassungsrechtliche Prüfung die Maßstäbe zugrunde gelegt, die das Bundesverfassungsgericht in seinem Urteil vom 2. März 2010[4] aufgestellt hat. Entsprechendes gilt für die Prüfung, ob eine unverhältnismäßige Beschränkung der Art. 7 und 8 der GRCh gegeben ist. Diese Frage ist auf Basis der Rechtsprechung des EuGH vom 8. April 2014 (die allerdings – wie aufzuzeigen ist – erheblichen Interpretationsbedarf ausgelöst hat)[5] zu beantworten. Die Stellungnahme enthält sich einer verfassungs*politischen* Bewertung einer Vorratsdatenspeicherung.

I. Verfassungsrechtliche Bedenken

Nach Auffassung der Bundesrechtsanwaltskammer bestehen durchgreifende Zweifel an der Verfassungskonformität des Gesetzentwurfs. Darüber hinaus begegnet der Entwurf Bedenken im Hinblick auf eine unverhältnismäßige Einschränkung der Gewährleistungen aus Art. 7 und 8 der Europäischen GRCh. Bezüglich der verfassungsrechtlichen Bedenken werden zunächst unter Ziff. I. 1. und 2. grundsätzliche Bedenken gegen den vorliegenden Entwurf genannt. Eine Befassung mit Einzelregelungen folgt unter Ziff. I. 3. Unter Ziff. II. wird auf Einwendungen eingegangen, die sich aus der GRCh ergeben.

1. Grundsätzliche Bedenken gegen die Zulässigkeit der anlasslosen Vorratsdatenspeicherung

Nach Auffassung der Bundesrechtsanwaltskammer bestehen grundsätzliche Zweifel, ob die anlasslose Vorratsdatenspeicherung, die mit dem vorliegenden Gesetzentwurf (erneut) eingeführt werden soll, den Anforderungen an eine verhältnismäßige Beschränkung des Art. 10 Abs. 1 GG genügt.

a) Die geplanten Regelungen zur Speicherung und Verwertung der Kommunikationsdaten greifen in den Schutzbereich des Art. 10 Abs. 1 GG ein. Art. 10 Abs. 1 GG gewährleistet das Telekommunikationsgeheimnis, welches die Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs vor einer Kenntnisnahme durch die öffentliche Gewalt schützt. Dieser Schutz erfasst nicht nur die Inhalte der Kommunikation. Geschützt ist vielmehr auch die Vertraulichkeit der näheren Umstände des Kommunikationsvorgangs, zu dem insbesondere gehört, ob, wann und wie oft zwischen welchen Personen oder Telekommunikationseinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist.[6]

   Bereits in dem vorstehend zitierten Urteil des Bundesverfassungsgerichts aus dem Jahr 2010 hat das Bundesverfassungsgericht angenommen, dass eine den Dienstanbietern von Telekommunikationsleistungen auferlegte Speicherung der Telekommunikationsverkehrsdaten

[4] BVerfGE 125, 260
[5] Urteile vom 8. April 2014 – C-293/12 und C-594/12 – DVBl 2014, 708
[6] Ständige Rechtsprechung des Bundesverfassungsgerichts, vgl. nur BVerfGE 125, 260, Rn. 189 (juris), m.w.N.

in das Telekommunikationsgeheimnis eingreift. Entsprechendes wurde für die im seinerzeitigen Gesetz enthaltenen Regelungen zur Datenübermittlung angenommen. Dabei hat das Bundesverfassungsgericht betont, schon in der vorsorglich anlasslosen und systematischen Datenspeicherung (und nicht erst und allein in deren späterer Verwendung) liege ein besonders schwerer Grundrechtseingriff.[7]

Es nimmt an, es handle sich um einen Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kenne.[8]

Diese Einschätzung entspricht derjenigen des EuGH in Bezug auf Eingriffe in die in Art. 7 und 8 der GRCh verankerten Grundrechte durch die Richtlinie 2006/24/EG, mit der die Mitgliedsstaaten verpflichtet wurden, den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder den Betreibern eines öffentlichen Kommunikationsnetzes eine Vorratsdatenspeicherung aufzugeben.[9]

b) Ungeachtet der vom Bundesverfassungsgericht und vom EuGH konstatierten Schwere des Eingriffs verfolgt der Gesetzgeber mit der hier zu beurteilenden Regelung legitime Zwecke, die einen Eingriff in das Telekommunikationsgeheimnis grundsätzlich rechtfertigen können. Dies hat das Bundesverfassungsgericht hinsichtlich der mit einer Vorratsdatenspeicherung angestrebten Effektivierung der Strafverfolgung und der Gefahrenabwehr grundsätzlich anerkannt. Dabei hat das Bundesverfassungsgericht auch ausdrücklich betont, eine illegitime Zielsetzung ergebe sich nicht schon daraus, dass die Telekommunikationsverkehrsdaten *anlasslos* vorsorglich gespeichert werden sollten. Eine vorsorglich anlasslose Datenspeicherung ist allerdings nur ausnahmsweise zulässig. Sie unterliegt sowohl hinsichtlich ihrer Begründung als auch hinsichtlich ihrer Ausgestaltung, insbesondere auch in Bezug auf die vorgesehenen Verwendungszwecke, besonders strengen Anforderungen.[10]

Diese Einschätzung entspricht auch derjenigen des EuGH hinsichtlich der Einschränkung der Rechte aus Art. 7 und 8 der GRCh durch die unionsrechtlichen Vorgaben zur Einführung einer Vorratsdatenspeicherung.

c) Zweifel bestehen aber an der *Geeignetheit* der Regelungen des vorliegenden Gesetzentwurfs.

aa) Soweit in der Diskussion über eine Vorratsdatenspeicherung allgemein bzw. in Äußerungen zum vorliegenden Entwurf die Eignung der Regelung zur Verfolgung der angestrebten Zwecke grundsätzlich mit dem Hinweis in Zweifel gezogen wird, es gebe keine belastbaren Nachweise dafür, dass eine Vorratsdatenspeicherung geeignet sei, die Aufklärungsquoten bei Straftaten zu erhöhen,[11] dürften derartige Bedenken (wohl) nicht durchgreifen. Entsprechendes gilt für den Einwand, terroristische Anschläge im EU-Ausland, und zwar auch in derartigen Staaten, bei denen eine Vorratsdatenspeicherung eingeführt worden sei (Beispiel Frankreich), belegten die mangelnde Eignung einer derartigen Maßnahme zur Gefahrenabwehr. Das Bundesverfassungsgericht hat in

[7] BVerfGE 125, 260, Rn. 190 (juris).
[8] BVerfGE 125, 260, Rn. 210 (juris).
[9] EuGH, Urt. vom 08.08.2014 – C-293/12 und C-594/12 –, DVBl 2014, 708, 709.
[10] BVerfGE 125, 260, Rn. 206 (juris). Auch wenn das BVerfG die europarechtliche Vorgabe einer anlasslosen sechsmonatigen Datenspeicherung auf Vorrat gerade noch für verfassungskonform hielt, um u.a. eine Vorlage an den EuGH zu vermeiden, kann nicht davon ausgegangen werden, dass es nun ohne Richtlinie seine 2010 geäußerte Auffassung aufgibt oder modifiziert.
[11] Dies geschieht meist unter Verweis auf das Gutachten des Max-Planck-Instituts zu möglichen Schutzlücken durch den Wegfall der Vorratsdatenspeicherung vom Juli 2011

seinem Urteil aus dem Jahr 2010 grundsätzlich angenommen, durch eine Vorratsdatenspeicherung würden Aufklärungsmöglichkeiten geschaffen, die sonst nicht bestünden. Für die Eignung sei es ausreichend, dass der angestrebte Zweck gefördert werde.[12]

Die Annahme, die Einführung einer Vorratsdatenspeicherung sei erst dann zulässig, wenn gesicherte empirische Erkenntnisse darüber vorlägen, ob mit einer flächendeckenden Vorratsdatenspeicherung das Ziel der Gefahrenabwehr unter Strafverfolgung überhaupt „*erreicht*“ werden könne,[13] dürfte den Maßstab, den das Bundesverfassungsgericht für die Zulässigkeit des hier in Rede stehenden Grundrechtseingriffs zugrunde gelegt hat, verfehlen. Zu bedenken ist allerdings, dass seit der Aufhebung der seinerzeitigen Regelungen zur Vorratsdatenspeicherung im Jahr 2010 durch das Bundesverfassungsgericht – soweit ersichtlich – keinerlei belastbare Erkenntnisse darüber gewonnen wurden, dass wegen des Wegfalls der Möglichkeiten einer anlasslosen Vorratsdatenspeicherung Lücken auf dem Gebiet der Strafverfolgung und/oder der Gefahrenabwehr deutlich geworden wären.

Das Argument, dass zur Verfolgung besonders schwerer Gesetzesverletzungen eine Speicherung der Verkehrsdaten der Gesamtbevölkerung im Inland erforderlich sei, um das jeweilige Täter- und Begünstigungsumfeld solcher besonders schwerer Straftaten wirksam bekämpfen zu können, steht in einem krassen Missverhältnis der Häufigkeit solcher Taten nach der polizeilichen Kriminalstatistik, der Aufklärungsquote und dem Anteil der Bevölkerung, der durch die Neuregelung betroffen sein wird. Nach der Klärung der Tat- und Tätertypologie gehört zur Annahme fehlender aber erfolgversprechender Zugriffe auf Verkehrsdaten der Vergangenheit eine empirisch gestützte Analyse der Wahrscheinlichkeit einer Aufklärung oder wenigstens ein begründeter Nachweis der Effizienzsteigerung von Ermittlungen auf diesem Gebiet. Liegt eine solche empirisch basierte Analyse nicht vor, sind alle Regelungen, die eine anlasslose Datenspeicherung aller Verkehrsdaten vorsehen, der Ausdruck eines Generalverdachts gegen die Bevölkerung.

bb) Bedenken gegen die Eignung der Maßnahme werden aber – nach Auffassung der Bundesrechtsanwaltskammer in überzeugender Weise – in der Stellungnahme der Bundesbeauftragten für den Datenschutz und Informationsfreiheit[14] geäußert.

Die Bundesbeauftragte verweist auf die Begründung des Entwurfs zu § 113a TKG-E, mit der die Ausnahmen von Call Shops, Internet-Cafes und öffentlich zugänglichen Telefon- oder W-LAN-Angeboten in Restaurants oder Hotels bestätigt werde. Auf diese Weise könnten Kommunikationswege genutzt werden, ohne Spuren in den auf Vorrat gespeicherten Daten zu hinterlassen.

cc) Ferner sollen nach der Vorstellung des Gesetzgebers auch E-Mail-Verkehrsdaten nicht zu den zu speichernden Daten gehören. Diese Auffassung äußert – allerdings ohne

[12] BVerfGE 125, 260, Rn. 207 (juris).
[13] So die Stellungnahme des Deutschen Anwaltsvereins zum Referentenentwurf des Bundesministeriums der Justiz und Verbraucherschutz für ein Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherpflicht für Verkehrsdaten, Mai 2015
[14] Stellungnahme der Bundesbeauftragten für den Datenschutz und Informationsfreiheit zum Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

Erläuterung, aus welchen Regelungen des Entwurfs dies abgeleitet wird – auch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit.[15]

Nach Auffassung der Bundesrechtsanwaltskammer bestehen Zweifel, ob eine derartige Absicht dem Text des Gesetzentwurfs mit hinreichender Deutlichkeit entnommen werden kann. Gestützt wird die Annahme, E-Mails seien von der Speicherung ausgenommen, auf § 113b Abs. 5 TKG-E, wonach nicht nur der Inhalt der Kommunikation Daten über aufgerufene Internetseiten, sondern auch *Daten von Diensten der elektronischen Post* nicht gespeichert werden dürfen.

Nach § 113b Abs. 3 TKG-E soll der Erbringer öffentlich zugänglicher Internetzugangsdienste die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse, eine eindeutige Kennung des Anschlusses sowie eine zugewiesene Benutzerkennung, Datum und Uhrzeit von Beginn und Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse unter Angabe der zugrundeliegenden Zeitzone speichern. Zu den Daten der elektronischen Post gehört aber auch die Internetprotokoll-Adresse des Absenders bzw. Teilnehmers der E-Mail-Versendung. Wenn aber bei Aufbau und Nutzung einer Internetverbindung nicht definiert ist, wozu diese verwendet wird, ist unklar, wie die Speicherung von Daten des E-Mail-Verkehrs ausgeschlossen werden soll.

dd) Unterstellt man, dass nach dem Gesetzentwurf die Speicherung von E-Mail-Verkehrsdaten tatsächlich unzulässig ist und geht man weiter davon aus, dass Derartiges, auch nach Vorstellung der Bundesregierung, ausscheiden muss, weil eine eventuelle Speicherung von E-Mail-Daten eine – nochmalige – erhebliche Intensivierung des Eingriffs in Art. 10 Abs. 1 GG bewirken würde, dann ergeben sich hieraus Bedenken gegen die Eignung des Gesetzentwurfs.

Die Bundesbeauftragte nimmt an, unterstelle man den Kriminellen (insbesondere solchen, die schwerste Straftaten verüben)

> *„nicht eine überwiegend ausgeprägt fehlende Intelligenz, dürfte sich ein Großteil der für die Strafverfolgung relevanten Korrespondenz in Zukunft auf die … dargestellten Kommunikationswege verlagern.“*

Basierend auf dieser plausiblen Annahme folgert die Bundesbeauftragte weiter, dass die mit der Vorratsdatenspeicherung erfassten Daten zu einem noch größeren Prozentsatz solche von unbescholtenen Bürgerinnen und Bürgern seien, die keinerlei Anlass für eine strafrechtliche Verfolgung gäben. Die Bundesbeauftragte verkennt in ihrer Stellungnahme nicht, dass das Bundesverfassungsgericht bereits in seinem Urteil aus dem Jahr 2010 auf entsprechende Möglichkeiten für Kriminelle hingewiesen und weiter angenommen hat, dies könne der Geeignetheit einer solchen Regelung nicht entgegengehalten werden. Zutreffend verweist die Bundesbeauftragte,[16] mit dieser Äußerung aber darauf, seinerzeit habe das Gericht nicht eine Speicherpraxis zugrunde gelegt, in der mit der E-Mail eines der meist genutzten Telekommunikationsmittel aus der Erfassung ausgeschlossen werde. Zudem seien möglicherweise auch Messenger-Dienste wie das zu Facebook gehörende WhatsApp nicht von der Speicherpflicht umfasst. Hieraus zieht die Bundesbeauftragte die Schlussfolgerung, bei einem

[15] Stellungnahme der Bundesbeauftragten, S. 4.
[16] Stellungnahme, S. 4 f.

dermaßen großen selbstgeschaffenen „blind spot“ sei auch unter Berücksichtigung der Maßgaben des Bundesverfassungsgerichts das Vorliegen einer geeigneten Maßnahme „*äußerst fraglich*“.

ee) Diese Bewertung verdient nach Auffassung der Bundesrechtsanwaltskammer Zustimmung. Auch wenn es grundsätzlich der Rechtsprechung des Bundesverfassungsgerichts entspricht, dass eine in grundrechtlich gesicherte Freiheiten eingreifende Maßnahme nicht deshalb als ungeeignet (und damit unverhältnismäßig) einzustufen ist, wenn die entsprechenden Zwecke effektiver mit schärferen Maßnahmen (die intensivere Grundrechtseingriffe bewirken) verfolgt werden könnten, besteht vorliegend die Sondersituation, dass für einen zentralen Teil der elektronischen Kommunikation die vorgesehene Speicherung von vornherein nicht greift. Gerade die naheliegende und einfache Möglichkeit, auf die nicht erfassten Kommunikationsmöglichkeiten auszuweichen, begründet im vorliegenden Fall gravierende Bedenken an der Geeignetheit der Maßnahme.

d) Des Weiteren bestehen – folgt man der fachkundigen Einschätzung der Bundesbeauftragten – auch Zweifel an der *Erforderlichkeit* der Maßnahme. In der Begründung zum Entwurf wird darauf verwiesen, dass eine Zugriffsmöglichkeit allein auf Daten, die aus betrieblichen Gründe bei den TK-Anbietern vorhandenen seien, mit den bestehenden Auskunftsrechten zu Unzulänglichkeiten bei der Strafverfolgung und Gefahrenabwehr führt. Grund hierfür sei der Umstand, dass die Speicherpraxis der Erbringer öffentlich zugänglicher Telekommunikationsdienste sehr unterschiedlich sei, sodass es derzeit vom Zufall abhänge, welche Daten bei einer Abfrage nach § 100g StPO abgerufen werden könnten.

Die Bundesbeauftragte hält diese Einschätzung aufgrund ihrer umfangreichen und jahrelangen Prüferfahrung bei den TK-Anbietern für nicht nachvollziehbar. Verkehrsdaten von Telefonverbindungen würden zu betrieblichen Zwecken regelmäßig zwischen drei und sechs Monaten aufgehoben. Eine Ausnahme hiervon bildeten lediglich den Teilnehmern zugewiesenen IP-Adressen, die grundsätzlich nur bis zu sieben Tagen gespeichert würden. Diese machten aber im Gesamtvolumen der zu speichernden Daten nur einen geringen Anteil aus.

Die Bundesbeauftragte verweist auf die Möglichkeit, die Speicheranordnung auf diese Datenart zu beschränken und für diese lediglich eine längere Speicherfrist festzusetzen. Diese Möglichkeit begründet Zweifel an der Erforderlichkeit der Maßnahme.

e) Selbst wenn man aber annehmen wollte, auf Basis des Maßstabs, den das Bundesverfassungsgericht in seinem Urteil aus dem Jahr 2010 zur seinerzeitigen Vorratsdatenspeicherung entwickelt habe, seien Geeignetheit und Erforderlichkeit der nunmehr geplanten Maßnahmen (noch) zu bejahen, folgt hieraus nicht, dass dies auch für die *Angemessenheit* des Eingriffs, also die Verhältnismäßigkeit, im engeren Sinne gilt. Im Rahmen der Verhältnismäßigkeitsprüfung ist nicht nur zu berücksichtigen, dass das verfolgte (grundsätzlich legitime) Ziel der Strafverfolgung und der Gefahrenabwehr wichtigen Gemeinwohlbelangen dient, die grundsätzlich geeignet sein könnten, auch den schweren Eingriff in Art. 10 Abs. 1 GG, der durch eine anlasslose Vorratsdatenspeicherung bewirkt wird, zu rechtfertigen. Aufgrund der vorstehend dargelegten Bedenken hinsichtlich Geeignetheit und Erforderlichkeit der Maßnahme wird aber deutlich, dass die Beförderung der mit der Speicherung von Telekommunikationsdaten angestrebten Zwecke (wenn überhaupt) nur in sehr beschränktem Umfang erreicht werden kann und dass eine begründete Vermutung dafür besteht, dass gerade der „Adressatenkreis“, bei dem die Berechtigung entsprechender Eingriffe

auf der Hand liegt (Straftäter bzw. potenzielle terroristische Attentäter), typischerweise nicht erfasst wird. Berücksichtigt man dies, so fällt die „Schaden/Nutzen"-Betrachtung zu Lasten des Gesetzentwurfes aus: Ein schwerwiegender Eingriff in Grundrechte von Millionen von Bürgern, die durch ihr Verhalten keinerlei Veranlassung zu einem entsprechenden Eingriff geboten haben, wird zugelassen, obwohl der „Nutzen" dieses Eingriffs nicht gegeben, zumindest aber äußerst fraglich bzw. gering ist. Eine Maßnahme mit hoher Eingriffsintensität ohne relevanten Nutzen für das mit der Maßnahme verfolgte Ziel kann nicht als angemessen und damit als verhältnismäßig eingestuft werden.

2. Kein hinreichender Schutz für Berufsgeheimnisträger

Selbst wenn man – entgegen der vorstehend vertretenen Auffassung – zu der Einschätzung gelangen wollte, die angestrebte gesetzliche Regelung stelle grundsätzlich keinen unverhältnismäßigen Eingriff in Art. 10 Abs. 1 GG dar, bedarf diese Aussage zumindest einer *Einschränkung für Berufsgeheimnisträger*, wie Ärzte, Psychotherapeuten und auch Rechtsanwälte.

a) Im Ausgangspunkt dürfte anerkannt sein, dass Telekommunikationsdaten von Berufsgeheimnisträgern wie Ärzten und Rechtsanwälten in besonderer Weise schutzwürdig sind, weil in derartigen Fällen ein entsprechend „sensibles" schutzwürdiges Vertrauensverhältnis zwischen dem Berufsgeheimnisträger und dessen Patienten/Mandanten besteht, in das durch die Erhebung von Verkehrsdaten des betreffenden Berufsträgers eingegriffen wird. So hat auch das Bundesverfassungsgericht – allerdings mit Blick auf ein in der seinerzeitigen Regelung (nur) statuiertes *Übermittlungs*verbot – in seiner Entscheidung aus dem Jahr 2010 zur seinerzeitigen Regelung über die Vorratsdatenspeicherung angemerkt, es sei verfassungsrechtlich als Ausfluß des Verhältnismäßigkeitsgrundsatzes geboten, zumindest für einen engen Kreis und auf besondere Vertraulichkeit angewiesener Telekommunikationsverbindungen ein Übermittlungsverbot vorzusehen. Dabei sei – so das Bundesverfassungsgericht – zu denken

> *„an Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit anderen Verschwiegenheitsverpflichtungen unterliegen (vgl. § 99 Abs. 2 TKG)."*[17]

Der vorliegende Gesetzentwurf greift diese Bewertung des Bundesverfassungsgericht auf und statuiert für die vom Bundesverfassungsgericht genannten Personen und Organisationen (aber auch *nur* für diese) ein grundsätzliches „*Speicherungsverbot*" – und zwar in § 113b Abs. 6 TKG-E. Daten von sonstigen Berufsgeheimnisträgern, denen im Zusammenhang mit diesen Daten nach § 53 Abs. 1 Nr. 1 bis Nr. 5 StPO ein Zeugnisverweigerungsrecht zusteht, werden nach dem Gesetzentwurf hingegen *nicht* durch ein Speicherungsverbot geschützt. Entsprechende Daten dürfen lediglich nicht abgerufen werden. Flankiert wird diese mit Blick auf Daten und Erkenntnisse aus diesem Bereich durch ein Verwertungsverbot (vgl. § 100g Abs. 4 Satz 1 und Satz 2 StPO-E).

[17] BVerfGE 125, 240, Rn. 238 (juris).

b) Diese Ausgestaltung des Schutzes von Berufsgeheimnisträgern, von dem u.a. auch Rechtsanwälte betroffen sind, ist defizitär. Sie begegnet durchgreifenden verfassungsrechtlichen Bedenken.

aa) Auch wenn das Bundesverfassungsgericht in seinem Urteil aus dem Jahr 2010 die besondere Schutzbedürftigkeit nur in Bezug auf Personen, Behörden und Organisationen aus dem sozialen oder kirchlichen Bereich aufgeführt hat, die in § 99 Abs. 2 TKG genannt sind, besteht kein ernstlicher Zweifel, dass auch bei sonstigen Berufsgeheimnisträgern wie Abgeordneten, Ärzten, Journalisten und Rechtsanwälten ein (teilweise mindestens gleichwertiges) Geheimhaltungsinteresse besteht. Aus der Tatsache, dass das Bundesverfassungsgericht in seinem Urteil aus dem Jahr 2010 nur die in § 99 Abs. 2 TKG genannten Personen bzw. Organisationen genannt hat, kann nicht im Gegenschluss auf eine geringere Schutzwürdigkeit sonstiger Berufsgeheimnisträger geschlussfolgert werden.

bb) Das im Gesetzentwurf enthaltene *Erhebungsverbot* gewährleistet keinen ausreichenden Schutz der besonders sensiblen Kommunikationsdaten von Berufsgeheimnisträgern wie Ärzten und Rechtsanwälten.[18]

So weist die zitierte Gemeinsame Stellungnahme der Bundesärzte-, Apotheken- und Psychotherapeutenkammer darauf hin, dass alle Patienten die Möglichkeiten benötigten, sich jederzeit, vor allem auch in Krisensituationen, an den Arzt oder Psychotherapeuten wenden zu können und dabei auf die *uneingeschränkte Gewährleistung der absoluten Vertraulichkeit* ihrer Gespräche vertrauen zu können. Bereits das Gefühl einer Registrierung könne eine unter Umständen überlebensnotwendige Kontaktaufnahme verhindern. Entsprechendes gilt auch für die in gleicher Weise schutzbedürftige Kommunikation zwischen Rechtsanwälten und ihren Mandanten.

cc) Das in § 100g Abs. 4 StPO-E vorgesehene Erhebungs- und Verwertungsverbot vermittelt keinen ausreichenden Schutz. Schon das Erhebungsverbot greift nicht, wenn sich der entsprechende Zugriff nicht unmittelbar gegen den Zeugnisverweigerungsberechtigten richtet, sondern gegen den Patienten bzw. den Mandanten. Werden bei diesen die entsprechenden Kommunikationsdaten erhoben, so erlangen die staatlichen Stellen ohne weiteres Kenntnis von dem fraglichen Kommunikationsvorgang, also u.a. auch darüber, ob, wann, wie oft und wie lange der Bürger mit seinem Anwalt, Arzt oder Psychotherapeuten telefoniert hat. Es gibt keine Anhaltspunkte für die Annahme, dass die Behörden im Fall einer Ermittlung gegen Dritte (die dann auch Adressat des Datenabrufs sind) regelmäßig und rechtzeitig erkennen können, dass sich die erhobenen Daten auf eine grundsätzlich geschützte Kommunikation mit einem Berufsgeheimnisträger beziehen. Verkehrsdaten sieht man nicht an, ob sie einem Berufsgeheimnisträger zuzuordnen sind. Sie werden zunächst zwangsläufig erhoben und erst in einem zweiten Schritt bei der Auswertung kann festgestellt werden, ob die Verkehrsdaten einem Berufsgeheimnisträger zuzuordnen sind. Dann aber ist genau das erhoben, was vermieden werden soll, nämlich die Tatsache einer geschützten Kommunikation eines Bürgers mit Berufsgeheimnisträgern.

[18] Vgl. in diesem Sinne auch die Gemeinsame Stellungnahme der Bundesärztekammer, der Bundespsychotherapeutenkammer und der Bundesapothekerkammer vom 10. Juli 2015; die Stellungnahme des DAV vom Mai 2015 und die Äußerung der Bundesbeauftragten, S. 15.

Angesichts dessen erweist sich also der Erhebungsschutz in § 100g Abs. 4 StPO-E als ungenügend, um die Vertraulichkeit der besonders schutzwürdigen Kommunikationsdaten zu gewährleisten.

dd) Das in § 100g Abs. 4 Satz 2 StPO-E vorgesehene *Verwendungsverbot* genügt nicht, um den vorstehend beschriebenen, durch das Gesetz ermöglichten Eingriff in die Kommunikationsdaten von Berufsgeheimnisträgern zu rechtfertigen bzw. hinsichtlich der Eingriffsintensität zu minimieren.[19]

Wenn der Umstand geschützter Kommunikation mit Berufsgeheimnisträgern erkannt wird, lässt er sich „technisch“ löschen, nicht aber in den Köpfen der Ermittler. Der Einwand, dies sei bei allen Verwertungsverboten der Fall, verkennt, dass Verwertungsverbote bisher eine Sanktion auf nicht gewünschtes rechtswidriges Verhalten darstellen, bei welchem eine andere Reaktion – wie Vermeidung rechtswidrigen Verhaltens – nunmehr unmöglich geworden ist. Bei Telekommunikationsdaten von Berufsgeheimnisträgern kann jedoch bereits die Speicherung ausgeschlossen werden, weil Telekommunikationsverbindungsdaten von Berufsgeheimnisträgern häufig aus öffentlichen Registern entnommen werden können, so z.B. bei Rechtsanwälten die im elektronischen Rechtsanwaltsverzeichnis nach § 31 Abs. 3 BRAO enthaltenen Telekommunikationsdaten, die der Rechtsanwalt der Rechtsanwaltskammer mitgeteilt hat (dazu auch unter I.6 a).

Die Strafprozessordnung und die im deutschen Strafprozess grundsätzlich anerkannte Dogmatik zu Verwertungsverboten gewährleisten keinen ausreichenden Schutz. So bestehen trotz des Verwendungsverbots in § 101 Abs. 4 Satz 2 StPO-E keine Zweifel daran, dass Kommunikationsdaten, die entgegen dem grundsätzlich bestehenden Erhebungsverbot erlangt worden sind, als Anknüpfung bzw. Anlasstatsache für weitere Ermittlungen dienen können. Die Konsequenz hieraus ist, dass letztlich die Verletzung der grundsätzlich besonders geschützten Kommunikationssphäre zwischen Arzt/Rechtsanwalt einerseits und Patient/Mandant andererseits eine entscheidende Ursache dafür setzen kann, dass es zu staatlichen Sanktionen gegenüber demjenigen kommt, der im Vertrauen auf die absolut geschützte Kommunikation mit seinem Arzt oder Rechtsanwalt elektronisch kommuniziert hat. Das Bewusstsein von dieser nicht auszuschließenden Möglichkeit stellt eine die Kommunikation behindernde Tatsache und damit eine – gravierende – Tangierung des Schutzbereichs aus Art. 10 GG dar.

Im Ergebnis stellt also der Verzicht auf ein Speicherungsverbot bei den genannten Berufsgeheimnisträgern diesen gegenüber eine Verletzung von Art. 10 Abs. 1 GG i.V.m. Art. 12 Abs. 1 GG dar. Bei den betroffenen Kommunikationspartnern (Patienten/Mandanten, Informanten) entsteht nicht nur – wie bei der Allgemeinheit – das Gefühl, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist. Vielmehr gilt dies auch für einen besonders sensiblen und folglich besonders schutzwürdigen Bereich des Privatlebens (Gesundheit bzw. Verhältnis Patient/Mandant).

[19] So auch die übereinstimmende Einschätzung in der Stellungnahme von Bundesärzte-, Apotheken- und Psychotherapeutenkammer, der Stellungnahme des DAV und der Bundesbeauftragten.

3. Verfassungsrechtliche Bewertung einzelner Regelungen des Entwurfs zur Änderung des TKG (Art. 2 des Gesetzentwurfs)

a) § 113b TKG-E

Diese Norm verpflichtet die Erbringer öffentlich zugänglicher Telekommunikationsdienste Verkehrsdaten für zehn Wochen zu speichern. Für Standortdaten beträgt die Speicherfrist vier Wochen. Dies stellt die zentrale Regelung des Entwurfs hinsichtlich der Datenspeicherung dar.

aa) Abgesehen von den oben (I. 2. Und 3.) dargelegten grundsätzlichen Bedenken gegen die anlasslose Vorratsdatenspeicherung, speziell im Hinblick auf Berufsgeheimnisträger, bestehen – wegen der sogleich zu erläuternden Eingriffsintensität – spezifische Bedenken bezüglich der *Speicherung der Standortdaten* nach § 113b Abs. 4 TKG-E. Die Regelung sieht vor, im Fall der Nutzung mobiler Telefondienste auch die bei Beginn einer mobilen Verbindung genutzte Funkzelle zu erfassen. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit weist darauf hin, dass in Deutschland über 45 Mio. Menschen ein Smartphone und somit mobile Verbindungen nutzen. Grundsätzlich sei ein Smartphone im eingeschalteten Zustand immer online, sodass eine Unterbrechung der Verbindung lediglich bei einem Netzverlust oder dem bewussten Ausschalten des Smartphones erfolgen würde. Tatsächlich gäbe es aber viele weitere Gründe für eine Kappung und den Neuaufbau einer mobilen Verbindung. Genannte werden beispielsweise der Wechsel von einer schnellen LTE-Verbindung zu einer langsameren UMTS-Verbindung oder die Verbindung mit einem WLAN-Netz, die einen Neuaufbau der Datenverbindung erforderlich mache. Gerade derartige Wechsel fänden in der Praxis sehr häufig statt, insbesondere, wenn sich der Nutzer des Smartphones bewege.[20]

Hieraus folgert die Bundesbeauftragte, dass in derartigen – durchaus typischen – Fällen jeweils für vier Wochen die Erstellung *engmaschiger Bewegungsprofile* ermöglicht werde. Die Annahme in der Gesetzesbegründung, dass grundsätzlich nur einzelne Standortdaten abgerufen werden sollten, um keine überflüssigen Bewegungsprofile zu erstellen, werde in der Praxis kaum greifen. Die Vorratsdatenspeicherung soll insbesondere dazu dienen, Ermittlungsansätze im Umfeld einer begangenen oder drohenden schweren Straftat zu liefern. Es sei daher eher unwahrscheinlich, dass die oben genannten Ausnahmen vom Grundsatz in der praktischen Anwendung tatsächlich die Regel darstellen würden.[21]

bb) Folgt man dieser – nach Auffassung der Bundesrechtsanwaltskammer richtigen – Einschätzung, dann wird jedenfalls in Bezug auf die Standortdaten die gesteigerte Intensität des Eingriffs deutlich: Die technische bestehende und in vielen Fällen naheliegende Möglichkeit „*engmaschige Bewegungsprofile*“ zu erstellen, stellt einen Eingriff in die grundrechtliche Freiheitssphäre dar, die über die bloße Erfassung des „Ob“, „Wann“ und der Dauer der Kommunikation hinausgeht. Auch bezüglich dieses Eingriffs gelten wiederum die bereits oben (B. I. 1. e)) dargelegten Bedenken: Angesichts des beschränkten Nutzens der entsprechenden Eingriffe (wegen der naheliegenden Annahme, dass Straftäter oder potenzielle Terroristen ein Kommunikationsverhalten an den Tag legen werden, das von der gesetzlich geregelten Erhebungs- und Speicherpflicht nicht erfasst wird) stellt sich die Frage nach der Angemessenheit einer derartig weitreichenden Eingriffsmöglichkeit, die durch § 113b Abs. 4 TKG-E geschaffen wird. Jedenfalls wird durch diese Möglichkeit das Gefühl,

[20] Stellungnahme, S. 21 f.
[21] Stellungnahme, S. 22.

dass das Privatleben der Betroffenen Gegenstand einer ständigen Überwachung ist, um die Komponente „Kenntnis des jeweiligen Aufenthaltsortes“ erweitert.

cc) Keine Bedenken dürften gegen die gesetzlich vorgesehene Dauer der Speicherung bestehen. Abgesehen von Zweifeln, ob die Dauer der Speicherung überhaupt ausreichend ist, um eine effektive Nutzung der gespeicherten Daten für Strafverfolgungszwecke zu ermöglichen,[22] bewegt sich der Gesetzgeber mit den im Gesetz vorgesehenen Fristen innerhalb des Rahmens, den das Bundesverfassungsgericht in seiner Entscheidung aus dem Jahr 2010 genannt hat. In diesem Urteil hatte das Bundesverfassungsgericht keine Bedenken gegen die Anordnung einer sechsmonatigen Speicherungspflicht von Telekommunikationsdaten.

4. Verfassungsrechtliche Bewertung einzelner Regelungen des Entwurfs zu Änderungen der Strafprozessordnung (Art. 1)

a) § 100g StPO-E (Erhebung von Verkehrsdaten)

§ 100g StPO-E enthält Vorgaben zur *Erhebung* der anlasslos gespeicherten Verkehrsdaten. Statthaft ist gemäß § 100g Abs. 2 StPO-E die Erhebung der Verkehrsdaten zum Zwecke der Strafverfolgung, wenn bestimmte Tatsachen den Verdacht einer schweren Straftat begründen. Ein abschließender Katalog dieser „schweren“ Straftat findet sich in § 100g Abs. 2 StPO-E. Dabei geht der Gesetzgeber davon aus, dass nur „*besonders schwere Straftaten*“ eine Datenerhebung rechtfertigen. Mit dieser Formulierung geht der Gesetzgeber über die Anforderungen hinaus, die das Bundesverfassungsgericht in seiner Entscheidung im Jahr 2010 zur seinerzeitigen gesetzlichen Regelung der Vorratsdatenspeicherung aufgestellt hatte. Das Bundesverfassungsgericht hatte insoweit nur einen Katalog von „*schweren Straftaten*“ gefordert.

Da sich der Katalog des § 100g Abs. 2 StPO-E grundsätzlich an der Entscheidung des Bundesverfassungsgerichts zum sogenannten „Großen Lauschangriff“ orientiert, wonach der Strafrahmen einen maßgeblichen Hinweis auf die Schwere der Straftat liefert,[23] dürfte der Katalog von § 100g Abs. 2 StPO-E grundsätzlich unbedenklich sein. Insoweit ist zu berücksichtigen, dass der durch die Datenerhebung bewirkte Eingriff in seiner Intensität hinter dem, der in der Form des „Großen Lauschangriffs“ erfolgt, zurückbleibt, sodass ein Abstellen auf Straftaten, bei denen das Ermittlungsinteresse einen „Großen Lauschangriff“ rechtfertigen kann, im Ausgangspunkt geeignet ist, eine Erhebung der gespeicherten Vorratsdaten zu rechtfertigen.

Zur Präzisierung der Anforderungen an das Vorliegen einer „besonders schweren Straftat“ hat das Bundesverfassungsgericht den Grundsatz aufgestellt, die besondere Schwere sei anzunehmen, wenn sie mit einer höheren Höchststrafe als fünf Jahre Freiheitsstrafe bewehrt sei. Bis auf eine Ausnahme (§ 184c Abs. 2 StGB, gewerbs- oder bandenmäßige Verbreitung, Erwerb und Besitz jugendpornografischer Schriften) ist diese Voraussetzung bei dem Katalog des § 100g Abs. 2 StPO-E erfüllt. Selbst wenn man bezüglich dieses Straftatbestandes aber annehmen wollte, hierbei handle es sich „nur“ um eine schwere, nicht aber eine „*besonders schwere*“ Straftat, bestünden keine verfassungsrechtlichen Bedenken, da – wie bereits ausgeführt – das Bundesverfassungsgericht in seiner Entscheidung zur Vorratsdatenspeicherung (anders als bei seiner Entscheidung zum „großen Lauschangriff“) das Vorliegen einer schweren Straftat grundsätzlich als ausreichend ansieht.

[22] Zweifel äußert insoweit die Stellungnahme des Deutschen Richterbundes vom Mai 2015
[23] BVerfGE 109, 279, 347

b) Die Verschwiegenheit der Rechtsanwälte ist für deren Mandanten von existenzieller Bedeutung. Die vorgesehene Speicherpflicht von Verkehrsdaten darüber, wer, wann, von welchem Stand aus und wie lange mit dem Strafverteidiger und Rechtsanwalt seines Vertrauens kommuniziert hat, durchbricht diese Verschwiegenheit. Damit widerspricht die Regelung dem verfassungsrechtlichen Gebot, das Verhältnis zwischen dem rechtsuchenden Bürger und dem Beistand und Schutz gewährenden Strafverteidiger und Rechtsanwalt unbeobachtet und unangetastet zu lassen (BVerfGE 109, 279, 322; BVerfG Beschl. v. 30.04.2007 – 2 BvR 2151/06 – Rz. 22 (El Masri)). Dieser Vertrauensschutz ist eine Ausprägung des Menschenrechts auf eine freie Lebensgestaltung und hat wenigstens die gleiche Qualität wie die kirchliche und die freie Seelsorge oder Notrufberatung.

c) Das Argument, es sei angeblich unmöglich, Telekommunikationsanschlüsse von Rechtsanwälten zu identifizieren, die von vornherein aus der Speicherpflicht ausgenommen werden könnten, überzeugt nicht. Eine solche Identifizierung ist den verpflichteten Telekommunikationsanbietern genauso gut möglich wie bei den von der Speicherpflicht ausgenommenen Seelsorge- und Notrufeinrichtungen. Die Ausnahmen erstrecken sich nicht nur auf bestimmte Nummernkreise in der Telekommunikation, sondern sind weitergehend auch von Eigenangaben der jeweiligen Anschlussinhaber abhängig. Im laufenden Vertragsverhältnis kann den Telekommunikationsbetreibern ohne weiteres zugemutet werden, ihre Kunden nach Merkmalen über den Berufsgeheimnisschutz zu befragen und diese Merkmale dann als Ausschlusskriterium für die Vorratsdatenspeicherung zu verwenden. Im Übrigen kann sich der Telekommunikationsanbieter bei Vertragsabschluss oder Vertragsänderung einen von den Rechtsanwaltskammern ausgestellten Anwaltsausweis vorzeigen lassen.

d) Weiter wäre es möglich, Daten aus dem elektronischen Rechtsanwaltsregister der Bundesrechtsanwaltskammer mit denen der Telekommunikationsanbieter abzugleichen. Die Telekommunikationsunternehmen müssten ohnehin täglich die Höchstspeicherfrist überprüfen und alle Verbindungs- und Standortdaten, bei denen die Höchstspeicherfrist abgelaufen ist, löschen. An diese tägliche Fristenprüfung könnten die bei der BRAK dokumentierten Anschlussdaten der Rechtsanwälte und Kammermitglieder durch einen entsprechenden Datenaustausch angekoppelt werden, so dass der ohnehin eingerichtete Löschungsalgorithmus des Telekommunikationsanbieters nur um eine Datenabfrage bei der BRAK ergänzt werden müsste.

e) Jedenfalls kann auch erwogen werden, anstelle der Nichterfassung eine sofortige Löschung der Daten durch die täglich vorzusehende Löschungsroutine bei den Telekommunikationsanbietern vorzusehen. Da die Telekommunikationsbetreiber spätestens monatlich in eine vertragsbezogene Kommunikation durch die Rechnungsstellung (bspw. auch zu Werbezwecken) eintreten, können im laufenden Vertrag mit einer einfachen Abfrage solche Merkmale erfasst werden.

5. Der Schutz der anwaltlichen Kommunikation kann bei anlasslos gespeicherten Verkehrsdaten zu Abrufzwecken (gem. §§ 113a ff. TKG-E) nicht ausreichend durch die strafprozessualen Verwertungs- und Verwendungsschranken des § 160a StPO geleistet werden.

a) Bereits mit der anlasslosen Speicherung von Verkehrsdaten zu Abrufzwecken ist der Schutz der Verschwiegenheit durchbrochen, denn bereits mit der Speicherung wird eine für die abrufende Stelle undifferenzierte Abruffähigkeit eröffnet, die ein nicht hinnehmbares Missbrauchspotential entfaltet. Ob nämlich eine befugt abrufende Stelle die in § 160a Abs. 1

StPO normierten Grenzen standardmäßig bereits mit der Erlangung solcher Daten beachtet, oder eine Ermittlungstätigkeit solange entfaltet, bis auf einen konkreten Hinweis oder Widerspruch hin, „zufällig“ oder „überraschend“ bekannt wird, dass die für die Ermittlungen genutzten Verkehrsdaten einer geschützten Telekommunikation mit einem Strafverteidiger, Rechtsanwalt oder einem anderen Kammermitglied zugeordnet ist, steht nicht von vornherein fest. Wahrscheinlich ist ein vorsorgliches „Aussortieren“ durch die Strafverfolgungsbehörden auf keinen Fall, weil sie nach der jetzt vorgeschlagenen Regelung unterschiedslos alle Daten abrufen und die damit gelegten Spuren weiter verfolgen dürfen.

b) Der Verweis auf das strafprozessuale Verwertungsverbot und die Begrenzung der Weiterverwendung von Daten in einem konkreten Ermittlungsverfahren gem. § 160a StPO ist im Übrigen ein schwacher Trost. Selbst wenn sich nachträglich herausstellt, dass bei dieser Arbeit nicht verwertbares Grundlagenmaterial verwendet wurde, ist der Umstand, dass eine Kommunikation zwischen Mandant und Berufsgeheimnisträger stattgefunden hat, nachträglich nicht mehr aus den Köpfen der Ermittler zu entfernen. Die Ermittler wissen zum einen um diese Kommunikation, denn sie befassen sich - auf den Hinweis hin - mit deren Verwertbarkeit. Zum anderen können die mittelbar aus diesem Wissen erworbenen Ermittlungsergebnisse ohne weiteres weiter verwertet werden, wenn diese Ergebnisse nicht vom Schutzbereich des § 160a StPO erfasst werden.

c) Dem kann nicht entgegen gehalten werden, dass nach dem geltenden Recht eine Abrufbarkeit von Daten, die für Abrechnungszwecke vorgehalten werden (§§ 96 ff. TKG), sowieso mit den bisherigen Eingriffsmaßnahmen der Verfassungsschutz-, Sicherheits- und Strafverfolgungsbehörden erreicht werden kann. Zum einen setzt dieser Abruf ebenfalls einen konkreten Verdacht voraus. Zum anderen entwickelt sich in der Praxis ein Verfahren dieser Behörden nicht entlang von Verkehrsdaten ohne Berufszuordnung als Spurenlage, sondern entlang anderer Anhaltspunkte, die in der Regel den Behörden zuerst Kenntnis vom vorhandenen und gebotenen Schutz des beruflichen Strafverteidiger- und Rechtsanwaltsgeheimnisses verschafft. Das schränkt schon von vornherein den Zugriff auf solche Daten ein.

b) § 101a StPO-E

Vorgaben hinsichtlich des Richtervorbehalts für die Datenverwendung und hinsichtlich der *Information des Betroffenen (Transparenz),* die das Bundesverfassungsgericht in seiner Entscheidung aus dem Jahr 2010 bezüglich einer Vorratsdatenspeicherung aufgestellt hat, sind in § 101a StPO-E enthalten.

aa) Durch § 101a Abs. 1 StPO-E i.V.m. § 100b Abs. 1 bis Abs. 4 StPO ist festgelegt, dass Vorratsdaten ausschließlich aufgrund einer richterlichen Anordnung erhoben werden. Eine Erhebung ohne richterliche Anordnung, insbesondere bei Gefahr in Verzug, ist ausdrücklich ausgeschlossen (vgl. § 101a StPO-E i.V.m. § 100b Abs. 1 Satz 2 und 3 StPO). Insoweit genügt der vorliegende Gesetzentwurf den Anforderungen des Bundesverfassungsgerichts.[24]

[24] So auch die Stellungnahme des Wissenschaftlichen Dienstes des Deutschen Bundestages zur Umsetzung der Vorgaben des Bundesverfassungsgerichts zur Vorratsdatenspeicherung durch den Gesetzentwurf der Bundesregierung vom 27. Mai 2015, WD 3-3000-108/15 vom 9. Juni 2015.

bb) Bedenken bestehen aber bezüglich der Regelungen des § 101a Abs. 6 StPO-E über die Information des Betroffenen. Das Bundesverfassungsgericht hatte in seiner Entscheidung aus dem Jahr 2010 gefordert, der Gesetzgeber müsse den Zugriff auf Verkehrsdaten als grundsätzlich offene Maßnahme ausgestalten. Dementsprechend sei der Betroffene vor der Abfrage bzw. Übermittlung seiner Daten grundsätzlich zu benachrichtigen. Eine heimliche Verwendung der Daten dürfe nur vorgesehen werden, wenn sie im Einzelfall erforderlich und richterlich angeordnet sei.[25]

Nach § 101a Abs. 6 StPO-E sind die Betroffenen **von** der Erhebung der Verkehrsdaten nach § 100g StPO-E zu benachrichtigen. Eine eindeutige Umsetzung der Vorgabe des Bundesverfassungsgerichts, dass der Betroffene regelmäßig **vor** der Datenabfrage bzw. der Übermittlung seiner Daten zu unterrichten ist, findet sich im Gesetz also nicht.[26]

Da in der Begründung zum Gesetzentwurf ausdrücklich darauf hingewiesen wird, dass das über die Datenverwendung entscheidende Gericht nach § 33 StPO dem Betroffenen vor seiner Entscheidung Gelegenheit zum rechtlichen Gehör geben müsse, kann unterstellt werden, dass hiermit der Anforderung des Bundesverfassungsgerichts genügt werden soll. In der vorliegenden Situation handelt es sich um eine Entscheidung des Richters außerhalb der Hauptverhandlung, die nach § 33 Abs. 2 StPO zunächst nur nach schriftlicher oder mündlicher Erklärung der Staatsanwaltschaft ergeht. Da nach § 33 Abs. 3 StPO bei einer solchen Entscheidung ein anderer Beteiligter zu hören ist, bevor zu seinem Nachteil Tatsachen oder Beweisergebnisse, zu denen er noch nicht gehört worden ist, verwertet werden, dürfte – soweit nicht im Ausnahmefall das Gebot der Geheimhaltung eingreift – den Anforderungen des Bundesverfassungsgerichts genügt sein. Allerdings erschließt sich nicht, warum in § 101 Abs. 6 StPO-E zur Vermeidung von Unklarheiten nicht von einer Benachrichtigung „*vor*“ der Erhebung die Rede ist.[27]

In *rechtspraktischer Hinsicht* dürfte – wie in der Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit dargelegt wird –[28] die vorherige Anhörung entgegen der Vorstellung des Bundesverfassungsgerichts den Ausnahmefall darstellen. Die Vorratsdatenspeicherung soll Spurenansätze liefern oder Strukturermittlungen ermöglichen. Gerade in derartigen Fällen ist schwerlich damit zu rechnen, dass die Ermittlungsbehörden ihre Ermittlungen offen legen werden, da dies typischerweise den Ermittlungserfolg gefährden dürfte. Dies verdeutlicht, dass die Transparenz bei der Datenerhebung realistischer Weise wohl in der Mehrzahl der Fälle nicht zum Tragen kommen wird, so dass die Regelung des § 101 Abs. 6 StPO-E (abgesehen von den Zweifeln an der Normenklarheit) grundsätzlich nicht den Anforderungen des Bundesverfassungsgerichts genügt, da dies eine vorherige Benachrichtigung „*grundsätzlich*“, also im Regelfall, gefordert hat und nur dann gegen eine heimliche Verwendung der Daten keine Bedenken hat, wenn diese im Einzelfall erforderlich ist und richterlich angeordnet wird.[29]

---

[25] BVerfGE 125, 240, Rn. 243 (juris).
[26] Dazu kritisch die Stellungnahme des Wissenschaftlichen Dienstes des Deutschen Bundestages, WD 3-3000-108/15, S. 18 und die Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, S. 18.
[27] In der Stellungnahme des Wissenschaftlichen Dienstes des Bundestags WD 3-3000-108/15, S. 18, werden daher auch Bedenken im Hinblick auf die Normklarheit der Regelung des § 101a Abs. 6 StPO-E geäußert.
[28] Stellungnahme, S. 18
[29] BVerfGE 125, 240, Rn. 243 (juris).

6. § 202d StGB („Datenhehlerei"), Art. 5

Abzulehnen ist auch die Einschränkung des Berufsgeheimnisschutzes für Verteidiger, Rechtsanwälte und Zeugenbeistände durch Hinzunahme des Straftatbestandes der „Datenhehlerei" in die Vorschriften, die ausnahmsweise einen Zugriff auf das Berufsgeheimnis oder den Ausschluss von der beruflichen Tätigkeit im Strafverfahren erlauben (Art. 1 Nrn. 6, 8 des Referentenentwurfs zu §§ 97, 138a und 160a StPO).

d) Während im geltenden Recht die Durchbrechung des Berufsgeheimnisschutzes einen qualifizierten Verdacht einer „Verstrickung" von Verteidigern und Rechtsanwälten in die eigentlich verfolgte Haupttat durch Offizialdelikte der Beteiligung, Begünstigung, Strafvereitelung oder Hehlerei geht, soll nach dem Referentenentwurf in Zukunft auch das neue Antragsdelikt der Datenhehlerei (§ 202d StGB-E) einen Ermittlungszugriff auf Strafverteidiger- und Rechtsanwaltsdokumentationen rechtfertigen. Normiert werden soll eine Strafbarkeit für den Besitz, die Weitergabe und Verwertung von Daten, die von einem anderen rechtswidrig erlangt wurden, in Bereicherungs- oder Schädigungsabsicht. Eine Drittbereicherung soll ausreichen. Der weite und umfassende Tatbestand des § 202d Abs. 1 StGB-E wird sodann in Absatz 3 durch einen Rechtfertigungsgrund begrenzt, der „Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher und beruflicher Pflichten dienen", von der Strafbarkeit ausnehmen will. Indem die vorgesehene doppelte Prüfung einer „Ausschließlichkeit" sowie der „Rechtmäßigkeit" die Möglichkeiten stark beschränken, in denen sich der vom Vorwurf betroffene Strafverteidiger oder Rechtsanwalt erst bei Bekanntgabe des Vorwurfs rechtfertigen kann und muss, stellt die in Art. 1 Nrn. 6, 8 des Referentenentwurfs vorgesehene Aufnahme der Datenhehlerei in den Ausnahmekatalog einen eigenständigen gravierenden Eingriff in den grundgesetzlichen Berufsgeheimnisschutz dar. Dass bereits ein Antragsdelikt mit geringer Strafdrohung ausreichen soll, das Berufsgeheimnis zu durchbrechen, ist ein außerordentlicher Misstrauensbeweis gegen die Funktionsfähigkeit der Rechtspflege und in die Funktion des Rechtsanwalts als Organ der Rechtspflege.

e) Durch die vorgesehene Ausweitung der Ausschlussgründe würden nicht nur alle Strafverteidiger und Rechtsanwälte einem erhöhten Strafverfolgungsrisiko ausgesetzt sein in Fällen, in denen Mandanten wegen der Entwendung nicht allgemein zugänglicher Daten oder wegen Datenhehlerei verdächtig sind. Es ist praktisch nicht vorstellbar, einen Mandanten zu beraten oder zu verteidigen, der wegen solcher Delikte verfolgt wird, ohne in Kontakt mit etwaigen Materialien über den Inhalt des Vorwurfs zu kommen. Schon die Übergabe solcher Daten an den Verteidiger oder beratenden Rechtsanwalt könnte tatbestandsmäßig sein. Es darf dem Verteidiger oder beratenden Rechtsanwalt aber nicht unterstellt werden, dass er beabsichtigt, sich an solchen Delikten des Mandanten zu beteiligen oder sie zu unterstützen.

f) In der Praxis der Ermittlungsverfahren ist es regelmäßig den Strafverfolgungsbehörden verborgen, welche inhaltlichen Gespräche zwischen einem Strafverteidiger oder Rechtsanwalt geführt, welche Dokumentationen angelegt und inwieweit durch die Mandatsführung auch Erkenntnisse über Dritte recherchiert werden, die dem Mandatszweck dienen. Beispielsweise gehört es zu den Aufgaben des Verteidigers, sich im Vorfeld einer gerichtlichen Hauptverhandlung über Mitangeklagte, Zeugen und Sachverständige zu informieren. Derartige Recherchen können dem Verteidigungszweck dienen, sind aber ohne Einverständnis des Mandanten nicht den Strafverfolgungsbehörden vorzeitig zu offenbaren (sog. „eigene Erhebungen des Strafverteidigers", vgl. dazu Strafrechtsausschuss der BRAK, Thesen zur Strafverteidigung, These 25 ff. m.w.N.). Indem Strafverfolgungsbehörden ohne Kenntnis der Dokumentationen des Strafverteidigers nicht prüfen können, ob die Voraussetzungen des § 202d Abs. 3 StGB-E nach den vorgesehenen Regelungen greifen, könnten sie nach der vorgesehenen Ausweitung die

Herausgabe aller an sich geheimnisgeschützten, für Verteidigungszwecke angelegten Dokumentationen vom Strafverteidiger oder Rechtsanwalt unter Berufung allein auf den Verdacht einer illegalen Datenerlangung erzwingen. Damit würden Vertrauensverhältnisse von Strafverteidigern und Rechtsanwälten unter einen Generalverdacht gestellt.

g) Es ist auch nicht ausgeschlossen, dass ein Verdacht der Datenhehlerei entstehen könnte, wenn der Strafverteidiger zunächst in Ausübung seiner Funktion rechtmäßig Zugang zu behördlichen Akten und Datenbeständen erhält, die Daten Dritter enthalten, die ihrerseits rechtswidrig erlangt wurden. Würden derartige Akten kopiert und an den Mandanten weiter gegeben – wozu der Strafverteidiger und Rechtsanwalt im Mandatsverhältnis verpflichtet ist – könnte eine tatbestandsmäßige Handlung schon angenommen werden, wenn die Strafverfolgungsbehörden an der in § 202d Abs.3 StGB-E geregelten „Ausschließlichkeit" der Erfüllung beruflicher Pflichten zweifeln. Gesteigert wird die Gefahr einer solchen Verdachtsbegründung, wenn die Strafverfolgungsbehörde die Akten elektronisch führt oder eine elektronische Kommunikation mit Behörden und Dritten unterhalten wird, die von der Strafverfolgungsbehörde nicht als „ausschließlich" oder „rechtmäßig" den beruflichen Aufgaben des Strafverteidigers oder Rechtsanwalts zugeschrieben wird. In allen aufgezeigten Fällen würde schon ein pflichtgemäßes Verhalten die Gefahr einer unabsichtlichen Verdachtsbegründung mit sich bringen, die zur Durchbrechung des Berufsgeheimnisschutzes im Strafverfahren und zum Ausschluss des Strafverteidigers und Rechtsanwalts von der Beistandsleistung ausreichen könnte.

II. Zweifel an der Vereinbarkeit mit Unionsrecht

Der Gesetzentwurf zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten begegnet nicht nur Bedenken im Hinblick auf seine Verfassungskonformität. Vielmehr ist auch dessen Vereinbarkeit mit Unionsrecht, konkret mit Art. 7 und 8 der GRCh zweifelhaft. Die Bundesrechtsanwaltskammer weist insoweit auf folgende Gesichtspunkte hin:

1. Anwendbarkeit der Charta der Grundrechte der Europäischen Union auf die Regelungsmaterie Vorratsdatenspeicherung

Der Anwendungsbereich der Charta der Grundrechte der Europäischen Union ist nur dann eröffnet, wenn Organe oder Einrichtungen der EU oder die Mitgliedsstaaten EU-Recht, also Primär- und Sekundärrecht der EU durchführen (Art. 51 Abs. 1 GRCh). Die Frage, was in diesem Sinne „Durchführung" des EU-Rechts ist, ist seit der Akerberg Fransson-Entscheidung des EuGH[30] umstritten.[31]

Vorliegend bedarf diese Streitfrage keiner Vertiefung, da die Anwendbarkeit der Charta der Grundrechte keinen ernsthaften Zweifeln unterliegt. Die Materie der Vorratsdatenspeicherung unterfällt dem Anwendungsbereich der Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002), da es sich hierbei im Sinne von Art. 1 der Richtlinie um eine Regelung in Bezug auf die Verarbeitung

[30] Urt. v. 23.02.2013 – Rs. C-617/10

[31] Hierzu nur Thym, NVwZ 2013, S. 889; siehe auch die Ausarbeitung des Wissenschaftlichen Dienstes des Deutschen Bundestags zu den europarechtlichen Spielräumen zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten in den Mitgliedsstaaten der Europäischen Union, PE 6-3000-53/15 vom 4. Juni 2015, S. 4 ff. m.w.N.

personenbezogener Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr dieser Daten und von elektronischen Kommunikationsgeräten und -diensten handelt. Art. 15 Abs. 1 dieser Richtlinie normiert eine Öffnungsklausel für die Mitgliedsstaaten, diese Rechte zu beschränken – mit der ausdrücklichen Maßgabe, dass alle beschränkenden Maßnahmen den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich der in Art. 6 Abs. 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen müssen.

Auch im Schrifttum besteht daher – soweit ersichtlich – weitgehend Konsens, dass die Mitgliedsstaaten bei Einführung nationaler Regelungen zur Vorratsdatenspeicherung auch Unionsrecht i.S.d. Art. 51 Abs. 1 GRCh ausführen.[32]

Gegen diese Einschätzung kann auch nicht eingewandt werden, dass mit der Entscheidung des Europäischen Gerichtshof zur Nichtigkeit der Richtlinie über die Vorratsdatenspeicherung (Richtlinie 2006/24/EG) vom 8. April 2014[33] eine „Renationalisierung" des Datenschutzrechts eingetreten sei, mit der Konsequenz, dass insoweit keine unionsrechtlichen Vorgaben (mehr) existieren, deren Durchführung i.S.v. Art. 51 Abs. 1 GRCh betroffen sein könnte. Gegen diese Annahme spricht die fortdauernde Existenz der Richtlinie 2002/58/EG, die durch das Urteil des EuGH zur Richtlinie über die Vorratsdatenspeicherung nicht berührt wird.

Gestützt wird die hier vertretene Auffassung auch dadurch, dass in der Gesetzesbegründung durch Betonung der Vereinbarkeit des Entwurfs mit Art. 7 und 8 GRCh deutlich wird, dass auch der Gesetzgeber annimmt, die Neuregelungen seien an diesen unionsrechtlichen Vorgaben zu messen.

2. Konkretisierung der unionsrechtlichen Anforderungen an eine Vorratsdatenspeicherung

Aus dem zitierten Urteil des EuGH vom 8. April 2014 ergibt sich in Zusammenhang mit Art. 51 Abs. 1 GRCh, dass nationale Regelungen zur Vorratsdatenspeicherung an Art. 7 und Art. 8 GRCh zu messen sind. Dabei lassen sich diesem Urteil des EuGH Vorgaben entnehmen, die bei nationalen Regelungen über die Einführung einer Vorratsdatenspeicherung zu beachten sind.

a) Der EuGH geht davon aus, dass eine anlasslose Vorratsdatenspeicherung einen schwerwiegenden Eingriff in die Grundrechte der Unionsbürger darstellt. Dies gilt bereits für die Verpflichtung zur Speicherung, nicht erst für den nachfolgenden Zugriff der Behörden auf die gespeicherten Daten. In Anlehnung an die Judikatur des Bundesverfassungsgerichts argumentiert der EuGH mit dem „*Gefühl der ständigen Überwachung*", das durch entsprechende Regelungen hervorgerufen wird.

   Zwar räumt der EuGH ein (auch insoweit im Einklang mit dem Bundesverfassungsgericht), dass mit der Vorratsdatenspeicherung anerkannte Gemeinwohlinteressen verfolgt würden, nämlich die Bekämpfung schwerer Kriminalität und die Wahrung der öffentlichen Sicherheit. Folglich liege auch keine Verletzung der Wesensgehaltsgarantie der Art. 7 und 8 GRCh vor. Ungeachtet dessen bejaht der EuGH einen Verstoß der Vorratsdatenspeicherungsrichtlinie, weil er in dieser eine unverhältnismäßige Einschränkung von Art. 7 und Art. 8 GRCh sieht. Dabei benennt der

[32] *Bäcker*, JA 2014, 1263, 1272 und *Priebe*, EuZW 2014, 456, 458; ebenso die Stellungnahme des Wissenschaftlichen Dienstes des Bundestags PE 6-3000-53/15, S. 8.
[33] C-293/12 und C-594/12, DVBl 2014, 708 ff.

EuGH maßgeblich fünf Defizite der Richtlinie, die nach seiner Einschätzung zu deren Unverhältnismäßigkeit führen.[34]

- Gerügt wird vom EuGH, dass der Personenkreis und der Umfang der betroffenen elektronischen Kommunikation praktisch unbegrenzt seien. Alle Personen und alle elektronischen Kommunikationsmittel würden anlasslos und ausnahmslos gespeichert. Erfasst würden insbesondere auch Träger von Berufsgeheimnissen.

- Die Richtlinie enthalte keine Kriterien, die den Zugang und die spätere Nutzung zu diesem „Datenmeer" begrenzten. Insoweit fehle es an einem hinreichenden prozeduralen Grundrechtsschutz.

- Beanstandet wird weiter die pauschale Frist für die Speicherung mit erheblichen Variationsmöglichkeiten von 6 bis 24 Monaten, ohne dass in der Richtlinie eine Differenzierung nach Datenkategorien oder anderen Kriterien vorgenommen werde.

- Der EuGH vermisst weitere einen angemessenen Missbrauchsschutz und hinreichende technische und organisatorische Schutzmechanismen einschließlich entsprechender Löschungspflichten.

- Letztlich fordert der EuGH eine Speicherung im Unionsgebiet, um eine Überwachung durch Behörden der EU-Mitgliedsstaaten zu ermöglichen.

Wörtlich formuliert der EuGH dann, dass „*aus der Gesamtheit der vorstehenden Erwägungen*" zu schließen sei, dass der Unionsgesetzgeber beim Erlass der Richtlinie 2006/24/EG die Grenzen überschritten habe, die er zur Wahrung des Grundsatzes der Verhältnismäßigkeit im Hinblick auf Art. 7, 8 und 52 Abs. 1 GRCh einhalten musste.[35]

b) Im Schrifttum ist umstritten, wie „scharf" bei Erlass einer nationalen Regelung zur Vorratsdatenspeicherung der entsprechende Katalog der vom EuGH geäußerten Bedenken abzuarbeiten ist, da der EuGH die Unverhältnismäßigkeit aus der „*Gesamtheit*" der von ihm konstatierten Defizite abgeleitet hat.[36]

Unklar bleibt also, ob bereits die Verfehlung einer der vom EuGH aufgestellten Anforderungen zur Unzulässigkeit einer nationalen Regelung über eine Vorratsdatenspeicherung führt. Konsens besteht aber weitgehend dahin, dass der EuGH in seinem Urteil zur Unverhältnismäßigkeit der Richtlinie über die Vorratsdatenspeicherung *weitergehende bzw. strengere* Anforderungen aufgestellt hat, als das Bundesverfassungsgericht in dem genannten Urteil aus dem Jahr 2010, mit dem das Gericht die nationalen Regelungen zur Einführung einer Vorratsdatenspeicherung beanstandet hatte. Wohl überwiegend wird angenommen, aus dem EuGH-Urteil sei abzuleiten, dass eine anlasslose und umfassende Vorratsdatenspeicherung unzulässig sei. Die vom EuGH geltend gemachte Rüge, dass durch eine anlasslose Vorratsdatenspeicherung alle Personen erfasst würden, die elektronische Telekommunikationsdienste nutzten, ohne dass sich jedoch die Personen, deren Daten auf Vorrat gespeichert würden, auch nur mittelbar in einer Lage befänden, die Anlass zur

[34] Zum Nachfolgenden vgl. *Kühling*, NVwZ 2014, 681, 683; ähnliche *Priebe*, EuZW 2014, 456, 458.
[35] Urt. v. 08.04.2014 – C-293/12 und C.594/12 –, Rn. 69, DVBl 2014, 708, 712.
[36] Vgl. z.B. *Kühling*, NVwZ 2014, 681, 683 und *Priebe*, EuZW 2014, 456, 458.

Strafverfolgung geben könnte, ist als Vorwurf charakterisiert worden, der „*das Rückgrat einer jeden Vorratsdatenspeicherung*“ trifft.[37]

Im Einklang hiermit steht die Einschätzung, mit dem Urteil des EuGH sei die Einführung einer flächendeckenden Vorratsdatenspeicherung „*vom Tisch*“ bzw. passé.[38]

c) Die vorstehend wiedergegebenen Bewertungen sind auf Basis des Urteils des EuGH über die Richtlinie zur Vorratsdatenspeicherung nicht nur plausibel, sondern vielmehr naheliegend. Auch wenn der vorliegende Entwurf eine Reihe der vom EuGH im Zusammenhang mit der Richtlinie über die Vorratsdatenspeicherung geltend gemachten Bedenken berücksichtigt (Reglementierung der Voraussetzungen des Zugriffs, entsprechende Vorgaben zur Speicherfrist und angemessene Vorkehrungen zum Missbrauchsschutz), verbleibt es dabei, dass der zentrale Vorwurf des EuGH, ein anlasslose Vorratsdatenspeicherung betreffe die Mehrzahl der europäischen Bürger in ihrer Grundrechtsposition, ohne dass sie irgendeinen Anlass für den insoweit bewirkten Grundrechtseingriff geliefert hätten, dem Wesen jeder „Vorrats“-Datenspeicherung zuwiderläuft. Ob der EuGH bei Gewährleistung eines hinreichenden Schutzes von Personen und Institutionen, insbesondere Berufsgeheimnisträgern, zu einer anderen Bewertung kommt (wenn im Übrigen die angemahnten Vorkehrungen zur Minimierung des Eingriffs eingehalten sind), erscheint zwar nicht a limine ausgeschlossen, begegnet aber erheblichen Zweifeln.

Jedenfalls der vorliegende Entwurf, der bei der Erhebung keine Beschränkung für die Mehrheit der Träger von Berufsgeheimnissen vorsieht, genügt nicht den Anforderungen des Art. 7 und 8 GRCh, wenn man sich an den Maßstäben orientiert, die der EuGH in seiner Entscheidung über die Vorratsdatenspeicherungsrichtlinie aufgestellt hat.

- - -

[37] *Wolff*, DÖV 2014, 608, 610.
[38] So z.B. *Moos*, K&R 2014, 158, 164; *Kühling*, NVwZ 2014, 681, 683; in der Sache ebenso *Spiecker* gen. Döhman, JZ 2014, 112 und *Wolff*, DÖV 2014, 608, 610.