Universität Augsburg
Juristische Fakultät

Prof. Dr. F. Wollenschläger - Juristische Fakultät - Universität Augsburg - 86135 Augsburg

Frau Vorsitzende
des Ausschusses für Recht und Verbraucherschutz des
Deutschen Bundestages
Renate Künast, MdB
Platz der Republik 1
11011 Berlin
Per Email: rechtsausschuss@bundestag.de

Prof. Dr. Ferdinand Wollenschläger
Lehrstuhl für Öffentliches Recht, Europarecht
und Öffentliches Wirtschaftsrecht

Universitätsstr. 24
86159 Augsburg

Tel +49 (0) 821 598-4550
Fax +49 (0) 821 598-4552

ferdinand.wollenschlaeger@jura.uni-augsburg.de
www.jura.uni-augsburg.de/wollenschlaeger

Augsburg, den 17.9.2015

Öffentliche Anhörung des Ausschusses für Recht und Verbraucherschutz am 21. September 2015 / Einführung einer Speicherpflicht für Verkehrsdaten BT-Drs. 18/5088; 18/5171; 18/4971

Sehr geehrte Frau Vorsitzende,

für die Einladung zur öffentlichen Anhörung des Ausschusses für Recht und Verbraucherschutz des Deutschen Bundestages am 21.9.2015 zur Einführung einer Speicherpflicht für Verkehrsdaten danke ich. In der Anlage überreiche ich vorab die erbetene schriftliche Stellungnahme.

Mit freundlichen Grüßen

Gez. Prof. Dr. Ferdinand Wollenschläger

Prof. Dr. Ferdinand Wollenschläger

Schriftliche Stellungnahme

Öffentliche Anhörung

des Ausschusses für Recht und Verbraucherschutz

des Deutschen Bundestages

zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

– Gesetzentwurf der Fraktionen der CDU/CSU und SPD zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (BT-Drs. 18/5088) –

– Gesetzentwurf der Bundesregierung zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (BT-Drs. 18/5171) –

– Antrag der Abgeordneten Jan Korte, Dr. André Hahn, Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE. Auf Vorratsdatenspeicherung verzichten (BT-Drs. 18/4971) –

am 21. September 2015

Inhaltsübersicht*

* Ich danke meinem Mitarbeiter Lukas Krönke für seine Mitwirkung an der Stellungnahme.

I. Zusammenfassende Gesamtbewertung

Eine Speicherpflicht für Verkehrsdaten stellt angesichts Anlasslosigkeit, Streubreite und Aussagekraft der Daten einen **gewichtigen Grundrechtseingriff** dar. **Nicht minder gewichtig** sind freilich die mit ihr verfolgten **Ziele**, nämlich besonders schwere Straftaten aufzuklären und Gefahren für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes abzuwehren. Auch hierbei handelt es sich um **Anliegen von hohem Verfassungsrang**: So obliegt dem Staat nach ständiger Rechtsprechung des Bundesverfassungsgerichts die grundrechtlich und rechtsstaatlich fundierte Pflicht, eine effektive Strafverfolgung sicherzustellen und Individualrechtsgüter vor Beeinträchtigungen durch Dritte zu schützen.

Vor diesem Hintergrund hat das **Bundesverfassungsgericht** in seinem Urteil vom 2.3.2010 eine **Speicherpflicht für Verkehrsdaten** (wenn auch nicht die frühere gesetzliche Regelung) für **prinzipiell mit dem Grundgesetz** vereinbar erklärt und Anforderungen formuliert: Diese umfassen namentlich eine Höchstspeicherdauer (sechs Monate), eine Beschränkung möglicher Verwendungszwecke (überragend wichtige Aufgaben des Rechtsgüterschutzes), die Gewährleistung von Datensicherheit und Transparenz sowie einen Richtervorbehalt.

Nachdem kein Verfassungsverbot einer Speicherpflicht für Verkehrsdaten besteht, stellt deren Einführung sowie deren Ausgestaltung im Detail – bei Wahrung der skizzierten Kautelen – eine im **rechtspolitischen Gestaltungsspielraum des demokratisch legitimierten Gesetzgebers** liegende und entsprechend zu verantwortende Entscheidung dar. Die hier zu beurteilenden **Gesetzentwürfe** der Fraktionen der CDU/CSU und SPD (BT-Drs. 18/5088) sowie der Bundesregierung (BT-Drs. 18/5171) **wahren** nicht nur **die verfassungsrechtlichen Grundsatzanforderungen** (dazu und zu Klarstellungspotential II.); vielmehr schöpfen sie den vom Grundgesetz belassenen Gestaltungsspielraum des Gesetzgebers nicht aus (namentlich Höchstspeicherfrist; erfasste Verkehrsdaten; Verwendungszwecke).

Anders als mitunter angenommen lässt sich dem **Urteil des Europäischen Gerichtshofs** vom 8.4.2014 **kein Verbot der Verkehrsdatenspeicherung** entnehmen (dazu III.). Zum einen ist schon die **Anwendbarkeit der EU-Grundrechte** (und damit die Maßgeblichkeit dieses Urteils) auf eine – wie vorliegend – nicht unionsrechtlich veranlasste nationale Regelung **zweifelhaft** (siehe zum insoweit beschränkten Anwendungsbereich der EU-Grundrechtecharta deren Art. 51 Abs. 1). Zum anderen hat der EuGH die Unverhältnismäßigkeit der früheren EU-Richtlinie in **Gesamtabwägung einer Vielzahl von grundrechtlich problematisierten Umständen** ausgesprochen, ohne – wie das Bundesverfassungsgericht – zwingend zu wahrende Ein-

zelanforderungen für künftige Regelungen zu formulieren. Dies verbietet, aus im Urteil grundrechtlich problematisierten Einzelaspekten – namentlich der anlasslosen Speicherung – die Unionsgrundrechtswidrigkeit der Verkehrsdatenspeicherung zu folgern. Vielmehr ist eine erneute Gesamtabwägung anzustellen, bei der neben der Anlasslosigkeit der Speicherung als besondere Schärfe des Eingriffs die – im Vergleich zur beanstandeten EU-Richtlinie – in vielerlei Hinsicht deutlich grundrechtsschonendere Regelung in den vorliegenden Gesetzentwürfen zu berücksichtigen ist, zumal Letztere sonstigen Einwänden des EuGH Rechnung tragen. Lässt sich auch der Inhalt einer künftigen EuGH-Entscheidung nicht mit letzter Gewissheit prognostizieren, so erscheinen die **Gesetzentwürfe jedenfalls unionsgrundrechtlich vertretbar**.

Die aktuelle **Mitteilung der Europäischen Kommission** gibt Anlass zur Erörterung der Pflicht zur Datenspeicherung im Inland sowie insbesondere zum Hinweis auf den nicht hinreichend berücksichtigten Umstand, dass polizeiliche und strafprozessuale Maßnahmen der Datenerhebung nicht dem Anwendungsbereich des Unionsrechts unterliegen (dazu IV.).

II. Verfassungsrechtlicher Rahmen

Die anlasslose Speicherung von Verkehrsdaten für Zwecke der Strafverfolgung, der Gefahrenabwehr und der Aufgaben der Nachrichtendienste“ ist nach dem Urteil des Bundesverfassungsgerichts vom 2.3.2010[1] mit dem insoweit betroffenen Fernmeldegeheimnis (Art. 10 GG) grundsätzlich vereinbar, so die Ausgestaltung der gesetzlichen Regelung dem besonderen Gewicht des Eingriffs Rechnung trägt (Rn. 204 ff.):

> Materiell verfassungsgemäß sind die Eingriffe in das Telekommunikationsgeheimnis, wenn sie legitimen Gemeinwohlzwecken dienen und im Übrigen dem Grundsatz der Verhältnismäßigkeit genügen …, das heißt zur Erreichung der Zwecke geeignet, erforderlich und angemessen sind …
>
> Eine sechsmonatige anlasslose Speicherung von Telekommunikationsverkehrsdaten für qualifizierte Verwendungen im Rahmen der Strafverfolgung, der Gefahrenabwehr und der Aufgaben der Nachrichtendienste, wie sie die §§ 113a, 113b TKG anordnen, ist danach mit Art. 10 GG nicht schlechthin unvereinbar. Der Gesetzgeber kann mit einer solchen Regelung legitime Zwecke verfolgen, für deren Erreichung eine solche Speicherung im Sinne des Verhältnismäßigkeitsgrundsatzes geeignet und erforderlich ist. Einer solchen Speicherung fehlt es auch in Bezug auf die Verhältnismäßigkeit im engeren Sinne nicht von vornherein an einer Rechtfertigungsfähigkeit. Bei einer Ausgestaltung, die dem besonderen Gewicht des hierin liegenden Eingriffs hinreichend Rechnung trägt, unterfällt eine anlasslose Speicherung der Telekommunikationsverkehrsdaten nicht schon als solche dem strikten Verbot einer Speicherung von Daten auf Vorrat im Sinne der Rechtsprechung des Bundesverfassungsgerichts …
>
> Die Effektivierung der Strafverfolgung, der Gefahrenabwehr und der Erfüllung der Aufgaben der Nachrichtendienste sind legitime Zwecke, die einen Eingriff in das Telekommunikationsgeheimnis grundsätzlich rechtfertigen können … Dabei liegt eine illegitime, das Freiheitsprinzip des Art. 10 Abs. 1 GG selbst aufhebende Zielsetzung nicht schon darin, dass die Telekommunikationsverkehrsdaten anlasslos vorsorglich gesichert werden sollen. Art. 10 Abs. 1 GG verbietet nicht jede vorsorgliche Erhebung und Speicherung von Daten überhaupt, sondern schützt vor einer unverhältnismäßigen Gestaltung solcher Datensammlungen und hierbei insbesondere vor entgrenzenden Zwecksetzungen. Strikt verboten ist lediglich die Speicherung von personenbezogenen Daten auf Vorrat zu unbestimmten und noch nicht bestimmbaren Zwecken … 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.

Gegenüber der Speicherung und Verwendung vorsorglich gespeicherter Verkehrsdaten sind an Auskunftansprüche hinsichtlich der Anschlussinhaber bestimmter IP-Adressen nach Auffassung des Bundesverfassungsgerichts geringere verfassungsrechtliche Anforderungen zu stellen (Rn. 254):

> Weniger strenge verfassungsrechtliche Maßgaben gelten für eine nur mittelbare Verwendung der vorsorglich gespeicherten Daten in Form von behördlichen Auskunftsansprüchen gegenüber den Diensteanbietern hinsichtlich der Anschlussinhaber bestimmter IP-Adressen, die diese unter Nutzung der vorgehaltenen Daten zu ermitteln haben. …

Im Hinblick auf die verfassungsrechtliche Zulässigkeit der Verkehrsdatenspeicherung ist zunächst festzuhalten, dass diese nach Auffassung des Bundesverfassungsgerichts zur Effektivierung der Strafverfolgung und der Gefahrenabwehr grundsätzlich geeignet (1.) und auch erfor-

---

[1] BVerfGE 125, 260. Die im Text angegebenen Randnummern beziehen sich auf http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs20100302_1bvr025608.html (16.9.2015).

derlich ist (2.). Darüber hinaus werden die Grundsatzanforderungen des Gerichts an die Ausgestaltung einer entsprechenden gesetzlichen Regelung durch die vorliegenden Gesetzentwürfe gewahrt. Im Einzelnen betrifft dies die Vorgaben hinsichtlich der Beschränkung der Speicherpflicht (3.), der Datensicherheit (4.), der Datenlöschung (5.), der Datenverwendung (6.), des Schutzes von Berufsgeheimnisträgern (7.) sowie der Verwendung von Standortdaten (8.). Zur Gewährleistung effektiven Rechtsschutzes für die Betroffenen sehen die Entwürfe ferner einen umfassenden Richtervorbehalt (9.) sowie weitreichende Transparenzregelungen (10.) vor. Hinsichtlich dieser Punkte bestehendes Klarstellungspotential wird abschließend zusammengefasst (11.).

1. Eignung

Kritiker der Einführung einer anlasslosen vorsorglichen Speicherung von Verkehrsdaten bezweifeln bereits deren grundsätzliche Eignung zur Effektivierung von Strafverfolgung und Gefahrenabwehr.[2] Neben mangelnder Aufklärungsrelevanz wird vorgebracht, dass sich Straftäter der Speicherung ihrer Daten durch Ausweichreaktionen entziehen könnten, etwa durch die Nutzung von Call-Shops, Internetcafés oder öffentlich zugänglichen W-LAN-Angeboten[3].

Insoweit ist freilich zu berücksichtigen, dass die verfassungsrechtlichen Anforderungen an die Geeignetheit der gesetzgeberischen Maßnahme nicht zu hoch angesetzt werden dürfen. Nicht erforderlich ist insbesondere, dass durch das eingesetzte Mittel der angestrebte Zweck vollumfänglich erreicht wird, es genügt vielmehr, dass die Wahrscheinlichkeit eines teilweisen Erfolgseintritts zumindest erhöht wird.[4] Vor diesem Hintergrund hat das Bundesverfassungsgericht keine Zweifel an der Eignung der Verkehrsdatenspeicherung artikuliert (Rn. 207):

> Eine vorsorglich anlasslose Speicherung von Telekommunikationsverkehrsdaten zur späteren anlassbezogenen Übermittlung an die für die Strafverfolgung oder Gefahrenabwehr zuständigen Behörden beziehungsweise an die Nachrichtendienste darf der Gesetzgeber zur Erreichung seiner Ziele als geeignet ansehen. Es werden hierdurch Aufklärungsmöglichkeiten geschaffen, die sonst nicht bestünden und angesichts der zunehmenden Bedeutung der Telekommunikation auch für die Vorbereitung und Begehung von Straftaten in vielen Fällen erfolgversprechend sind. Unerheblich ist, ob die vom Gesetzgeber geschaffenen Regelungen in der Lage sind, lückenlos alle Telekommunikationsverbindungen zu rekonstruieren. Auch wenn eine solche Datenspeicherung nicht sicherstellen kann,

---

[2] Vgl. den Antrag der Abgeordneten Korte, Hahn, Jelpke, Kunert, Pau, Petzold, Renner, Steinke, Tempel, Wawzyniak und der Fraktion DIE LINKE, BT-Drs. 18/4971, S. 3 f.; ferner die Stellungnahme des Deutschen Anwaltvereins zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz für ein Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, 2015, S. 9 ff., abrufbar unter: http://anwaltverein.de/de/newsroom/sn-25-15-referentenentwurf-des-bundesministeriums-der-justiz-und-fuer-verbraucherschutz-fuer-ein-gesetz-zur-einfuehrung-einer-sp (16.9.2015).

[3] Vgl. die Stellungnahme der BfDI zum Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, 2015, S. 4 f., abrufbar unter: http://www.bfdi.bund.de/DE/Datenschutz/Themen/Telefon_Internet/TelefonArtikel/VoarratsdatenspeicherungReloaded.pdf;jsessionid=660B3B442D8A97CDFCDFB0F4EB17CB7A.1_cid319?__blob=publicationFile&v=3 (16.9.2015).

[4] Siehe BVerfGE 16, 147 ff. (183); E 30, 292 ff. (316); E 33, 171 ff. (187); E 67, 151 ff. (173 ff.); E 96, 10 ff. (23 ff.).

dass alle Telekommunikationsverbindungen verlässlich bestimmten Anschlussnehmern zugeordnet werden können, und etwa Kriminelle die Speicherung durch die Nutzung von Hotspots, Internetcafés, ausländischen Internettelefondiensten oder unter falschen Namen angemeldeten Prepaid-Handys unterlaufen können, kann dies der Geeignetheit einer solchen Regelung nicht entgegenhalten werden. Diese erfordert nicht, dass das Regelungsziel in jedem Einzelfall tatsächlich erreicht wird, sondern verlangt lediglich, dass die Zweckerreichung gefördert wird …

2. Erforderlichkeit

Das Bundesverfassungsgericht hielt darüber hinaus fest, dass ein milderes, in seiner Effektivität vergleichbares Mittel nicht ersichtlich sei. Insbesondere stelle das sogenannte „Quick-Freezing-Verfahren", die einzelfallbezogene Speicherung von Verkehrsdaten bei Vorliegen eines konkreten Anlasses, keine ebenso effektive Maßnahme wie die anlasslose vorsorgliche Verkehrsdatenspeicherung dar (Rn. 208):

Der Gesetzgeber darf eine sechsmonatige Speicherung der Telekommunikationsverkehrsdaten auch als erforderlich beurteilen. Weniger einschneidende Mittel, die ebenso weitreichende Aufklärungsmaßnahmen ermöglichen, sind nicht ersichtlich. Eine vergleichbar effektive Aufklärungsmöglichkeit liegt insbesondere nicht im sogenannten Quick-Freezing-Verfahren, bei dem an die Stelle der anlasslos-generellen Speicherung der Telekommunikationsdaten eine Speicherung nur im Einzelfall und erst zu dem Zeitpunkt angeordnet wird, zu dem dazu etwa wegen eines bestimmten Tatverdachts konkreter Anlass besteht. Ein solches Verfahren, das Daten aus der Zeit vor der Anordnung ihrer Speicherung nur erfassen kann, soweit sie noch vorhanden sind, ist nicht ebenso wirksam wie eine kontinuierliche Speicherung, die das Vorhandensein eines vollständigen Datenbestandes für die letzten sechs Monate gewährleistet.

Die Einführung einer anlasslosen vorsorglichen Speicherung von Verkehrsdaten darf daher zum Zwecke der Effektivierung der Strafverfolgung und der Gefahrenabwehr auch als erforderlich angesehen werden.

3. Umfang der Speicherpflicht

a) Anforderungen des Bundesverfassungsgerichts

Die Verhältnismäßigkeit der Verkehrsdatenspeicherung setzt zunächst eine wirksame Begrenzung der Speicherpflicht voraus. Dabei sind sowohl sachliche Beschränkungen hinsichtlich der Art der zu speichernden Daten zu beachten als auch eine zeitliche Obergrenze. Mit Blick auf die Art der zu speichernden Daten betonte das Bundesverfassungsgericht zunächst, dass die Speicherung nur der Verkehrsdaten – in Abgrenzung zum Inhalt der Telekommunikation – eine wirksame Eingrenzung der Speicherpflicht darstelle. In zeitlicher Hinsicht sah das Gericht eine Speicherdauer von höchstens sechs Monaten als noch mit den verfassungsrechtlichen Anforderungen vereinbar an (Rn. 215):

Eine sechsmonatige Speicherung der Telekommunikationsverkehrsdaten hebt auch nicht bereits aus sich heraus das Prinzip des Art. 10 Abs. 1 GG als solches auf; sie verletzt weder dessen Menschenwürdekern (Art. 1 Abs. 1 GG) noch dessen Wesensgehalt (Art. 19 Abs. 2 GG). Sie bleibt trotz ihrer außerordentlichen Weite noch wirksam begrenzt. So wird der Inhalt der Telekommunikation von der auf die Verkehrsdaten beschränkten Speicherung ausgespart. Auch bleibt die Speicherungsdauer zeitlich begrenzt. Zwar ist eine Speicherungsdauer von sechs Monaten angesichts des Umfangs und der Aussagekraft der gespeicherten Daten sehr lang und liegt an der Obergrenze dessen, was unter Verhältnismäßigkeitserwägungen rechtfertigungsfähig ist. Nach ihrem Ablauf kann sich der

Bürger jedoch darauf verlassen, dass seine Daten – sofern sie nicht aus gewichtigem Anlass ausnahmsweise abgerufen wurden – gelöscht werden und für niemanden mehr rekonstruierbar sind.

Die verfassungsrechtliche Zulässigkeit der anlasslosen vorsorglichen Verkehrsdatenspeicherung setzt nach Auffassung des Bundesverfassungsgerichts ferner voraus, dass auch auf die Speicherung von Daten über die von den Nutzern aufgerufenen Internetseiten verzichtet wird (Rn. 218):

Umgekehrt darf die Speicherung der Telekommunikationsverkehrsdaten nicht als Schritt hin zu einer Gesetzgebung verstanden werden, die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielte. Eine solche Gesetzgebung wäre, unabhängig von der Gestaltung der Verwendungsregelungen, von vornherein mit der Verfassung unvereinbar. Die verfassungsrechtliche Unbedenklichkeit einer vorsorglich anlasslosen Speicherung der Telekommunikationsverkehrsdaten setzt vielmehr voraus, dass diese eine Ausnahme bleibt. Sie darf auch nicht im Zusammenspiel mit anderen vorhandenen Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger führen. Maßgeblich für die Rechtfertigungsfähigkeit einer solchen Speicherung ist deshalb insbesondere, dass sie nicht direkt durch staatliche Stellen erfolgt, dass sie nicht auch die Kommunikationsinhalte erfasst und dass auch die Speicherung der von ihren Kunden aufgerufenen Internetseiten durch kommerzielle Diensteanbieter grundsätzlich untersagt ist.

b) Bewertung der Gesetzentwürfe

Die vorliegenden Gesetzentwürfe begrenzen den Umfang der Verkehrsdatenspeicherung sowohl in zeitlicher Hinsicht als auch hinsichtlich der Art der zu speichernden Daten wirksam. Gemäß § 113b Abs. 1 Nr. 1 TKG-E sind die von der Speicherpflicht umfassten Daten grundsätzlich für einen Zeitraum von zehn Wochen zu speichern. Eine hiervon abweichende Vorgabe besteht gemäß § 113b Abs. 1 Nr. 2 TKG-E für Standortdaten, für die eine Speicherung von lediglich vier Wochen vorgesehen ist. Die Gesetzentwürfe bleiben damit deutlich hinter der vom Bundesverfassungsgericht für zulässig erachteten Höchstspeicherfrist von sechs Monaten zurück.[5]

Hinsichtlich der Art der zu speichernden Daten bestimmt § 113b Abs. 5 TKG-E ausdrücklich, dass der Inhalt der Kommunikation sowie Daten über aufgerufene Internetseiten nicht gespeichert werden dürfen. Darüber hinaus untersagt die Vorschrift auch die Speicherung der Daten von Diensten der elektronischen Post. Nicht ausdrücklich geregelt ist hingegen, ob moderne Kommunikationsformen wie WhatsApp, Skype sowie Chatprogramme ebenfalls von der Speicherpflicht ausgenommen sind. § 113b Abs. 2 S 2 Nr. 1 TKG-E sieht lediglich eine Speicherpflicht bei „Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht“ vor. Die Gesetzentwürfe stoßen daher teilweise auf Kritik, da sie mit Blick auf den Umfang der Speicherpflicht

[5] Die Beschränkung der Speicherfrist auf lediglich zehn Wochen stößt aus ermittlungstechnischen Gründen vereinzelt auf Kritik, vgl. etwa die Stellungnahme des Deutschen Richterbundes zum Referentenentwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, 2015, S. 4 f.

nicht hinreichend bestimmt seien.[6] Indes sehen die Gesetzentwürfe eine Ausnahme von der Speicherpflicht ausdrücklich nur für Dienste der elektronischen Post, also – nach dem Duden – nur für die Kommunikation per E-Mail[7] vor. Demgegenüber ermöglicht die offene Formulierung des § 113b Abs. 2 S. 2 Nr. 1 TKG-E gerade auch die Erfassung moderner Kommunikationsformen und die Anpassung an aktuelle technische Entwicklungen. Von einer Einbeziehung moderner Kommunikationsangebote wie WhatsApp und Skype in die Speicherpflicht gemäß § 113b TKG-E ist daher auszugehen. Insoweit empfiehlt sich eine ausdrückliche Klarstellung (in der Gesetzesbegründung). Verfassungsrechtliche Bedenken gegen die Einbeziehung moderner Kommunikationsangebote in die Speicherpflicht gemäß § 113b TKG-E bestehen nicht. Denn mit der Ausnahmeregelung für den Bereich der elektronischen Post gehen die Gesetzentwürfe bereits über die Anforderungen des Bundesverfassungsgerichts an die Begrenzung der Speicherpflicht hinaus.

4. Datensicherheit

a) Anforderungen des Bundesverfassungsgerichts

Angesichts der Aussagekraft der Verkehrsdaten und der damit verbundenen Gefahr eines illegalen Zugriffs fordert das Bundesverfassungsgericht sowohl hinsichtlich der Speicherung als auch der Übermittlung der Verkehrsdaten die Gewährleistung eines besonders hohen Sicherheitsstandards (Rn. 221 f.):

> Eine Speicherung der Telekommunikationsverkehrsdaten im Umfang des § 113a TKG bedarf der gesetzlichen Gewährleistung eines besonders hohen Standards der Datensicherheit.
>
> Angesichts des Umfangs und der potentiellen Aussagekraft der mit einer solchen Speicherung geschaffenen Datenbestände ist die Datensicherheit für die Verhältnismäßigkeit der angegriffenen Vorschriften von großer Bedeutung. Dieses gilt besonders, weil die Daten bei privaten Diensteanbietern gespeichert werden, die unter den Bedingungen von Wirtschaftlichkeit und Kostendruck handeln und dabei nur begrenzte Anreize zur Gewährleistung von Datensicherheit haben. Sie handeln grundsätzlich privatnützig und sind nicht durch spezifische Amtspflichten gebunden. Zugleich ist die Gefahr eines illegalen Zugriffs auf die Daten groß, denn angesichts ihrer vielseitigen Aussagekraft können diese für verschiedenste Akteure attraktiv sein. Geboten ist daher ein besonders hoher Sicherheitsstandard, der über das allgemein verfassungsrechtlich gebotene Maß für die Aufbewahrung von Daten der Telekommunikation hinausgeht. Solche Anforderungen der Datensicherheit gelten dabei sowohl für die Aufbewahrung der Daten als auch für deren Übermittlung; ebenso bedarf es effektiver Sicherungen zur Gewährleistung der Löschung der Daten.

---

[6] Vgl. etwa Stellungnahme der BfDI zum Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, 2015, S. 21; Stellungnahme des Deutschen Anwaltvereins zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz für ein Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, 2015, S. 20 f.

[7] Siehe die Synonyme zu „E-Mail“ bei Duden Online: „(EDV) E-Brief, E-Post, elektronische Post, elektronischer Brief, Mail“, http://www.duden.de/rechtschreibung/E_Mail (16.9.2015).

Die Entscheidung des Bundesverfassungsgerichts stellt – bei Betonung des gesetzgeberischen Spielraums (Rn. 224) – konkrete Sicherungsmaßnahmen in den Raum, die ein hinreichend hohes Maß an Datensicherheit zu gewährleisten vermögen. Danach sind für die Speicherung der Datenbestände gesonderte Speichereinrichtungen und eine anspruchsvolle Verschlüsselung zu verwenden. Ferner ist der Zugriff auf die Daten durch die Mitwirkung von mindestens zwei Personen sowie eine revisionssichere Protokollierung zu sichern. Überdies ist sicherzustellen, dass die Anforderungen an die zu treffenden Sicherungsmaßnahmen fortlaufend an den Entwicklungsstand der Fachdiskussion angepasst werden. Die Konkretisierung der technischen Anforderungen darf der Gesetzgeber dabei grundsätzlich einer Aufsichtsbehörde anvertrauen. Verfassungsrechtlich geboten ist jedoch eine für die Öffentlichkeit transparente Kontrolle der Sicherheitsmaßnahmen sowie eine angemessene Sanktionierung von Verstößen gegen das Erfordernis der Datensicherheit (Rn. 224 f.).

Die Verfassung gibt nicht detailgenau vor, welche Sicherheitsmaßgaben im Einzelnen geboten sind. Im Ergebnis muss jedoch ein Standard gewährleistet werden, der unter spezifischer Berücksichtigung der Besonderheiten der durch eine vorsorgliche Telekommunikationsverkehrsdatenspeicherung geschaffenen Datenbestände ein besonders hohes Maß an Sicherheit gewährleistet. Dabei ist sicherzustellen, dass sich dieser Standard – etwa unter Rückgriff auf einfachgesetzliche Rechtsfiguren wie den Stand der Technik … – an dem Entwicklungsstand der Fachdiskussion orientiert und neue Erkenntnisse und Einsichten fortlaufend aufnimmt. Entsprechend ist vorzusehen, dass die speicherpflichtigen Unternehmen – zum Beispiel auf der Grundlage von in regelmäßigen Abständen zu erneuernden Sicherheitskonzepten – ihre Maßnahmen hieran nachprüfbar anpassen müssen. Das Gefährdungspotential, das sich aus den in Frage stehenden Datenbeständen ergibt, erlaubt es nicht, die beschriebenen Sicherheitsanforderungen einer freien Abwägung mit allgemeinen wirtschaftlichen Gesichtspunkten zu unterwerfen. Wenn der Gesetzgeber eine flächendeckende Speicherung der Telekommunikationsverkehrsdaten ausnahmslos vorschreibt, gehört es zu den erforderlichen Voraussetzungen, dass die betroffenen Anbieter nicht nur ihre Pflicht zur Speicherung, sondern auch die korrespondierenden Anforderungen zur Datensicherheit erfüllen können. Anknüpfend an die sachverständigen Stellungnahmen liegt es nahe, dass nach dem gegenwärtigen Stand der Diskussion grundsätzlich eine getrennte Speicherung der Daten, eine anspruchsvolle Verschlüsselung, ein gesichertes Zugriffsregime unter Nutzung etwa des Vier-Augen-Prinzips sowie eine revisionssichere Protokollierung sichergestellt sein müssen, um die Sicherheit der Daten verfassungsrechtlich hinreichend zu gewährleisten.

Erforderlich sind gesetzliche Regelungen, die einen solchen besonders hohen Sicherheitsstandard in qualifizierter Weise jedenfalls dem Grunde nach normenklar und verbindlich vorgeben. Dabei steht es dem Gesetzgeber frei, die technische Konkretisierung des vorgegebenen Maßstabs einer Aufsichtsbehörde anzuvertrauen. Der Gesetzgeber hat dabei jedoch sicherzustellen, dass die Entscheidung über Art und Maß der zu treffenden Schutzvorkehrungen nicht letztlich unkontrolliert in den Händen der jeweiligen Telekommunikationsanbieter liegt. Die zu stellenden Anforderungen sind entweder durch differenzierte technische Vorschriften – möglicherweise gestuft auf verschiedenen Normebenen – oder in allgemeingenereller Weise vorzugeben und dann in transparenter Weise durch verbindliche Einzelentscheidung der Aufsichtsbehörden gegenüber den einzelnen Unternehmen zu konkretisieren. Verfassungsrechtlich geboten sind weiterhin eine für die Öffentlichkeit transparente Kontrolle unter Einbeziehung des unabhängigen Datenschutzbeauftragten … sowie ein ausgeglichenes Sanktionensystem, das auch Verstößen gegen die Datensicherheit ein angemessenes Gewicht beimisst.

b) Bewertung der Gesetzentwürfe

Die Gesetzentwürfe entsprechen den Anforderungen des Bundesverfassungsgerichts im Bereich der Datensicherheit.

§ 113f Abs. 1 S. 1 TKG-E fordert bei der Umsetzung der Verpflichtungen im Rahmen der vorsorglichen Verkehrsdatenspeicherung einen **besonders hohen Standard an Datensicherheit und Datenqualität**. Zur Gewährleistung der Sicherheit der angelegten Datenbestände sollen die Erbringer öffentlich zugänglicher Telekommunikationsdienste gemäß § 113d S. 1 TKG-E verpflichtet werden, die gespeicherten Daten durch technische und organisatorische Maßnahmen gegen unbefugte Kenntnisnahme und Verwendung zu schützen. Diese Maßnahmen sollen unter anderem die Verwendung eines besonders sicheren Verschlüsselungsverfahrens (§ 113d S. 2 Nr. 1 TKG-E), die Speicherung der Daten in gesonderten Speichereinrichtungen (§ 113d S. 2 Nr. 2 TKG-E) sowie die notwendige Mitwirkung von mindestens zwei Personen beim Zugriff auf die Daten (§ 113d S. 2 Nr. 5 TKG-E) umfassen. § 113e TKG-E sieht vor, dass Zeitpunkt, Art und Zweck jedes Zugriffs auf die Datenbestände sowie die zugreifenden Personen zum Zwecke der Datenschutzkontrolle zu protokollieren sind.

Die Gesetzentwürfe enthalten darüber hinaus in § 113d S. 1 TKG-E die Vorgabe, dass der Schutz der Datenbestände durch Maßnahmen **nach dem Stand der Technik** sichergestellt wird. Das Verfahren zur fortlaufenden Anpassung der Sicherungsmaßnahmen an den jeweiligen Entwicklungsstand wird in § 113f TKG-E geregelt. Danach soll die Bundesnetzagentur in Absprache mit dem Bundesamt für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit einen Katalog der technischen Vorkehrungen und sonstigen Maßnahmen zur Datensicherheit erstellen (Abs. 1) und die darin enthaltenen Anforderungen fortlaufend unter Berücksichtigung des Stands der Technik sowie der Fachdiskussion überprüfen und gegebenenfalls Anpassungen vornehmen (Abs. 2).

Um eine Einhaltung dieser Anforderungen gewährleisten zu können, haben die Erbringer öffentlich zugänglicher Telekommunikationsdienste gemäß § 113g S. 1 TKG-E die zur Erfüllung der ihnen zugewiesenen Aufgaben betriebenen Systeme, die für diese Systeme zu erwartenden Gefährdungen sowie die technischen Vorkehrungen und sonstigen Maßnahmen zur Abwehr dieser Gefährdungen in das gemäß § 109 Abs. 4 TKG anzulegende Sicherheitskonzept aufzunehmen. Dieses Sicherheitskonzept ist der Bundesnetzagentur unverzüglich nach Beginn der Speicherung sowie unverzüglich nach jeder Änderung des Konzepts vorzulegen. Gemäß § 121 Abs. 1 StPO-E hat die Bundesnetzagentur in ihren Tätigkeitsbericht auch Umfang und Ergebnisse ihrer Überprüfung der Sicherheitskonzepte sowie etwaige Beanstandungen oder sonstige Ergebnisse durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit aufzunehmen. Verstöße gegen die Datensicherheit sind ferner § 149 Abs. 1 TKG-E entsprechend zu sanktionieren.

Zusammenfassend ist festzustellen, dass die Gesetzentwürfe hinsichtlich ihrer konkreten Ausgestaltung dem vom Bundesverfassungsgericht angemahnten Erfordernis der Gewährleistung eines besonders hohen Standards der Datensicherheit entsprechen.[8]

5. Datenlöschung

a) Anforderungen des Bundesverfassungsgerichts

Neben den Vorgaben hinsichtlich der Speicherung und Übermittlung der Verkehrsdaten fordert das Bundesverfassungsgericht auch wirksame Sicherungsmaßnahmen betreffend die Löschung der gespeicherten Datenbestände (Rn. 222):

> Angesichts des Umfangs und der potentiellen Aussagekraft der mit einer solchen Speicherung geschaffenen Datenbestände ist die Datensicherheit für die Verhältnismäßigkeit der angegriffenen Vorschriften von großer Bedeutung. … Solche Anforderungen der Datensicherheit gelten dabei sowohl für die Aufbewahrung der Daten als auch für deren Übermittlung; ebenso bedarf es effektiver Sicherungen zur Gewährleistung der Löschung der Daten.

Für die Löschung der gespeicherten Verkehrsdaten durch die Telekommunikationsunternehmen nach Ablauf der gesetzlich vorgesehenen Speicherdauer erachtete das Gericht eine Löschungsfrist von einem Monat für ausreichend (Rn. 270):

> … Auch hat der Gesetzgeber gemäß § 113a Abs. 1, 11 TKG mit sechs Monaten und einer sich hieran anschließenden Löschungsfrist von einem Monat eine verfassungsrechtlich noch vertretbare Speicherungsdauer bestimmt. …

Darüber hinaus ist sicherzustellen, dass die gespeicherten Datenbestände unverzüglich gelöscht werden, sofern sie für den vorgesehenen Erhebungszweck nicht (mehr) erforderlich sind. Die Löschung der Daten ist zu protokollieren (Rn. 235):

> Die Begrenzung der Datenverwendung auf bestimmte Zwecke muss auch für die Verwendung der Daten nach deren Abruf und Übermittlung an die abrufenden Behörden sichergestellt und verfahrensmäßig flankiert werden. Insoweit ist gesetzlich zu gewährleisten, dass die Daten nach Übermittlung unverzüglich ausgewertet werden und, sofern sie für die Erhebungszwecke unerheblich sind, gelöscht werden … Im Übrigen ist vorzusehen, dass die Daten vernichtet werden, sobald sie für die festgelegten Zwecke nicht mehr erforderlich sind, und dass hierüber ein Protokoll gefertigt wird …

b) Bewertung der Gesetzentwürfe

Hinsichtlich der Löschung der gespeicherten Datenbestände durch die Diensteanbieter bleiben die Gesetzentwürfe deutlich hinter der verfassungsrechtlich zulässigen Löschungsfrist von einem Monat zurück. So sieht § 113b Abs. 8 TKG-E vor, dass die bei den Telekommunikationsunternehmen gespeicherten Verkehrsdaten innerhalb einer Woche nach Ablauf der vorgesehenen Speicherfrist irreversibel zu löschen sind oder ihre irreversible Löschung sicherzustellen

---

[8] Ebenso: Ausarbeitung der Wissenschaftlichen Dienste des Bundestags über die Umsetzung der Vorgaben des Bundesverfassungsgerichts zur Vorratsdatenspeicherung durch den Gesetzentwurf der Bundesregierung vom 27. Mai 2015, 2015, S. 8 ff.

ist. Die Löschung ist gemäß § 113e Abs. 1 TKG-E zu protokollieren. Ein Verstoß gegen diese Verpflichtung ist gemäß § 149 Abs. 1 Nr. 38 TKG-E zu sanktionieren.

Die vorliegenden Gesetzentwürfe werden teilweise dahingehend kritisiert, dass sie zwar ein Überschreiten der Höchstspeicherfrist durch die Telekommunikationsunternehmen sanktionierten, auf Seiten der Behörden für diesen Fall jedoch weder ein Abruf- noch ein Verwertungsverbot vorsähen.[9] Tatsächlich wird die Frage des Abrufs von Daten nach Ablauf der Höchstspeicherfrist durch die Gesetzentwürfe nicht ausdrücklich geregelt. Auch die Gesetzesbegründung liefert insoweit keinen klaren Hinweis auf den gesetzgeberischen Willen. Einen Anhaltspunkt liefert jedoch § 100g Abs. 2 StPO-E, der die Behörden zur Erhebung von „nach § 113b des Telekommunikationsgesetzes gespeicherten Verkehrsdaten" ermächtigt. § 113b TKG-E enthält neben der Verpflichtung der Diensteanbieter zur Speicherung der Verkehrsdaten auch die Regelungen über die jeweiligen Höchstspeicherfristen. Der Verweis auf § 113b TKG-E kann demnach so verstanden werden, dass die Befugnis zur Erhebung von Verkehrsdaten nur im Rahmen der gesetzlichen Höchstspeicherfrist bestehen soll.

Überdies wird die Wahrung der Höchstspeicherfrist durch die Verpflichtung der Diensteanbieter zur Löschung der Daten sowie die Sanktionierung von Verstößen gegen diese Verpflichtung hinreichend sichergestellt. Zur Klarstellung ist eine ausdrückliche Regelung der Verwendung von Verkehrsdaten nach Ablauf der Höchstspeicherfrist zu erwägen.

Die Gesetzentwürfe treffen ferner effektive Sicherungsmaßnahmen hinsichtlich der Löschung abgerufener Verkehrsdaten durch die Sicherheitsbehörden. Gemäß § 101a Abs. 3 S. 1 StPO-E sind „personenbezogene Daten"[10], die durch eine Maßnahme gemäß § 100g StPO-E erhoben wurden, entsprechend zu kennzeichnen und unverzüglich auszuwerten. Die Kennzeichnung muss gemäß § 101a Abs. 3 S. 2 StPO-E erkennen lassen, ob es sich bei den erhobenen Daten um gemäß § 113b TKG vorsorglich gespeicherte Verkehrsdaten handelt. Diese Kennzeichnung ist gemäß § 101a Abs. 3 S. 3 StPO-E auch im Falle der Übermittlung an eine andere Stelle

---

[9] Stellungnahme des Deutschen Anwaltvereins zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz für ein Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, 2015, S. 25; Stellungnahme der BfDI zum Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, 2015, S. 24.

[10] Neben der Bezeichnung „Verkehrsdaten" verwenden die Gesetzentwürfe in § 101a Abs. 3 StPO-E die Bezeichnung „personenbezogene Daten", in § 101a Abs. 4 S. 3 und 4 StPO-E „verwertbare personenbezogene Daten". Zur Gewährleistung normenklarer Regelungen sollte einheitlich die Bezeichnung „Verkehrsdaten" verwendet werden, vgl. auch die Ausarbeitung der Wissenschaftlichen Dienste des Bundestags über die Umsetzung der Vorgaben des Bundesverfassungsgerichts zur Vorratsdatenspeicherung durch den Gesetz-entwurf der Bundesregierung vom 27. Mai 2015, 2015, S. 13 und 14 f.

aufrechtzuerhalten.[11] Gemäß § 101a Abs. 3 S. 4 StPO-E richtet sich die Löschung der Daten nach den Vorgaben des § 101 Abs. 8 StPO. Danach sind die Daten unverzüglich zu löschen, soweit sie für die Strafverfolgung und für eine etwaige gerichtliche Überprüfung der Maßnahme nicht mehr erforderlich sind. Die Löschung ist aktenkundig zu machen.

Teilweise wird kritisiert, die Gesetzentwürfe ließen – anders als vom Bundesverfassungsgericht gefordert[12] – eine Regelung zur Löschung von von vornherein unerheblichen Daten vermissen.[13] Die Regelung des § 101 Abs. 8 StPO, auf die § 101a Abs. 3 S. 4 StPO-E verweist, sieht eine unverzügliche Löschung „nicht mehr erforderlich[er]" Daten vor. Hierunter lassen sich dem Wortlaut nach, gerade in verfassungskonformer Auslegung, auch von vornherein nicht erforderliche Daten fassen.[14] Aus Gründen der Normklarheit empfiehlt sich freilich eine gesetzliche Klarstellung.[15]

Zusammenfassend ist daher festzustellen, dass die Gesetzentwürfe den Vorgaben des Bundesverfassungsgerichts hinsichtlich der Löschung der gespeicherten Datenbestände gerecht werden.

6. Verwendung für überragend wichtige Aufgaben des Rechtsgüterschutzes

a) Anforderungen des Bundesverfassungsgerichts

Das Bundesverfassungsgericht fordert weiterhin, dass die Voraussetzungen für die Datenverwendung umso enger zu begrenzen sind, je schwerwiegender durch die Speicherung in die Telekommunikationsfreiheit eingegriffen wird. In Anbetracht der Schwere des Eingriffs durch die anlasslose systematische Speicherung fast aller Verkehrsdaten ist eine Verwendung nur für überragend wichtige Aufgaben des Rechtsgüterschutzes zulässig (Rn. 227):

---

[11] Die Gesetzgebungskompetenz des Bundes zum Erlass datenschutzrechtlicher Vorgaben für die Gefahrenabwehrbehörden der Länder in Frage stellend: Ausarbeitung der Wissenschaftlichen Dienste des Bundestags über die Umsetzung der Vorgaben des Bundesverfassungsgerichts zur Vorratsdatenspeicherung durch den Gesetzentwurf der Bundesregierung vom 27. Mai 2015, 2015, S. 15 f. Vgl. zu einer Kompetenz kraft Sachzusammenhangs BVerfGE 125, 260 (314 f.).

[12] BVerfGE 125, 260 (332 f.).

[13] Vgl. die Ausarbeitung der Wissenschaftlichen Dienste des Bundestags über die Umsetzung der Vorgaben des Bundesverfassungsgerichts zur Vorratsdatenspeicherung durch den Gesetzentwurf der Bundesregierung vom 27. Mai 2015, 2015, S. 13 f.

[14] Eine solche Lesart unterstreichen auch verschiedene Kommentierungen zu § 101 Abs. 8 StPO, vgl. etwa *B. Schmitt*, in: Meyer-Goßner (Hrsg.), Strafprozessordnung, 58. Aufl. 2015, § 101 Rn. 27: „[…] müssen unverzüglich gelöscht werden, wenn sie weder zu Zwecken der Strafverfolgung noch für eine etwaige gerichtliche Überprüfung (weiterhin) erforderlich sind […]"; ferner *R. Eschelbach*, in: Satzger/Schluckebier/Widmaier (Hrsg.), Strafprozessordnung, 2014, § 101 Rn. 36, der auf eine entsprechende Einschränkung gänzlich verzichtet.

[15] So auch Ausarbeitung der Wissenschaftlichen Dienste des Bundestags über die Umsetzung der Vorgaben des Bundesverfassungsgerichts zur Vorratsdatenspeicherung durch den Gesetzentwurf der Bundesregierung vom 27. Mai 2015, 2015, S. 13 f.

Die Verwendung der durch eine anlasslos systematische Speicherung praktisch aller Telekommunikationsverkehrsdaten gewonnenen Datenbestände unterliegt dementsprechend besonders hohen Anforderungen. Insbesondere ist diese nicht in gleichem Umfang verfassungsrechtlich zulässig wie die Verwendung von Telekommunikationsverkehrsdaten, die die Diensteanbieter in Abhängigkeit von den jeweiligen betrieblichen und vertraglichen Umständen – von den Kunden teilweise beeinflussbar – nach § 96 TKG speichern dürfen. Angesichts der Unausweichlichkeit, Vollständigkeit und damit gesteigerten Aussagekraft der über sechs Monate systematisch vorsorglich erhobenen Verkehrsdaten hat ihr Abruf ein ungleich größeres Gewicht. Da eine Auswertung dieser Daten tief in das Privatleben eindringende Rückschlüsse und unter Umständen detaillierte Persönlichkeits- und Bewegungsprofile ermöglicht, kann insoweit nicht ohne weiteres davon ausgegangen werden, dass der Rückgriff auf diese Daten grundsätzlich geringer wiegt als eine inhaltsbezogene Telekommunikationsüberwachung … Vielmehr kann auch die Verwendung solcher Daten nur dann als verhältnismäßig angesehen werden, wenn sie besonders hochrangigen Gemeinwohlbelangen dient. Eine Verwendung der Daten kommt deshalb nur für überragend wichtige Aufgaben des Rechtsgüterschutzes in Betracht, das heißt zur Ahndung von Straftaten, die überragend wichtige Rechtsgüter bedrohen[,] oder zur Abwehr von Gefahren für solche Rechtsgüter.

Im Rahmen der Strafverfolgung wurde eine Verwendung aufgrund eines durch bestimmte Tatsachen begründeten Verdachts einer schweren Straftat für zulässig erachtet, wobei die Qualifikation der Straftaten als schwer bereits in der jeweiligen Strafnorm angelegt sein muss. Zur Orientierung kann hierbei etwa auf den Strafrahmen der Norm zurückgegriffen werden (Rn. 228 f.):

Für die Strafverfolgung folgt hieraus, dass ein Abruf der Daten zumindest den durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat voraussetzt. Welche Straftatbestände hiervon umfasst sein sollen, hat der Gesetzgeber abschließend mit der Verpflichtung zur Datenspeicherung festzulegen. Ihm kommt hierbei ein Beurteilungsspielraum zu. Er kann dabei entweder auf bestehende Kataloge zurückgreifen oder einen eigenen Katalog schaffen, etwa um Straftaten, für die die Telekommunikationsverkehrsdaten besondere Bedeutung haben, zu erfassen. Die Qualifizierung einer Straftat als schwer muss aber in der Strafnorm – insbesondere etwa durch deren Strafrahmen – einen objektivierten Ausdruck finden … Eine Generalklausel oder lediglich die Verweisung auf Straftaten von erheblicher Bedeutung reichen hingegen nicht aus.

Über die abstrakte Festlegung eines entsprechenden Straftatenkatalogs hinaus hat der Gesetzgeber sicherzustellen, dass ein Rückgriff auf die vorsorglich gespeicherten Telekommunikationsverkehrsdaten nur dann zulässig ist, wenn auch im Einzelfall die verfolgte Straftat schwer wiegt … und die Verwendung der Daten verhältnismäßig ist.

Eine Verwendung im Bereich der Gefahrenabwehr ist zulässig, wenn tatsächliche Anhaltspunkte auf das Bestehen einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder auf eine gemeine Gefahr hindeuten. Eine Differenzierung zwischen den unterschiedlichen im Rahmen der Gefahrenabwehr tätigen Behörden, insbesondere hinsichtlich der Nachrichtendienste, ist hierbei nicht erforderlich (Rn. 231 f.).

Die Abwägung zwischen dem Gewicht des in der Datenspeicherung und Datenverwendung liegenden Eingriffs und der Bedeutung einer wirksamen Gefahrenabwehr führt dazu, dass ein Abruf der vorsorglich gespeicherten Telekommunikationsverkehrsdaten nur zur Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr zugelassen werden darf … Die gesetzliche Ermächtigungsgrundlage muss diesbezüglich zumindest tatsächliche Anhaltspunkte einer konkreten Gefahr für die zu schützenden Rechtsgüter verlangen. Dieses Erfordernis führt dazu, dass Vermutungen oder allgemeine Erfahrungssätze nicht ausreichen, um den Zugriff auf die Daten zu rechtfertigen. Vielmehr müssen bestimmte Tatsachen festgestellt sein, die die Prognose einer konkreten Gefahr tragen …

Die verfassungsrechtlichen Anforderungen für die Verwendung der Daten zur Gefahrenabwehr gelten für alle Eingriffsermächtigungen mit präventiver Zielsetzung. Sie gelten damit auch für die Verwendung der Daten durch die Nachrichtendienste. Da die Beeinträchtigung durch den Eingriff in allen diesen Fällen für die Betroffenen die gleiche ist, besteht hinsichtlich dieser Anforderungen kein Anlass zu behördenbezogenen Differenzierungen, etwa

zwischen Polizeibehörden und anderen mit präventiven Aufgaben betrauten Behörden wie Verfassungsschutzbehörden …

b) Bewertung der Gesetzentwürfe

Die Gesetzentwürfe begrenzen die Verwendung der gespeicherten Datenbestände in Einklang mit den verfassungsrechtlichen Vorgaben auf die Gewährleistung des Schutzes überragend wichtiger Rechtsgüter.

aa) Strafverfolgung

Im Bereich der Strafverfolgung ist die Erhebung von gemäß § 113b TKG-E vorsorglich gespeicherten Verkehrsdaten gemäß § 100g Abs. 2 S. 1 StPO-E zulässig, sofern bestimmte Tatsachen den Verdacht der Begehung einer „*besonders* schweren Straftat“ [Hervorhebung nicht im Original] begründen. Die Gesetzentwürfe gehen insoweit über die Forderung des Bundesverfassungsgerichts hinaus, das bereits den Verdacht einer „schweren Straftat“ als ausreichend erachtete. Für die Bestimmung einer Straftat als „besonders schwer“ hat das Bundesverfassungsgericht bereits in der Vergangenheit maßgeblich auf den Strafrahmen abgestellt. Danach soll eine besonders schwere Straftat nur vorliegen, wenn sie mit einer Höchststrafe von mindestens fünf Jahren Freiheitsstrafe bewehrt ist.[16]

Die Gesetzentwürfe formulieren sodann in § 100g Abs. 2 S. 2 StPO-E einen abschließenden Katalog besonders schwerer Straftaten. Die dort genannten Straftaten betreffen die Terrorismusbekämpfung oder den Schutz höchstpersönlicher Rechtsgüter und sind jeweils mit einer Höchststrafe von mehr als fünf Jahren Freiheitsstrafe bewehrt. Einzig § 184c Abs. 2 StGB, der gemäß § 100g Abs. 2 S. 2 Nr. 1 lit. b StPO-E in den Katalog aufgenommen wurde, sieht für gewerbs- oder bandenmäßige Verbreitung, Erwerb und Besitz jugendpornographischer Schriften lediglich eine Höchststrafe von fünf Jahren vor. § 184c Abs. 2 StGB stellt jedoch eine (für eine Verkehrsdatenspeicherung ausreichende) „schwere“ Straftat im Sinne der Rechtsprechung des Bundesverfassungsgerichts dar: Er ist gemäß § 100a Abs. 2 Nr. 1 lit. g StPO Bestandteil des dort geführten Katalogs schwerer Straftaten. Die Einstufung der dort aufgeführten Straftat-

[16] BVerfGE 109, 279 (347 f.).

bestände als „schwer“ hat das Bundesverfassungsgericht in seiner Entscheidung zur TKÜ-Neuregelung ausdrücklich anerkannt.[17] Die Erhebung von gemäß § 113b TKG-E vorsorglich gespeicherten Verkehrsdaten ist daher entsprechend den verfassungsrechtlichen Vorgaben auf die Verfolgung schwerer Straftaten beschränkt.[18]

Darüber hinaus verlangt § 100g Abs. 2 S. 1 StPO-E, dass die Straftat auch im Einzelfall als besonders schwerwiegend anzusehen ist, die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts des Beschuldigten auf andere Weise erheblich erschwert oder aussichtslos wäre und die Erhebung der Daten auch nicht außer Verhältnis zur Bedeutung der Sache steht. Gemäß § 101a Abs. 4 S. 1 Nr. 1 StPO-E soll die Verwendung von nach § 100g Abs. 2 StPO-E erhobenen personenbezogenen Daten ferner in anderen Strafverfahren zur Aufklärung von Straftaten zulässig sein, die ihrerseits eine Datenerhebung gemäß § 100g Abs. 2 StPO-E rechtfertigen würden.[19]

bb) Gefahrenabwehr

Für den Bereich der Gefahrenabwehr sehen die Gesetzentwürfe in § 101a Abs. 4 S. 1 Nr. 2 StPO-E in Einklang mit den verfassungsrechtlichen Vorgaben vor, dass eine Verwendung der nach § 100g Abs. 2 StPO-E erhobenen personenbezogenen Daten ausschließlich zur Abwehr von konkreten Gefahren für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes zulässig sein soll.

---

[17] BVerfGE 129, 208 (241 ff.).

[18] So auch Ausarbeitung der Wissenschaftlichen Dienste des Bundestags über die Umsetzung der Vorgaben des Bundesverfassungsgerichts zur Vorratsdatenspeicherung durch den Gesetzentwurf der Bundesregierung vom 27. Mai 2015, 2015, S. 10 ff. Der Straftatenkatalog des § 100g Abs. 2 StPO-E wird jedoch mitunter als noch zu kurz greifend kritisiert, vgl. die Stellungnahme des Deutschen Richterbundes zum Referentenentwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, 2015, S. 2 f.

[19] Angesichts der Befugnis zur Weitergabe von Daten zur Aufklärung von Straftaten, die ihrerseits eine Datenerhebung rechtfertigen würden (§ 101a Abs. 4 S. 1 Nr. 1 Var. 1 StPO-E), wird die eigenständige Bedeutung der Befugnis zur Weitergabe zum Zwecke der Ermittlung des Aufenthalts der einer solchen Straftat beschuldigten Person (Var. 2) infrage gestellt, vgl. die Ausarbeitung der Wissenschaftlichen Dienste des Bundestags über die Umsetzung der Vorgaben des Bundesverfassungsgerichts zur Vorratsdatenspeicherung durch den Gesetzentwurf der Bundesregierung vom 27. Mai 2015, 2015, S. 15.

7. Berufsgeheimnisträger

a) Anforderungen des Bundesverfassungsgerichts

Als nicht von vornherein unzulässig erachtete das Bundesverfassungsgericht auch die Speicherung von Verkehrsdaten bei Berufsgruppen, die auf die Wahrung eines besonderen Vertrauensverhältnisses angewiesen sind. Die Antragsteller im seinerzeitigen Verfahren haben einen unzureichenden Schutz von Berufsgeheimnisträgern ausdrücklich gerügt (Rn. 106 f., 144):

> Die angegriffenen Vorschriften verstießen auch gegen Art. 12 Abs. 1 GG. Die §§ 113a und 113b TKG griffen unverhältnismäßig in die Berufsausübungsfreiheit der kommerziellen Anbieter von Telekommunikationsdienstleistungen und in die Berufsfreiheit der Angehörigen von Vertrauensberufen ein.
>
> So berühre es das Vertrauensverhältnis zwischen Rechtsanwalt und Mandant, wenn durch Auswertung von Telekommunikationsverkehrsdaten das Mandatsverhältnis aufgedeckt werden könne. Auch schrecke die Vorratsdatenspeicherung von der telekommunikativen Kontaktaufnahme mit spezialisierten Beratern ab, weil daraus weitreichende Schlüsse auf Gesundheit und Geisteszustand, Religion oder finanzielle Verhältnisse gezogen werden könnten. Journalisten drohe der Verlust von Informanten. Diesen negativen Auswirkungen stehe kein messbares öffentliches Interesse gegenüber. Angesichts der geringen Zahl von Verfahren, in denen es auf die Kommunikation von und mit Berufsgeheimnisträgern ankomme, seien die Belange des Rechtsgüterschutzes auch ohne Vorratsdatenspeicherung gewährleistet.
>
> Berufsgeheimnisträger seien nicht gesondert geschützt. Besonders beeinträchtigend wirke sich dies bei Ärzten und nicht ausschließlich als Strafverteidiger tätigen Anwälten aus …

Gleichwohl erachtete das Gericht einen differenzierten Schutz von Vertrauensbeziehungen für ausreichend (Rn. 237 f.):

> Verfassungsrechtliche Grenzen können sich schließlich auch hinsichtlich des Umfangs der abzurufenden Daten ergeben. So lassen sich unter Verhältnismäßigkeitsgesichtspunkten vielfältige Abstufungen zwischen den verschiedenen Auskunftsbegehren ausmachen, etwa danach, ob sie nur eine einzelne Telekommunikationsverbindung betreffen, sie auf die Übermittlung der Daten aus allein einer Funkzelle zu einem bestimmten Zeitpunkt zielen, sie bezogen sind nur auf die Kommunikation zwischen einzelnen Personen – begrenzt möglicherweise auf einen bestimmten Zeitraum oder eine bestimmte Form der Kommunikation – und hierbei auch die Standortdaten ein- oder ausschließen beziehungsweise ob sie auf eine vollständige Übermittlung der Daten einer Person zur Erstellung eines möglichst detaillierten Bewegungs- oder Persönlichkeitsprofils zielen. Auch kann es in Blick auf das Eingriffsgewicht einen Unterschied machen, ob bei der Datenübermittlung Filter zwischengeschaltet werden, mit denen bestimmte Telekommunikationsverbindungen zum Schutz von besonderen Vertrauensbeziehungen ausgesondert werden.
>
> Angesichts der hohen Schwellen, die nach den vorstehenden Maßgaben schon grundsätzlich für die Verwendung vorsorglich gespeicherter Telekommunikationsverkehrsdaten gelten, hat der Gesetzgeber bei der näheren Regelung des Umfangs der Datenverwendung allerdings einen Gestaltungsspielraum. Insbesondere steht es ihm grundsätzlich auch frei, solche Verhältnismäßigkeitserwägungen dem zur Entscheidung über die Anordnung eines Datenabrufs berufenen Richter bei der Prüfung im Einzelfall zu überlassen. Verfassungsrechtlich geboten ist als Ausfluss des Verhältnismäßigkeitsgrundsatzes jedoch, zumindest für einen engen Kreis von auf besondere Vertraulichkeit angewiesenen Telekommunikationsverbindungen ein grundsätzliches Übermittlungsverbot vorzusehen. Zu denken ist hier etwa 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).

b) Bewertung der Gesetzentwürfe

Die Gesetzentwürfe enthalten verschiedene Regelungen, die den Schutz von besonderen Vertrauensbeziehungen respektive Berufsgeheimnisträgern sicherstellen sollen. Hinsichtlich des

vom Bundesverfassungsgericht ausdrücklich geforderten Schutzes von auf besondere Vertraulichkeit angewiesenen Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen sehen die Gesetzentwürfe in § 113b Abs. 6 TKG-E vor, dass Daten über die in § 99 Abs. 2 TKG genannten Verbindungen grundsätzlich nicht gespeichert werden dürfen. Die Gesetzentwürfe gehen insoweit noch über das vom Gericht geforderte Übermittlungsverbot hinaus.

Die Gesetzentwürfe treffen ferner auch Regelungen zum Schutze weiterer Telekommunikationsverbindungen, die auf eine besondere Vertraulichkeit angewiesen sind. So ist gemäß § 100g Abs. 4 S. 1 StPO-E die Erhebung von vorsorglich gespeicherten Verkehrsdaten unzulässig, sofern sie voraussichtlich Erkenntnisse erbringen würde, über die der Betroffene gemäß § 53 Abs. 1 S. 1 Nr. 1–5 StPO zur Zeugnisverweigerung berechtigt wäre. Dies gilt gemäß § 100g Abs. 4 S. 5 StPO-E auch dann, wenn sich die Ermittlungsmaßnahme nicht gegen die zur Zeugnisverweigerung berechtigte Person richtet. Erkenntnisse, die trotz dieses Erhebungsverbots gewonnen werden, dürfen gemäß § 100g Abs. 4 S. 2 StPO-E nicht verwendet werden und sind gemäß § 100g Abs. 4 S. 3 StPO-E unverzüglich zu löschen. Ihre Erlangung sowie ihre Löschung sind zu protokollieren, § 100g Abs. 4 S. 4 StPO-E.

Die Regelungen zum Schutz von Berufsgeheimnisträgern werden in verschiedenen Stellungnahmen als unzureichend kritisiert.[20] Um einen effektiven Schutz zu gewährleisten, müsse das Speicherungsverbot nicht nur die Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen erfassen, sondern auch die übrigen zur Zeugnisverweigerung berechtigten Gruppen.[21] Ein solches Speicherungsverbot dürfte indes schon technisch nur schwer durchführbar sein, da alle in Deutschland tätigen Telekommunikationsanbieter – laut Gesetzesbegründung immerhin mehr als 1000[22] – über eine entsprechende Liste sämtlicher Berufsgeheimnisträger verfügen müssten, die der fortlaufenden Aktualisierung bedürfte; im Übrigen ist die Führung derartiger Listen wiederum datenschutzrechtlich relevant. Insbesondere ist jedoch zu berücksichtigen, dass das Bundesverfassungsgericht – wie bereits dargestellt – auch für die

---

[20] Vgl. Stellungnahme der BfDI zum Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, 2015, S. 15 f.; Stellungnahme des Deutschen Anwaltvereins zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz für ein Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, 2015, S. 12 ff.; *I. Spiecker gen. Döhmann/S. Simitis*, A Never-Ending Story: Die Vorratsdatenspeicherung, abrufbar unter: http://www.verfassungsblog.de/a-never-ending-story-die-vorratsdatenspeicherung/#.Vfk41EaLW3A (16.9.2015).

[21] Stellungnahme der BfDI zum Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, 2015, S. 15 f.; Stellungnahme des Deutschen Anwaltvereins zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz für ein Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, 2015, S. 14 f.

[22] Begründung des Gesetzentwurfs, BT-Drs. 18/5088, S. 33.

ausdrücklich genannten Verbindungen im sozialen und kirchlichen Bereich gerade kein Speicherungsverbot gefordert hat, sondern einen Schutz (grundsätzlich) auf Übermittlungsebene für ausreichend erachtet hat. Nachdem das Bundesverfassungsgericht für sonstige Vertrauensbeziehungen – trotz der einleitend skizzierten Rüge – kein Übermittlungsverbot gefordert, sondern einen differenzierten Schutz (Erhebungsverbot) für ausreichend erachtet hat, erscheint der Schutz auf Erhebungs- respektive Verwertungsebene ausreichend. Zu berücksichtigen ist insoweit auch, dass ein Übermittlungsverbot auf Seiten der Diensteanbieter hinsichtlich der Daten von Betroffenen, die gemäß § 53 Abs. 1 S. 1 Nr. 1–5 StPO zur Zeugnisverweigerung berechtigt wären, nicht in Betracht kommt: Denn dies setzt eine Beurteilung von Inhalt und weiteren Umständen (z.B. Ermittlungsstand) voraus, wozu die Telekommunikationsunternehmen rechtlich und tatsächlich nicht in der Lage sind.[23]

Die Regelungen der Gesetzentwürfe zum Schutz von Berufsgeheimnisträgern gewährleisten somit auch den verfassungsrechtlich gebotenen Schutz von auf besondere Vertraulichkeit angewiesenen Telekommunikationsverbindungen und gehen dabei teilweise noch über die vom Bundesverfassungsgericht gestellten Anforderungen hinaus.[24]

8. Standortdaten

a) Anforderungen des Bundesverfassungsgerichts

Die Einbeziehung von Standortdaten in die Verkehrsdatenspeicherung ermöglicht, besonders weitreichende Einblicke in die Privat- und Intimsphäre der Betroffenen zu gewinnen sowie umfassende Bewegungsprofile zu erstellen (Rn. 211 f.):

> Die Aussagekraft dieser Daten ist weitreichend. Je nach Nutzung von Telekommunikationsdiensten seitens der Betroffenen lassen sich schon aus den Daten selbst – und erst recht, wenn diese als Anknüpfungspunkte für weitere Ermittlungen dienen – tiefe Einblicke in das soziale Umfeld und die individuellen Aktivitäten eines jeden Bürgers gewinnen. Zwar werden mit einer Telekommunikationsverkehrsdatenspeicherung, wie in § 113a TKG vorgesehen, nur die Verbindungsdaten (Zeitpunkt, Dauer, beteiligte Anschlüsse sowie – bei der Mobiltelefonie – der Standort) festgehalten, nicht aber auch der Inhalt der Kommunikation. Auch aus diesen Daten lassen sich jedoch bei umfassender und automatisierter Auswertung bis in die Intimsphäre hineinreichende inhaltliche Rückschlüsse ziehen. Adressaten (deren Zugehörigkeit zu bestimmten Berufsgruppen, Institutionen oder Interessenverbänden oder die von ihnen angebotenen Leistungen), Daten, Uhrzeit und Ort von Telefongesprächen erlauben, wenn sie über einen längeren Zeitraum beobachtet werden, in ihrer Kombination detaillierte Aussagen zu gesellschaftlichen oder politischen Zugehörigkeiten sowie persönlichen Vorlieben, Neigungen und Schwächen derjenigen, deren Verbindungsdaten ausgewertet werden. Einen Vertraulichkeitsschutz gibt es insoweit nicht. Je nach Nutzung der Telekommunikation und künftig in zunehmender Dichte kann eine solche Speicherung die Erstellung aussagekräftiger

[23] Ausarbeitung der Wissenschaftlichen Dienste des Bundestags über die Umsetzung der Vorgaben des Bundesverfassungsgerichts zur Vorratsdatenspeicherung durch den Gesetzentwurf der Bundesregierung vom 27. Mai 2015, 2015, S. 16 f.

[24] So auch Ausarbeitung der Wissenschaftlichen Dienste des Bundestags über die Umsetzung der Vorgaben des Bundesverfassungsgerichts zur Vorratsdatenspeicherung durch den Gesetzentwurf der Bundesregierung vom 27. Mai 2015, 2015, S. 16 f.

Persönlichkeits- und Bewegungsprofile praktisch jeden Bürgers ermöglichen. Bezogen auf Gruppen und Verbände erlauben die Daten überdies unter Umständen die Aufdeckung von internen Einflussstrukturen und Entscheidungsabläufen.

Eine Speicherung, die solche Verwendungen grundsätzlich ermöglicht und in bestimmten Fällen ermöglichen soll, begründet einen schwerwiegenden Eingriff …

Die ist im Rahmen der verhältnismäßigen Ausgestaltung zu berücksichtigen, ohne dass die Einbeziehung von Standortdaten unzulässig ist (vgl. Rn. 237).

b) Bewertung der Gesetzentwürfe

Der besonderen Schwere des Eingriffs trägt der Gesetzgeber zunächst dadurch Rechnung, dass er die Voraussetzungen für die Erhebung von Standortdaten gegenüber der gegenwärtigen Rechtslage verschärft. Anders als zuvor soll zur Ermittlung des Aufenthaltsortes einer Person nicht mehr auf zu geschäftlichen Zwecken gespeicherte Verkehrsdaten zurückgegriffen werden dürfen. Von den Telekommunikationsdienstanbietern gespeicherte Standortdaten dürfen künftig ausschließlich unter den strengeren Voraussetzungen des § 100g Abs. 2 TKG-E erhoben werden. Eine Erhebung von zu geschäftlichen Zwecken gespeicherten Standortdaten gemäß § 100g Abs. 1 StPO-E ist nunmehr ausschließlich für die Zukunft oder in Echtzeit zulässig, § 100g Abs. 1 S. 3 StPO-E.

Der besonderen Schwere des Eingriffs in die Rechte der Betroffenen wird ferner dadurch Rechnung getragen, dass Standortdaten gemäß § 113b Abs. 1 Nr. 2 TKG-E einer kürzeren Speicherfrist von lediglich vier Wochen – gegenüber zehn Wochen für sonstige Verkehrsdaten – unterliegen.

9. Richtervorbehalt

a) Anforderungen des Bundesverfassungsgerichts

Mit Blick auf die Gewährleistung effektiven Rechtsschutzes für die Betroffenen fordert das Bundesverfassungsgericht insbesondere, dass die Abfrage oder Übermittlung der Verkehrsdaten aufgrund der Schwere des Grundrechtseingriffs grundsätzlich unter Richtervorbehalt zu stellen sind (Rn. 248):

Nach der Rechtsprechung des Bundesverfassungsgerichts kann bei Ermittlungsmaßnahmen, die einen schwerwiegenden Grundrechtseingriff bewirken, verfassungsrechtlich eine vorbeugende Kontrolle durch eine unabhängige Instanz geboten sein. Dies gilt insbesondere, wenn der Grundrechtseingriff heimlich erfolgt und für den Betroffenen unmittelbar nicht wahrnehmbar ist … Für die Abfrage und Übermittlung von Telekommunikationsverkehrsdaten kann dies der Fall sein. Angesichts des Gewichts des hierin liegenden Eingriffs reduziert sich der Spielraum des Gesetzgebers dahingehend, dass solche Maßnahmen grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen sind. Richter können aufgrund ihrer persönlichen und sachlichen Unabhängigkeit und ihrer ausschließlichen Bindung an das Gesetz die Rechte des Betroffenen im Einzelfall am besten und sichersten wahren … Eine Ausnahme gilt nach Art. 10 Abs. 2 Satz 2 GG für die Kontrolle von Eingriffen in die Telekommunikationsfreiheit durch die Nachrichtendienste. Hier kann an die Stelle einer vorbeugenden richterlichen Kontrolle die

– gleichfalls spezifisch auf die jeweilige Maßnahme bezogene – Kontrolle durch ein von der Volksvertretung bestelltes Organ oder Hilfsorgan treten …

b) Bewertung der Gesetzentwürfe

Die Gesetzentwürfe genügen den verfassungsrechtlichen Anforderungen. § 101a Abs. 1 S. 1 StPO-E verweist für die Erhebung von Verkehrsdaten gemäß § 100g StPO-E auf die §§ 100a Abs. 3, 100b Abs. 1–4 StPO. Die Durchführung einer Maßnahme bedarf daher grundsätzlich der richterlichen Anordnung. Eine ausnahmsweise Anordnung durch die Staatsanwaltschaft kommt grundsätzlich nur bei Gefahr im Verzug in Betracht, § 100b Abs. 1 S. 2 StPO. Diese Ausnahme soll jedoch gemäß § 101a Abs. 1 S. 2 StPO-E auf die Erhebung von gemäß § 113b TKG-E gespeicherten Daten keine Anwendung finden, sondern lediglich für die Erhebung von zu geschäftlichen Zwecken gespeicherten Verkehrsdaten gemäß § 100g Abs. 1 StPO-E zulässig sein. Die Durchführung einer Ermittlungsmaßnahme gemäß § 100g Abs. 2 StPO-E unterliegt hingegen uneingeschränkt dem Vorbehalt richterlicher Anordnung.

10. Transparenz

a) Anforderungen des Bundesverfassungsgerichts

Die Verwendung von vorsorglich anlasslos gespeicherten Verkehrsdaten ermöglicht es, tiefgehende Einblicke in das Privatleben der Bürger zu erhalten, ohne dass diese davon Kenntnis erlangen. Das Bundesverfassungsgericht knüpft die Verwendung solcher Datenbestände daher an eine hinreichende Transparenz (Rn. 240 ff.):

Zu den Voraussetzungen der verfassungsrechtlich unbedenklichen Verwendung von durch eine solche Speicherung gewonnenen Daten gehören Anforderungen an die Transparenz. Soweit möglich muss die Verwendung der Daten offen erfolgen. Ansonsten bedarf es grundsätzlich zumindest nachträglich einer Benachrichtigung der Betroffenen. Unterbleibt ausnahmsweise auch diese, bedarf die Nichtbenachrichtigung einer richterlichen Entscheidung.

Eine vorsorglich anlasslose Speicherung aller Telekommunikationsverkehrsdaten über sechs Monate ist unter anderem deshalb ein so schwerwiegender Eingriff, weil sie ein Gefühl des ständigen Überwachtwerdens hervorrufen kann; sie erlaubt in unvorhersehbarer Weise tiefe Einblicke in das Privatleben, ohne dass der Rückgriff auf die Daten für den Bürger unmittelbar spürbar oder ersichtlich ist. Der Einzelne weiß nicht, was welche staatliche Behörde über ihn weiß, weiß aber, dass die Behörden vieles, auch Höchstpersönliches über ihn wissen können.

Der Gesetzgeber muss die diffuse Bedrohlichkeit, die die Datenspeicherung hierdurch erhalten kann, durch wirksame Transparenzregeln auffangen ...

Zu den Transparenzanforderungen zählt der Grundsatz der Offenheit der Erhebung und Nutzung von personenbezogenen Daten. Eine Verwendung der Daten ohne Wissen des Betroffenen ist verfassungsrechtlich nur dann zulässig, wenn andernfalls der Zweck der Untersuchung, dem der Datenabruf dient, vereitelt wird. Für die Gefahrenabwehr und die Wahrnehmung der Aufgaben der Nachrichtendienste darf der Gesetzgeber dies grundsätzlich annehmen. Demgegenüber kommt im Rahmen der Strafverfolgung auch eine offene Erhebung und Nutzung der Daten in Betracht (vgl. § 33 Abs. 3 und 4 StPO). Ermittlungsmaßnahmen werden hier zum Teil auch sonst mit Kenntnis des Beschuldigten und in seiner Gegenwart durchgeführt (vgl. zum Beispiel §§ 102, 103, 106 StPO). Dementsprechend ist der Betroffene vor der Abfrage beziehungsweise Übermittlung seiner Daten grundsätzlich zu benachrichtigen. Eine heimliche Verwendung der Daten darf nur vorgesehen werden, wenn sie im Einzelfall erforderlich und richterlich angeordnet ist.

b) Bewertung der Gesetzentwürfe

Die Gesetzentwürfe enthalten verschiedene Regelungen, um die Transparenz der Erhebung anlasslos systematisch gespeicherter Verkehrsdaten zu gewährleisten.

Die Betroffenen sind gemäß § 101a Abs. 6 S. 1 StPO-E von der Erhebung der Verkehrsdaten zu benachrichtigen. Ein Unterbleiben oder Zurückstellen der Benachrichtigung darf gemäß § 101a Abs. 6 S. 2 StPO-E nur auf Anordnung des zuständigen Gerichts erfolgen. Der genaue Zeitpunkt der Benachrichtigung des Betroffenen lässt sich den Gesetzentwürfen nicht ausdrücklich entnehmen. Dies weckt mitunter die Befürchtung, der Entwurf führe in der Praxis zu einer Umkehrung des vom Bundesverfassungsgericht geforderten Regel-Ausnahme-Verhältnisses.[25] Gemäß § 100g StPO-E soll jedoch die Erhebung von vorsorglich gespeicherten Verkehrsdaten grundsätzlich offen erfolgen. Die Betroffenen sind daher – wie auch die Gesetzesbegründung noch einmal ausdrücklich klarstellt[26]– bereits vor der Anordnung der Datenerhebung gemäß § 33 StPO anzuhören. Von dieser Anhörung darf das Gericht nur ausnahmsweise in den Fällen des § 33 Abs. 4 StPO absehen, insbesondere dann, wenn eine vorherige Anhörung den Zweck der Anordnung gefährden würde. Das Unterbleiben der Benachrichtigung im Rahmen der Anhörung gemäß § 33 StPO bedarf somit in jedem Falle der richterlichen Anordnung. Auch nach Anordnung der Maßnahme durch das Gericht ist der Betroffene gemäß § 101a Abs. 6 S. 1 StPO-E von der Durchführung der Maßnahme zu unterrichten, wobei die Benachrichtigung der Gesetzesbegründung zufolge noch vor Beginn der Maßnahme zu erfolgen hat.[27] Die Zurückstellung der Benachrichtigung bedarf wiederum der gerichtlichen Anordnung, § 101a Abs. 6 S. 2 StPO-E. Dass diese Regelung in der Praxis zu der befürchteten Umkehrung des Regel-Ausnahme-Verhältnisses führen soll, ist daher nicht ersichtlich. Zur Klarstellung ist zu erwägen, den Wortlaut des § 101a Abs. 6 S. 1 StPO-E dahingehend zu ändern, dass eine Benachrichtigung des Betroffenen „grundsätzlich vor“ Erhebung der Daten zu erfolgen hat.[28]

Um die Transparenz der Ermittlungsmaßnahmen gemäß § 100g StPO-E weiter zu steigern, sieht § 101b StPO-E vor, dass die Erhebung der Verkehrsdaten umfassend statistisch zu erfassen ist.

---

[25] Stellungnahme der BfDI zum Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, 2015, S. 18. Siehe auch die Ausarbeitung der Wissenschaftlichen Dienste des Bundestags über die Umsetzung der Vorgaben des Bundesverfassungsgerichts zur Vorratsdatenspeicherung durch den Gesetzentwurf der Bundesregierung vom 27. Mai 2015, 2015, S. 18 f.

[26] Begründung des Gesetzentwurfs, BT-Drs. 18/5088, S. 36.

[27] Begründung des Gesetzentwurfs, BT-Drs. 18/5088, S. 36.

[28] Vgl. auch die Ausarbeitung der Wissenschaftlichen Dienste des Bundestags über die Umsetzung der Vorgaben des Bundesverfassungsgerichts zur Vorratsdatenspeicherung durch den Gesetzentwurf der Bundesregierung vom 27. Mai 2015, 2015, S. 18 f.

Die statistische Erfassung soll sowohl einen Überblick über das Ausmaß der entsprechenden Ermittlungsmaßnahmen verschaffen als auch ihre bessere Evaluierung ermöglichen.

Im Ergebnis ist daher festzuhalten, dass die Gesetzentwürfe den vom Bundesverfassungsgericht gestellten Anforderungen an die Transparenz der Erhebung anlasslos vorsorglich gespeicherter Verkehrsdaten gerecht werden.

11. Klarstellungspotential

Obgleich die Gesetzentwürfe die in der Entscheidung des Bundesverfassungsgerichts vom 2.3.2010 herausgearbeiteten Grundsatzanforderungen wahren, sind – in Zusammenfassung der vorstehenden Ausführungen – Klarstellungen hinsichtlich folgender Punkte zu erwägen:

- Umfang der Speicherpflicht: Einbeziehung moderner Kommunikationsangebote (II.3.b);
- Datenlöschung: Zulässigkeit der Verwendung von Verkehrsdaten nach Ablauf der Höchstspeicherfrist (II.5.b);
- Terminologie: Einheitliche Verwendung der Bezeichnung „Verkehrsdaten“ (II.5.b, Fn. 10);
- Datenlöschung: Löschungspflicht für von vornherein unerhebliche Daten (II.5.b);
- Transparenz: Zeitpunkt der Benachrichtigung des Betroffenen vor Abruf gespeicherter Verkehrsdaten (II.10.b).

III. Unions(grund)rechtlicher Rahmen

Hinsichtlich des unions(grund)rechtlichen Rahmens stellt sich schon die Frage, ob die Unionsgrundrechte auch nach Nichtigerklärung der Vorratsdatenspeicherungs-Richtlinie 2006/24/EG[29] durch den Europäischen Gerichtshof (EuGH)[30] auf nationale Regelungen zur Verkehrsdatenspeicherung überhaupt anwendbar und damit die vom EuGH ausbuchstabierten unionsgrundrechtlichen Anforderungen einschlägig sind; dies ist zweifelhaft (1.). Unabhängig davon lässt sich dem Urteil des EuGH kein zwingendes unionsgrundrechtliches Verbot der Verkehrsdatenspeicherung entnehmen, vielmehr erscheinen die Gesetzentwürfe jedenfalls unionsgrundrechtlich vertretbar (2.).

---

[29] Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG.

[30] EuGH, Urteil vom 8.4.2014, C-293/12 u. C-594/12 – Digital Rights Ireland Ltd.

1. Fragliche Anwendbarkeit der Unionsgrundrechte

Gemäß Art. 51 Abs. 1 S. 1 GRCh bindet die Grundrechtecharta die Mitgliedstaaten der Europäischen Union ausschließlich bei der Durchführung des Rechts der Union. Ob hiervon nach der Ungültigerklärung der Richtlinie 2006/24/EG durch den Gerichtshof der Europäischen Union noch die Rede sein kann, erscheint fraglich. Zunächst erfolgt die Einführung einer Pflicht zur vorsorglichen Speicherung von Verkehrsdaten gerade nicht mehr zur Umsetzung unionsrechtlicher Vorgaben, sondern beruht auf einer eigenen Entscheidung des nationalen Gesetzgebers.

Für den Bereich des Datenschutzes bestehen jedoch weiterhin unionsrechtliche Vorgaben, namentlich diejenigen der Richtlinie 2002/58/EG[31], aus denen sich die Anwendbarkeit der Grundrechtecharta ergeben könnte. So sind die Mitgliedstaaten gemäß Art. 5 Abs. 1 der Richtlinie 2002/58/EG grundsätzlich verpflichtet, die Vertraulichkeit aller mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten zu gewährleisten:

> Die Mitgliedstaaten stellen die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch innerstaatliche Vorschriften sicher. Insbesondere untersagen sie das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer, wenn keine Einwilligung der betroffenen Nutzer vorliegt, es sei denn, dass diese Personen gemäß Artikel 15 Absatz 1 gesetzlich dazu ermächtigt sind …

Eine Abweichung der Mitgliedstaaten von ihrer Verpflichtung kommt daher nur mit Einwilligung der betroffenen Nutzer oder nach Maßgabe des Art. 15 Abs. 1 RL 2002/58/EG in Betracht. Letzterer bestimmt:

> [1]Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5 … dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für die nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. [2]Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. [3]Alle in diesem Absatz genannten Maßnahmen müssen den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen.

Hieraus könnte man nun folgern, dass die Verkehrsdatenspeicherung vom Anwendungsbereich des Unionsrechts erfasst ist. Insoweit ist freilich zu bedenken, dass eine Bindung der Mitgliedstaaten an die Unionsgrundrechte nicht bereits bei jedweden Bezug zum Unionsrecht gegeben ist. Dies schlägt sich schon im restriktiv gefassten Wortlaut des Art. 51 Abs. 1 Satz 1 GRCh

---

[31] 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.

nieder („ausschließlich"), ferner in den in der Grundrechtecharta enthaltenen Kompetenzvorbehalten zugunsten der Mitgliedstaaten (Art. 51 Abs. 1 S. 1 und 2, Abs. 2; Art. 52 Abs. 5 S. 1 GRCh). Hinzu kommt der mit einer Grundrechtsbindung einhergehende Unitarisierungseffekt, zumal dieser die Einräumung von Gestaltungsspielräumen in Frage stellt.[32] Vor diesem Hintergrund bedarf es eines durch Unionsrecht hinreichend determinierten Sachverhalts.[33] Auch in seinem Urteil zur Anti-Terror-Datei hat das Bundesverfassungsgericht betont: „Insofern darf die Entscheidung (gemeint ist die Entscheidung des EuGH vom 26.2.2013, C-617/10 – Fransson, Anm. d. Verfassers) nicht in einer Weise verstanden und angewendet werden, nach der für eine Bindung der Mitgliedstaaten durch die in der Grundrechtecharta niedergelegten Grundrechte der Europäischen Union jeder sachliche Bezug einer Regelung zum bloß abstrakten Anwendungsbereich des Unionsrechts oder rein tatsächliche Auswirkungen auf dieses ausreiche. Vielmehr führt der Europäische Gerichtshof auch in dieser Entscheidung ausdrücklich aus, dass die Europäischen Grundrechte der Charta nur in ‚unionsrechtlich geregelten Fallgestaltungen, aber nicht außerhalb derselben Anwendung finden'."[34]

Die Ausnahmevorschrift in Art. 15 Abs. 1 RL 2002/58/EG könnte nun für einen unionsrechtlich hinreichend determinierten Sachverhalt sprechen.[35] Insoweit zu berücksichtigen ist freilich, dass die Richtlinie selbst ausweislich ihres Art. 1 Abs. 3 nicht gilt für „Tätigkeiten, die nicht in den Anwendungsbereich des Vertrags zur Gründung der Europäischen Gemeinschaft fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, und auf keinen Fall für Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Tätigkeit die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich."

---

[32] Vgl. *J. Masing*, JZ 2015, S. 477 (485 ff.); *F. Wollenschläger*, Grundrechtsschutz und Unionsbürgerschaft, in: Hatje/Müller-Graff (Hrsg.), Enzyklopädie Europarecht I, 2014, § 8 Rn. 31.

[33] Vgl. etwa EuGH, Urteil vom 6.3.2014, Rs. C-206/13, Rn. 26 f. – Siragusa; Urteil vom 10.7.2014, Rs. C-198/13, Rn. 35 – Hernández, Urteil vom 11.11.2014, Rs. C-333/13, Rn. 87 ff. – Dano. Weiter: EuGH, Urteil vom 26.2.2013, Rs. C-617/10 – Fransson. Umfassend dazu m.w.N. *F. Wollenschläger*, Grundrechtsschutz und Unionsbürgerschaft, in: Hatje/Müller-Graff (Hrsg.), Enzyklopädie Europarecht I, 2014, § 8 Rn. 30 f.

[34] BVerfGE 133, 277 (316).

[35] Dazu und zum Folgenden aus der Literatur – eine Bindung an die Unionsgrundrechte annehmend: *M. Bäcker*, JA 2014, S. 1263 (1272); *F. Boehm/M. D. Cole*, MMR 2014, S. 569 (570); *R. Priebe*, EuZW 2014, S. 456 (458); *A. Roßnagel*, MMR 2014, S. 372 (376); Ausarbeitung der Wissenschaftlichen Dienste des Bundestags zu Europarechtlichen Spielräumen zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten in den Mitgliedstaaten der Europäischen Union, 2015, S. 4 ff.; ferner VerfGH Wien, Entscheidung vom 27.6.2014, G 47/2012, Rn. 144, abrufbar unter: https://www.vfgh.gv.at/cms/vfgh-site/attachments/1/5/8/CH0006/CMS1409900579500/vds_schriftliche_entscheidung.pdf (16.9.2015). Allgemein zur Anwendbarkeit der GRCh auf mitgliedstaatliche Maßnahmen zum Zweck der nationalen Sicherheit auch *M. Schlikker*, NJOZ 2014, S. 1281 (1282). A.A. *C. D. Classen*, EuR 2014, S. 441 (447). Siehe ferner *W. Ewer/T. Thienel*, NJW 2014, S. 30 (33 f.).

Zweifelsohne steht diese Regelung in einem latenten Spannungsverhältnis zur Regelung des Art. 15 Abs. 1 S. 1 RL 2002/58/EG, der Maßnahmen aus den in Art. 1 Abs. 3 RL 2002/58/EG genannten Gründen, namentlich im polizei- und strafrechtlichen Bereich, zulässt und an Kautelen knüpft. Prima facie lässt sich dieses Spannungsverhältnis dadurch auflösen, dass man die Speicherung der Verkehrsdaten durch die Telekommunikationsunternehmen von deren Abruf durch Strafverfolgungs- und Sicherheitsbehörden trennt und ersteres, nicht aber Letzteres der Richtlinie unterstellt.[36] Dem entgegenzuhalten ist indes, dass es wegen des untrennbaren Zusammenhangs der sicherheitsrechtlich motivierten Pflicht zur Datenspeicherung mit dem demselben Zweck dienenden Abruf der Daten fragwürdig erscheint, beide Regelungen verschiedenen Grundrechtsregimes zu unterstellen. Die Grundrechtskonformität der Datenspeicherung lässt sich nicht ohne Berücksichtigung der Verwendungszwecke beurteilen, zu denen die Daten gespeichert werden. Dies illustriert die EuGH-Entscheidung zur Vorratsdatenspeicherung eindrücklich, die sich gegen eine parzellierte Grundrechtsbetrachtung ausgesprochen hat und dem Unionsgesetzgeber sogar aus Gründen des Grundrechtsschutzes angelastet hat, zu wenig im Bereich des Datenabrufs zu regeln. Insbesondere habe die Richtlinie selbst kein objektives Kriterium vorgesehen, den Zugang der Behörden zu den Daten auf Straftaten zu beschränken, „die im Hinblick auf das Ausmaß und die Schwere des Eingriffs in die in Art. 7 und Art. 8 der Charta verankerten Grundrechte als hinreichend schwer angesehen werden können, um einen solchen Eingriff zu rechtfertigen“.[37]

Es spricht daher viel dafür, Art. 15 Abs. 1 RL 2002/58/EG als klarstellende Öffnungsklausel zugunsten der Mitgliedstaaten zu sehen, trotz der den Telekommunikationsunternehmen aufzuerlegenden Datenschutzpflichten Regelungen der Verkehrsdatenspeicherung einzuführen. Erwägungsgrund 11 der Richtlinie legt ein entsprechendes Verständnis nahe, wenn er Art. 15 Abs. 1 RL 2002/58/EG in Zusammenhang mit Art. 1 Abs. 3 RL 2002/58/EG sieht:

> Wie die Richtlinie 95/46/EG gilt auch die vorliegende Richtlinie nicht für Fragen des Schutzes der Grundrechte und Grundfreiheiten in Bereichen, die nicht unter das Gemeinschaftsrecht fallen. Deshalb hat sie keine Auswirkungen auf das bestehende Gleichgewicht zwischen dem Recht des Einzelnen auf Privatsphäre und der Möglichkeit der Mitgliedstaaten, Maßnahmen nach Artikel 15 Absatz 1 dieser Richtlinie zu ergreifen, die für den Schutz der öffentlichen Sicherheit, für die Landesverteidigung, für die Sicherheit des Staates (einschließlich des wirtschaftlichen Wohls des Staates, soweit die Tätigkeiten die Sicherheit des Staates berühren) und für die Durchsetzung strafrechtlicher Bestimmungen erforderlich sind. Folglich betrifft diese Richtlinie nicht die Möglichkeit der Mitgliedstaaten zum rechtmäßigen Abfangen elektronischer Nachrichten oder zum Ergreifen anderer Maßnahmen,

---

[36] Vgl. das Gutachten des Juristischen Dienstes des Europäischen Parlaments vom 22.12.2014, LIBE – Questions relating to the judgement of the Court of Justice of 8 April 2014 in Joined Cases C-293/12 and C-549/12, *Digital Rights Ireland* and *Seitlinger and others* – Directive 2006/24/EC on data retention – Consequences of the judgement, SJ-0890/14, S. 15 ff., abrufbar unter: https://netzpolitik.org/wp-upload/2014-12-22_SJ-0890-14_Legal_opinion.pdf (16.9.2015).

[37] EuGH, Urteil vom 8.4.2014, C-293/12 u. C-594/12, Rn. 60 – Digital Rights Ireland Ltd.

sofern dies erforderlich ist, um einen dieser Zwecke zu erreichen, und sofern dies im Einklang mit der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten in ihrer Auslegung durch die Urteile des Europäischen Gerichtshofs für Menschenrechte erfolgt. Diese Maßnahmen müssen sowohl geeignet sein als auch in einem strikt angemessenen Verhältnis zum intendierten Zweck stehen und ferner innerhalb einer demokratischen Gesellschaft notwendig sein sowie angemessenen Garantien gemäß der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten entsprechen.

Als klarstellende Öffnungsklausel vermag Art. 15 Abs. 1 Satz 3 RL 2002/58/EG indes, gerade im nur schwach vergemeinschafteten Bereich des Polizei- und Strafrechts, keine Grundrechtsbindung der Mitgliedstaaten auszulösen mangels hinreichender Determinierung des Sachverhalts durch Unionsrecht.

Die Verpflichtung auf die Unionsgrundrechte in Art. 15 Abs. 1 Satz 3 RL 2002/58/EG hat für diese Frage keine weitere Relevanz: Als Sekundärrecht kann diese Regelung nämlich den im Rang des Primärrechts stehenden (vgl. Art. 6 Abs. 1 S. 1 a.E. EUV) Art. 51 Abs. 1 S. 1 GRCh weder einschränken noch erweitern. Damit gilt: Entweder fällt die Verkehrsdatenspeicherung in den Anwendungsbereich des Unionsrechts i.S.d. Art. 51 Abs. 1 S. 1 GRCh oder nicht. Im ersten Fall gibt Art. 15 Abs. 1 Satz 3 RL 2002/58/EG jene Charta-Bestimmung deklaratorisch wieder und hat keine eigenständige Bedeutung, im zweiten Fall widerspricht er Primärrecht und ist nichtig. Überdies bleibt festzuhalten, dass nicht einmal die Richtlinie selbst die Frage nach einer Anwendbarkeit der Unionsgrundrechte widerspruchsfrei beantwortet. Denn der die Regelung des Art. 15 Abs. 1 RL 2002/58/EG erläuternde Erwägungsgrund 11 geht (anders als jener) lediglich von einer Bindung an die EMRK aus, die wiederum Art. 15 Abs. 1 Satz 3 RL 2002/58/EG nicht erwähnt. Dass eine generelle Bindung der Mitgliedstaaten an die EMRK besteht, steht außer Frage, ist deren Anwendungsbereich doch anders als der des Art. 51 Abs. 1 S. 1 GRCh gegenständlich unbeschränkt.[38] Art. 1 EMRK formuliert einschränkungslos: „Die Hohen Vertragsparteien sichern allen ihrer Hoheitsgewalt unterstehenden Personen die in Abschnitt I bestimmten Rechte und Freiheiten zu."

Ginge man von einer Anwendbarkeit der Unionsgrundrechte auf die Mitgliedstaaten aus, wäre schließlich zu berücksichtigen, dass bei Ausfüllung unionsrechtlich nicht determinierter Spielräume den Mitgliedstaaten oftmals ein Ermessensspielraum zuerkannt wird, so dass die EuGH-Entscheidung nicht 1:1 übertragen werden kann.[39]

---

[38] Zur Frage der Anwendbarkeit der EMRK, wenn die Mitgliedstaaten zwingende Vorgaben des Unionsrechts durchführen *F. Wollenschläger*, Grundrechtsschutz und Unionsbürgerschaft, in: Hatje/Müller-Graff (Hrsg.), Enzyklopädie Europarecht I, 2014, § 8 Rn. 37 f.

[39] Vgl. *J. Masing*, JZ 2015, S. 477 (485 f.); kritisch *F. Wollenschläger*, Grundrechtsschutz und Unionsbürgerschaft, in: Hatje/Müller-Graff (Hrsg.), Enzyklopädie Europarecht I, 2014, § 8 Rn. 75 ff.

2. Kein zwingendes unionsrechtliches Verbot der Verkehrsdatenspeicherung

Das Urteil des EuGH zur Verkehrsdatenspeicherung wird überdies oftmals dahin interpretiert, dass der Gerichtshof dieser einen unionsgrundrechtlichen Riegel vorgeschoben habe.[40] Diese Interpretation geht zu weit. Denn weder enthält das Urteil einen derartigen Ausspruch unmittelbar noch lässt er sich aus den Erwägungen des Gerichtshofs ableiten. Vielmehr hat der EuGH die Unverhältnismäßigkeit der angegriffenen Regelung in Gesamtabwägung einer Vielzahl von grundrechtlich problematisierten Umständen ausgesprochen (Rn. 69):

> Aus der Gesamtheit der vorstehenden Erwägungen ist zu schließen, dass der Unionsgesetzgeber beim Erlass der Richtlinie 2006/24 die Grenzen überschritten hat, die er zur Wahrung des Grundsatzes der Verhältnismäßigkeit im Hinblick auf die Art. 7, 8 und 52 Abs. 1 der Charta einhalten musste.

Es lässt sich dem Urteil indes nicht entnehmen, dass bereits einzelne grundrechtlich problematisierte Aspekte der Regelung – namentlich die anlasslose Speicherung – für sich genommen die Unionsgrundrechtswidrigkeit der Verkehrsdatenspeicherung begründen würden. Eine Extrapolation des Urteils auf die hier zu beurteilenden Gesetzentwürfe bewegt sich folglich im Bereich des Spekulativen. Anders als das Bundesverfassungsgericht formulierte der Gerichtshof ja auch keine konkreten Voraussetzungen, unter denen eine vorsorgliche Speicherung von Verkehrsdaten zulässig ist.[41]

Blickt man auf die geplante Regelung im Lichte des Urteils, so ist zunächst festzuhalten, dass der EuGH eine Verletzung des Wesensgehalts der Art. 7 f. GRCh verneint (a) und auch an der Eignung der Verkehrsdatenspeicherung keine Zweifel angemeldet hat (b). Hinzu kommt, dass die zu beurteilenden Gesetzentwürfe Einwänden des Gerichtshofs Rechnung tragen, namentlich der gebotenen Beschränkung der Verwendungszwecke (c), dem Schutz von Berufsgeheimnisträgern (d), den materiell- und verfahrensrechtliche Anforderungen für den Zugang zu Datenbeständen (e) sowie der Datensicherheit (f). Dass trotz alldem allein die ebenfalls problematisierte Anlasslosigkeit der Speicherung zur Unionsgrundrechtswidrigkeit führt, ist fraglich; vielmehr erscheinen die Gesetzentwürfe jedenfalls unionsgrundrechtlich vertretbar (g).

---

[40] Vgl. den Antrag der Abgeordneten Korte, Hahn, Jelpke, Kunert, Pau, Petzold, Renner, Steinke, Tempel, Wawzyniak und der Fraktion DIE LINKE, BT-Drs. 18/4971, S. 3; *G. Otto/M. Seitlinger*, MR-Int 2014, S. 22 (22 f.); *I. Spiecker gen. Döhmann*, JZ 2014, S. 1109 (1112); *H. A. Wolff*, DÖV 2014, S. 608 (610). A.A. *W. Durner*, DVBl. 2014, S. 712 (714); *N. Härting*, BB 2014, S. 1105 (1105); *S. Simitis*, NJW 2014, S. 2158 (2160).

[41] So auch Ausarbeitung der Wissenschaftlichen Dienste des Bundestags zu Europarechtlichen Spielräumen zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten in den Mitgliedstaaten der Europäischen Union, 2015, S. 14.

a) Wahrung des Wesensgehalts (Art. 52 Abs. 1 S. 1 GRCh)

Der Gerichtshof der Europäischen Union stellte in seiner Entscheidung zur Vorratsdatenspeicherungsrichtlinie zunächst fest, dass die anlasslose vorsorgliche Speicherung von Verkehrsdaten keinen Eingriff in den unantastbaren Wesensgehalt der Art. 7 f. GRC darstelle (Rn. 39 f.):

> Zum Wesensgehalt des Grundrechts auf Achtung des Privatlebens und der übrigen in Art. 7 der Charta verankerten Rechte ist festzustellen, dass die nach der Richtlinie 2006/24 vorgeschriebene Vorratsspeicherung von Daten zwar einen besonders schwerwiegenden Eingriff in diese Rechte darstellt, doch nicht geeignet ist, ihren Wesensgehalt anzutasten, da die Richtlinie, wie sich aus ihrem Art. 1 Abs. 2 ergibt, die Kenntnisnahme des Inhalts elektronischer Kommunikation als solchen nicht gestattet.
>
> Die Vorratsspeicherung von Daten ist auch nicht geeignet, den Wesensgehalt des in Art. 8 der Charta verankerten Grundrechts auf den Schutz personenbezogener Daten anzutasten, weil die Richtlinie 2006/24 in ihrem Art. 7 eine Vorschrift zum Datenschutz und zur Datensicherheit enthält, nach der Anbieter von öffentlich zugänglichen elektronischen Kommunikationsdiensten bzw. Betreiber eines öffentlichen Kommunikationsnetzes, unbeschadet der zur Umsetzung der Richtlinien 95/46 und 2002/58 erlassenen Vorschriften, bestimmte Grundsätze des Datenschutzes und der Datensicherheit einhalten müssen. Nach diesen Grundsätzen stellen die Mitgliedstaaten sicher, dass geeignete technische und organisatorische Maßnahmen getroffen werden, um die Daten gegen zufällige oder unrechtmäßige Zerstörung sowie zufälligen Verlust oder zufällige Änderung zu schützen.

b) Eignung

Auch der Gerichtshof sah die vorsorgliche Verkehrsdatenspeicherung als grundsätzlich geeignet an, schwere Kriminalität zu bekämpfen und somit zur Wahrung der öffentlichen Sicherheit beizutragen (Rn. 41 f.):

> Zu der Frage, ob die Vorratsspeicherung der Daten zur Erreichung des mit der Richtlinie 2006/24 verfolgten Ziels geeignet ist, ist festzustellen, dass angesichts der wachsenden Bedeutung elektronischer Kommunikationsmittel die nach dieser Richtlinie auf Vorrat zu speichernden Daten den für die Strafverfolgung zuständigen nationalen Behörden zusätzliche Möglichkeiten zur Aufklärung schwerer Straftaten bieten und insoweit daher ein nützliches Mittel für strafrechtliche Ermittlungen darstellen. Die Vorratsspeicherung solcher Daten kann somit als zur Erreichung des mit der Richtlinie verfolgten Ziels geeignet angesehen werden.
>
> Diese Beurteilung kann nicht durch den … Umstand in Frage gestellt werden, dass es mehrere elektronische Kommunikationsweisen gebe, die nicht in den Anwendungsbereich der Richtlinie 2006/24 fielen oder die eine anonyme Kommunikation ermöglichten. Dieser Umstand vermag zwar die Eignung der in der Vorratsspeicherung der Daten bestehenden Maßnahme zur Erreichung des verfolgten Ziels zu begrenzen, führt aber, wie der Generalanwalt in Nr. 137 seiner Schlussanträge ausgeführt hat, nicht zur Ungeeignetheit dieser Maßnahme.

c) Verwendung nur zur Bekämpfung schwerer Straftaten

Der Gerichtshof bemängelte, dass die streitgegenständliche Regelung kein objektives Kriterium enthalte, das den Zugang zu den Datenbeständen und ihre Verwendung auf die Verfolgung hinreichend gewichtiger Straftaten beschränke (Rn. 60):

> Zweitens kommt zu diesem generellen Fehlen von Einschränkungen hinzu, dass die Richtlinie 2006/24 kein objektives Kriterium vorsieht, das es ermöglicht, den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung zwecks Verhütung, Feststellung oder strafrechtlicher Verfolgung auf Straftaten zu beschränken, die im Hinblick auf das Ausmaß und die Schwere des Eingriffs in die in Art. 7 und Art. 8 der Charta verankerten Grundrechte als hinreichend schwer angesehen werden können, um einen solchen Eingriff zu rechtfertigen. Die Richtlinie 2006/24 nimmt im Gegenteil in ihrem Art. 1 Abs. 1 lediglich allgemein auf die von jedem Mitgliedstaat in seinem nationalen Recht bestimmten schweren Straftaten Bezug.

Im Gegensatz zur Richtlinie 2006/24, die eine Verwendung der Datenbestände allgemein zur Verfolgung von im jeweiligen Recht der Mitgliedstaaten bestimmten schweren Straftaten vorsah, soll die Datenerhebung im Bereich der Strafverfolgung gemäß § 100g Abs. 2 StPO-E ausschließlich zur Verfolgung der abschließend aufgezählten besonders schweren Straftaten zulässig sein. Es handelt sich hierbei um Straftaten zur Terrorismusbekämpfung oder zum Schutz höchstpersönlicher Rechtsgüter. Darüber hinaus ist die Erhebung gemäß § 100g Abs. 2 S. 1 StPO-E nur zulässig, wenn die Straftat auch im Einzelfall als besonders schwerwiegend anzusehen ist, die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts des Beschuldigten auf andere Weise erheblich erschwert oder aussichtslos wäre und die Erhebung der Daten auch nicht außer Verhältnis zur Bedeutung der Sache steht.

Die Gesetzentwürfe entsprechen somit der vom Gerichtshof geforderten Beschränkung des Zugangs zu den Datenbeständen sowie ihrer Verwendung auf die Verfolgung hinreichend gewichtiger Straftaten.

d) Schutz von Berufsgeheimnisträgern

Des Weiteren hat der Gerichtshof beanstandet, dass die Richtlinie Ausnahmen zum Schutz von Berufsgeheimnisträgern vermissen lasse (Rn. 58): „Zudem sieht sie keinerlei Ausnahme vor, so dass sie auch für Personen gilt, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen."

Demgegenüber enthalten die vorliegend zu beurteilenden Gesetzentwürfe, wie bereits gezeigt, konkrete Maßnahmen zum Schutz von Berufsgeheimnisträgern. Zum einen werden gemäß § 113b Abs. 6 TKG-E Daten über die in § 99 Abs. 2 TKG genannten Verbindungen bereits grundsätzlich von der Speicherpflicht ausgenommen. Zum anderen werden Berufsgeheimnisträger auch auf der Verwertungsebene durch die Regelung des § 100g Abs. 4 StPO-E hinreichend geschützt.[42]

e) Materiell- und verfahrensrechtliche Anforderungen für den Zugang zu Datenbeständen

Mit Blick auf die Regelungen über den Zugang zu den angelegten Datenbeständen stellte der Gerichtshof verschiedene sowohl materiell- als auch verfahrensrechtliche Defizite fest. Zu-

[42] Strenger Ausarbeitung der Wissenschaftlichen Dienste des Bundestags zu Europarechtlichen Spielräumen zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten in den Mitgliedstaaten der Europäischen Union, 2015, S. 18.

nächst rügte er dabei das Fehlen einer Beschränkung des Kreises der Zugangsberechtigten sowie einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle (Rn. 61 f.):

> Überdies enthält die Richtlinie 2006/24 keine materiell- und verfahrensrechtlichen Voraussetzungen für den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung. Art. 4 der Richtlinie, der den Zugang dieser Behörden zu den auf Vorrat gespeicherten Daten regelt, bestimmt nicht ausdrücklich, dass der Zugang zu diesen Daten und deren spätere Nutzung strikt auf Zwecke der Verhütung und Feststellung genau abgegrenzter schwerer Straftaten oder der sie betreffenden Strafverfolgung zu beschränken sind, sondern sieht lediglich vor, dass jeder Mitgliedstaat das Verfahren und die Bedingungen festlegt, die für den Zugang zu den auf Vorrat gespeicherten Daten gemäß den Anforderungen der Notwendigkeit und der Verhältnismäßigkeit einzuhalten sind.
>
> Insbesondere sieht die Richtlinie 2006/24 kein objektives Kriterium vor, das es erlaubt, die Zahl der Personen, die zum Zugang zu den auf Vorrat gespeicherten Daten und zu deren späterer Nutzung befugt sind, auf das angesichts des verfolgten Ziels absolut Notwendige zu beschränken. Vor allem unterliegt der Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten keiner vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle, deren Entscheidung den Zugang zu den Daten und ihre Nutzung auf das zur Erreichung des verfolgten Ziels absolut Notwendige beschränken soll und im Anschluss an einen mit Gründen versehenen Antrag der genannten Behörden im Rahmen von Verfahren zur Verhütung, Feststellung oder Verfolgung von Straftaten ergeht. Auch sieht die Richtlinie keine präzise Verpflichtung der Mitgliedstaaten vor, solche Beschränkungen zu schaffen.

Darüber hinaus rügte der Gerichtshof auch das Fehlen von konkreten Vorgaben für die Bemessung der Speicherfrist (Rn. 63 f.):

> Drittens schreibt die Richtlinie 2006/24 hinsichtlich der Dauer der Vorratsspeicherung in ihrem Art. 6 vor, dass die Daten für einen Zeitraum von mindestens sechs Monaten auf Vorrat zu speichern sind, ohne dass eine Unterscheidung zwischen den in Art. 5 der Richtlinie genannten Datenkategorien nach Maßgabe ihres etwaigen Nutzens für das verfolgte Ziel oder anhand der betroffenen Personen getroffen wird.
>
> Die Speicherungsfrist liegt zudem zwischen mindestens sechs Monaten und höchstens 24 Monaten, ohne dass ihre Festlegung auf objektiven Kriterien beruhen muss, die gewährleisten, dass sie auf das absolut Notwendige beschränkt wird.

Die Gesetzentwürfe sehen gemäß § 113c Abs. 1 TKG-E die Übermittlung von Datenbeständen ausschließlich an Strafverfolgungsbehörden, die eine Übermittlung in Verbindung mit der Verfolgung einer besonders schweren Straftat verlangen, oder Gefahrenabwehrbehörden zur Abwehr konkreter Gefahren für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes vor. Darüber hinaus steht die Erhebung von anlasslos auf Vorrat gespeicherten Daten – wie bereits dargestellt – gemäß § 101a Abs. 1 StPO-E in Verbindung mit §§ 100a Abs. 3, 100b Abs. 1–4 StPO vollständig unter dem Vorbehalt richterlicher Anordnung.

Den Bedenken des Gerichtshofs wird schließlich auch dahingehend Rechnung getragen, dass § 113b Abs. 1 TKG-E allgemein eine feste Speicherfrist für Verkehrsdaten vorsieht, und dabei zwischen Daten aus öffentlich zugänglichen Telefondiensten, öffentlich zugänglichen Internetdiensten sowie Standortdaten unterscheidet. Während für die erstgenannten Daten eine Speicherfrist von jeweils zehn Wochen vorgesehen ist, wird die Speicherfrist für Standortdaten auf-

grund ihrer besonderen Brisanz auf lediglich vier Wochen beschränkt. Die Richtlinie ließ darüber hinausgehend eine Speicherung von bis zu 24 Monaten zu, mithin für einen fast zehn Mal so langen Zeitraum.

f) Datensicherheit

Der Gerichtshof hat darüber hinaus bemängelt, dass die Richtlinie keine ausreichenden Garantien gegen einen Missbrauch der Daten durch Gewährleistung eines besonders hohen Sicherheitsstandards enthalte und auch eine Vernichtung der Daten nach Ablauf der vorgesehenen Speicherfrist nicht gewährleistet werde. Schließlich sei eine Einhaltung der genannten Erfordernisse nur zu garantieren, wenn auch eine Speicherung der Daten auf dem Gebiet der Europäischen Union sichergestellt werde (Rn. 66 ff.).

Darüber hinaus ist in Bezug auf die Regeln zur Sicherheit und zum Schutz der von den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder den Betreibern eines öffentlichen Kommunikationsnetzes auf Vorrat gespeicherten Daten festzustellen, dass die Richtlinie 2006/24 keine hinreichenden, den Anforderungen von Art. 8 der Charta entsprechenden Garantien dafür bietet, dass die auf Vorrat gespeicherten Daten wirksam vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu ihnen und jeder unberechtigten Nutzung geschützt sind. Erstens sieht Art. 7 der Richtlinie 2006/24 keine speziellen Regeln vor, die der großen nach der Richtlinie auf Vorrat zu speichernden Datenmenge, dem sensiblen Charakter dieser Daten und der Gefahr eines unberechtigten Zugangs zu ihnen angepasst sind. Derartige Regeln müssten namentlich klare und strikte Vorkehrungen für den Schutz und die Sicherheit der fraglichen Daten treffen, damit deren Unversehrtheit und Vertraulichkeit in vollem Umfang gewährleistet sind. Auch sieht die Richtlinie keine präzise Verpflichtung der Mitgliedstaaten vor, solche Regeln zu schaffen.

Art. 7 der Richtlinie 2006/24 in Verbindung mit Art. 4 Abs. 1 der Richtlinie 2002/58 und Art. 17 Abs. 1 Unterabs. 2 der Richtlinie 95/46 gewährleistet nicht, dass die genannten Anbieter oder Betreiber durch technische und organisatorische Maßnahmen für ein besonders hohes Schutz- und Sicherheitsniveau sorgen, sondern gestattet es ihnen u. a., bei der Bestimmung des von ihnen angewandten Sicherheitsniveaus wirtschaftliche Erwägungen hinsichtlich der Kosten für die Durchführung der Sicherheitsmaßnahmen zu berücksichtigen. Vor allem gewährleistet die Richtlinie 2006/24 nicht, dass die Daten nach Ablauf ihrer Speicherungsfrist unwiderruflich vernichtet werden.

Zweitens schreibt die Richtlinie nicht vor, dass die fraglichen Daten im Unionsgebiet auf Vorrat gespeichert werden, so dass es nicht als vollumfänglich gewährleistet angesehen werden kann, dass die Einhaltung der in den beiden vorstehenden Randnummern angesprochenen Erfordernisse des Datenschutzes und der Datensicherheit, wie in Art. 8 Abs. 3 der Charta ausdrücklich gefordert, durch eine unabhängige Stelle überwacht wird. Eine solche Überwachung auf der Grundlage des Unionsrechts ist aber ein wesentlicher Bestandteil der Wahrung des Schutzes der Betroffenen bei der Verarbeitung personenbezogener Daten …

Mit Blick auf den nach den Gesetzentwürfen für die Speicherung und Übermittlung der Datenbestände erforderlichen Sicherheitsstandard kann auf die Ausführungen zur verfassungsrechtlichen Zulässigkeit der Regelung verwiesen werden. Generell wird dabei ein besonders hoher Standard an Datensicherheit und Datenqualität gefordert, der durch konkrete technische Vorgaben gesichert und mittels eines durch die Bundesnetzagentur zu erstellenden und fortlaufend zu aktualisierenden Anforderungskatalogs an den jeweiligen Stand der Technik angepasst werden soll.

Schließlich sehen die Gesetzentwürfe in § 113b Abs. 8 TKG-E vor, dass die Verkehrsdaten innerhalb einer Woche nach Ablauf der vorgesehenen Speicherfrist irreversibel zu löschen sind

oder ihre irreversible Löschung sicherzustellen ist. Die Löschung ist gemäß § 113e Abs. 1 TKG-E zu protokollieren. Ein Verstoß gegen diese Verpflichtung ist gemäß § 149 Abs. 1 Nr. 38 TKG-E zu sanktionieren.

g) Anlasslosigkeit

Weitergehend als das Bundesverfassungsgericht problematisierte der Gerichtshof, dass sich die Regelung auf alle Nutzer elektronischer Kommunikationsmittel gleichermaßen erstrecke, ohne einen Zusammenhang zwischen den gespeicherten Daten oder dem betroffenen Personenkreis und dem Regelungsziel – der Bekämpfung schwerer Kriminalität sowie der Wahrung der öffentlichen Sicherheit – zu fordern (Rn. 57 ff.).

Hierzu ist erstens festzustellen, dass sich die Richtlinie 2006/24 generell auf alle Personen und alle elektronischen Kommunikationsmittel sowie auf sämtliche Verkehrsdaten erstreckt, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des Ziels der Bekämpfung schwerer Straftaten vorzusehen.

Die Richtlinie 2006/24 betrifft nämlich zum einen in umfassender Weise alle Personen, 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. Sie gilt also auch für Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte. Zudem sieht sie keinerlei Ausnahme vor, so dass sie auch für Personen gilt, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen.

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

Mit Blick auf die durch den Gerichtshof bemängelte Streubreite der Speicherpflicht ist zunächst festzuhalten, dass die Gesetzentwürfe eine Erhebung der Datenbestände ausschließlich zur Verfolgung von – abschließend aufgezählten und auch im Einzelfall besonders schwer wiegenden – schweren Straftaten sowie zur Abwehr konkreter Gefahren für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes vorsehen. Insoweit kann auf die oben stehenden Ausführungen zur verfassungsrechtlichen Zulässigkeit der Regelung verwiesen werden. Überdies finden sich Differenzierungen hinsichtlich einzelner Kommunikationsmittel (Ausschluss elektronischer Post; differenzierte Speicherdauer bzgl. einzelner Daten).

An der Anlasslosigkeit der Speicherungspflicht halten die Gesetzentwürfe fest. Dies kennzeichnet die Verkehrsdatenspeicherung im Gegensatz zu Verfahren wie dem des Quick-Freezing. Hieraus lässt sich indes nicht die Unionsgrundrechtswidrigkeit ableiten.[43] Denn anzustellen ist

[43] So auch Ausarbeitung der Wissenschaftlichen Dienste des Bundestags zu Europarechtlichen Spielräumen zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten in den Mitgliedstaaten der Europäischen Union, 2015, S. 17 f.

eine Gesamtabwägung, in die die Anlasslosigkeit als zwar grundrechtsintensiver, aber doch nur ein Aspekt des Eingriffs einzustellen ist. Beurteilt man die Gesetzentwürfe im Lichte des Urteils, so ist festzustellen, dass diese – im Vergleich zur beanstandeten Regelung – in vielerlei Hinsicht grundrechtsschonender ausfallen, was bei einer erneuten Entscheidung des EuGH und der in dieser anzustellenden Gesamtabwägung nicht außer Betracht bleiben kann. Hingewiesen sei auf:

- Speicherfrist: statt einer Speicherfrist von mindestens sechs bis höchstens 24 Monaten ist eine Speicherfrist von lediglich vier bzw. zehn Wochen vorgesehen;
- Speichervolumen: der Bereich der elektronischen Post ist von der Speicherpflicht ausgenommen;
- Berufsgeheimnisträger: Berufsgeheimnisträger werden durch ein Speicherungs- bzw. Verwertungsverbot geschützt;
- Datenverwendung: eine Verwendung der gespeicherten Daten ist nur – und zudem nur als Ultima Ratio – zur Verfolgung abschließend genannter besonders schwerer Straftaten oder zur Abwehr von konkreten Gefahren für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes zulässig;
- Datenabruf: für den Abruf der Daten werden konkrete materiell- und verfahrensrechtliche Vorgaben aufgestellt;
- Datensicherheit: der zu gewährleistende Standard der Datensicherheit wird detailliert vorgegeben;
- Löschung: für die Verfolgung der genannten Straftaten unerhebliche Daten sind unverzüglich zu löschen;
- Richtervorbehalt und Transparenz (Benachrichtigungspflichten).

Auch die Verneinung einer Verletzung des Wesensgehalts (siehe oben) spricht gegen ein Verständnis des Urteils als generelles Verbot einer auch anlasslosen Verkehrsdatenspeicherung. Hinzu kommt, dass keine Aussage im Urteil des EuGH die hier zu beurteilende Unionsgrundrechtswidrigkeit zwingend nahelegt.

Schließlich dürfte die vom EuGH in den Raum gestellte Differenzierung anhand eines bestimmten Zeitraums, geografischen Gebiets oder Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, in der Praxis kaum vergleichbare Ermittlungsmöglichkeiten schaffen. Denn eine solche Regelung setzt – ähnlich dem bereits thematisierten Quick-Freezing-Verfahren – erst zu einem Zeitpunkt an, zu dem bereits ein konkreter Anlass für Maßnahmen besteht. Die Methode ist daher weniger effektiv als eine kontinuierliche Speicherung

von Verkehrsdaten. Darüber hinaus dürfte eine solche Regelung auch erhebliche praktische Probleme mit sich bringen. So erscheint bereits fraglich, nach welchen Kriterien sich das Bestehen oder Nichtbestehen eines hinreichend engen Zusammenhangs eines Gebiets oder Personenkreises zu einer bestimmten schweren Straftat bemisst. Ferner vermag eine solche Differenzierung zwar die Eingriffsintensität mit Blick auf die Art. 7 f. GRCh zu reduzieren, jedoch brächte eine Unterscheidung hinsichtlich des Bestehens der Speicherpflicht anhand bestimmter „gefährlicher Gebiete“ oder „gefährlicher Personenkreise“ neue rechtliche Probleme, insbesondere die Gefahr von Diskriminierungen mit sich. Eine Differenzierung anhand eines hinreichend engen Zusammenhangs zu bestimmten schweren Straftaten stellt daher eine nicht zweifelsfreie Alternative zur anlasslosen kontinuierliche Speicherung von Verkehrsdaten dar.

IV. Würdigung der Mitteilung der Europäischen Kommission

Mit Blick auf die aktuelle Mitteilung der Europäischen Kommission[44] sei ergänzend auf die Pflicht zur Datenspeicherung im Inland (1.) sowie den Umstand, dass polizeiliche und strafprozessuale Maßnahmen der Datenerhebung nicht dem Anwendungsbereich des Unionsrechts unterliegen (2.), eingegangen. Fragen des Schutzes von Berufsgeheimnisträgern und der Geeignetheit wurden bereits erörtert, worauf verwiesen sei (siehe III.2.d bzw. III.2.b).

1. Pflicht zur Datenspeicherung im Inland

Die in einer Pflicht zur Datenspeicherung im Inland liegende Beschränkung der Marktfreiheiten ist nicht per se unionsrechtswidrig, sondern einer Rechtfertigung aus zwingenden Gründen des Allgemeininteresses zugänglich[45]. Zu diesen Rechtfertigungsgründen rechnet der Schutz von Unionsgrundrechten.[46] Angesichts des Anwendungsvorrangs des vom demokratisch legitimierten Unionsgesetzgeber erlassenen Sekundärrechts richtig ist, dass sekundärrechtliche Konkretisierungen nicht unter unmittelbaren Rekurs auf das EU-Primärrecht, namentlich EU-Grundrechte, überspielt werden dürfen, namentlich eine Vollharmonisierung durch Sekundärrecht.[47] Dieser Anwendungsvorrang des Sekundärrechts steht freilich unter dem Vorbehalt der Primärrechtskonformität des Sekundärrechtsakts (siehe nur Art. 51 Abs. 1 S. 1, Art. 52 Abs. 1 GRCh). Insoweit ist zu berücksichtigen, dass der EuGH aus unionsgrundrechtlichen Gründen den bestehenden EU-sekundärrechtlichen Schutz im Kontext der Verkehrsdatenspeicherung in seinem Urteil vom 8.4.2015 für nicht ausreichend erachtet hat (Rn. 66 f.):

> Darüber hinaus ist in Bezug auf die Regeln zur Sicherheit und zum Schutz der von den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder den Betreibern eines öffentlichen Kommunikationsnetzes auf Vorrat gespeicherten Daten festzustellen, dass die Richtlinie 2006/24 keine hinreichenden, den Anforderungen von Art. 8 der Charta entsprechenden Garantien dafür bietet, dass die auf Vorrat gespeicherten Daten wirksam vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu ihnen und jeder unberechtigten Nutzung geschützt sind. Erstens sieht Art. 7 der Richtlinie 2006/24 keine speziellen Regeln vor, die der großen nach der Richtlinie auf Vorrat zu speichernden Datenmenge, dem sensiblen Charakter dieser Daten und der Gefahr eines unberechtigten Zugangs zu ihnen angepasst sind. Derartige Regeln müssten namentlich klare und strikte Vorkehrungen für den Schutz und die Sicherheit der fraglichen Daten treffen, damit deren Unversehrtheit und Vertraulichkeit in vollem Umfang gewährleistet sind. Auch sieht die Richtlinie keine präzise Verpflichtung der Mitgliedstaaten vor, solche Regeln zu schaffen.

---

[44] TRIS/(2015) 02810, so wie abrufbar unter https://netzpolitik.org/2015/wir-veroeffentlichen-stellungnahme-der-eu-kommission-zu-vorratsdatenspeicherung-noch-viele-weitere-maengel/#doc (17.9.2015).

[45] Siehe nur EuGH, Rs. C-55/94, Slg. 1995, I-4165, Rn. 37 – Gebhard; *F. Wollenschläger*, Unionsrechtliche Grundlagen des Öffentlichen Wirtschaftsrechts, in: R. Schmidt/F. Wollenschläger (Hrsg.), Kompendium Öffentliches Wirtschaftsrecht, 4. Aufl. 2015, § 1, Rn. 71.

[46] Siehe nur EuGH, Rs. C-390/12, EU:C:2014:281, Rn. 30 ff. – Pfleger (auch nach Inkrafttreten der GRCh); Rs. C-112/00, Slg. 2003, I-5659, Rn. 74 ff. – Schmidberger; *F. Wollenschläger*, Unionsrechtliche Grundlagen des Öffentlichen Wirtschaftsrechts, in: R. Schmidt/F. Wollenschläger (Hrsg.), Kompendium Öffentliches Wirtschaftsrecht, 4. Aufl. 2015, § 1, Rn. 36, 71.

[47] Siehe nur EuGH, Rs. C-265/12, EU:C:2013:498, Rn. 31 – Citroën Belux NV.

Art. 7 der Richtlinie 2006/24 in Verbindung mit Art. 4 Abs. 1 der Richtlinie 2002/58 und Art. 17 Abs. 1 Unterabs. 2 der Richtlinie 95/46 gewährleistet nicht, dass die genannten Anbieter oder Betreiber durch technische und organisatorische Maßnahmen für ein besonders hohes Schutz- und Sicherheitsniveau sorgen, sondern gestattet es ihnen u. a., bei der Bestimmung des von ihnen angewandten Sicherheitsniveaus wirtschaftliche Erwägungen hinsichtlich der Kosten für die Durchführung der Sicherheitsmaßnahmen zu berücksichtigen. Vor allem gewährleistet die Richtlinie 2006/24 nicht, dass die Daten nach Ablauf ihrer Speicherungsfrist unwiderruflich vernichtet werden.

Vor diesem Hintergrund hängt die Unionsrechtskonformität der Pflicht zur Datenspeicherung im Inland davon ab, ob im EU-Ausland ein den unionsrechtlichen Anforderungen entsprechendes Schutzniveau gewährleistet werden kann. Hiervon kann allein aufgrund des bestehenden EU-sekundärrechtlichen Rahmens nicht ausgegangen werden, wie sich aus der soeben zitierten Passage des EuGH-Urteils ergibt. Vielmehr ist ein solches durch entsprechende Vorgaben im nationalen Recht sicherzustellen. Deren Möglichkeit bedarf einer separaten Prüfung.

Hinsichtlich möglicher Konflikte mit datensicherheitsrechtlichen Anforderungen des Bundesverfassungsgerichts (II.4.) ist zu berücksichtigen, dass, insoweit sich eine Speichermöglichkeit im EU-Ausland (einschließlich eines bestimmten Schutzniveaus) als unionsrechtlich zwingend geboten erweist, nationale Grundrechte – und damit die datensicherheitsrechtlichen Anforderungen – keine Anwendung finden.[48]

2. Beschränkter Anwendungsbereich des Unionsrechts

Hinsichtlich der Einwände gegen die **Erhebung sonstiger, nicht vorratsdatengespeicherter Verkehrsdaten** (§ 100g Abs. 1 StPO-E) sei angemerkt, dass diese nach Nichtigerklärung der Vorratsdatenspeicherungs-Richtlinie 2006/24/EG nicht dem Unionsrecht unterliegt. Vielmehr bestimmt Art. 1 Abs. 3 RL 2002/58/EG, dass diese, wie bereits ausgeführt, nicht gilt für „Tätigkeiten, die nicht in den Anwendungsbereich des Vertrags zur Gründung der Europäischen Gemeinschaft fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, und auf keinen Fall für Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Tätigkeit die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich.“ Eine vergleichbare Regelung enthält im Übrigen Art. 3 Abs. 2 1. SpS der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr:

---

[48] BVerfGE 118, 79 (95 ff.); E 122, 1 (21 f.); 130, 151 (177 f.); *F. Wollenschläger*, Verfassungsrechtliche Grundlagen des Öffentlichen Wirtschaftsrechts, in: R. Schmidt/F. Wollenschläger (Hrsg.), Kompendium Öffentliches Wirtschaftsrecht, 4. Aufl. 2015, § 2, Rn. 27.

Diese Richtlinie findet keine Anwendung auf die Verarbeitung personenbezogener Daten, die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, und auf keinen Fall auf Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich.

Mangels Durchführung von Unionsrecht besteht damit auch kein Anknüpfungspunkt für die Anwendbarkeit der Unionsgrundrechte (Art. 51 Abs. 1 S. 1 GRCh). Hiervon ist auch nach Auffassungen auszugehen, die die Speicherung – nicht aber die Erhebung – von Verkehrsdaten dem Anwendungsbereich des Unionsrechts unterstellen (siehe oben, III.1.).

So hält etwa das Gutachten des Juristischen Dienstes des Europäischen Parlaments zu Folgen des EuGH-Urteils vom 8.4.2014 diesen beschränkten Anwendungsbereich des Unionsrechts ausdrücklich fest:

That said, these conclusions do not necessarily apply to other national measures, going beyond "retention" of data initially collected by private service providers for business purposes, and concerning rather a subsequent processing of the retained data by public authorities on grounds of public interest, such as, for examples, the rules on the access and the use of such data by the law enforcement authorities of the Member States. If such national measures – adopted mostly in the area of criminal law or national security – fall outside the scope of the e-Privacy Directive (see Article 1(3)) and the scope of Directive 95/46 (see Article 3(2), 1st indent), and unless they fall within the scope of Union law on another ground, they will be considered as being outside of Union law and, as a consequence, the Charter will not be applicable to them.[49]

Dieser beschränkte Anwendungsbereich des Unionsrechts ist auch hinsichtlich der sonstigen Einwände gegen (die von der Speicherpflicht zu trennenden) strafprozessualen bzw. polizeilichen Eingriffsbefugnisse zu berücksichtigen.

München, den 17. September 2015

Gez. Prof. Dr. Ferdinand Wollenschläger

[49] Gutachten des Juristischen Dienstes des Europäischen Parlaments vom 22.12.2014, LIBE – Questions relating to the judgement of the Court of Justice of 8 April 2014 in Joined Cases C-293/12 and C-549/12, *Digital Rights Ireland* and *Seitlinger and others* – Directive 2006/24/EC on data retention – Consequences of the judgement, SJ-0890/14, Rn. 80, abrufbar unter: https://netzpolitik.org/wp-upload/2014-12-22_SJ-0890-14_Legal_opinion.pdf (16.9.2015).