19. Wahlperiode

Deutscher Bundestag
Ausschuss für Recht und Verbraucherschutz

Wortprotokoll
der 17. Sitzung

Ausschuss für Recht und Verbraucherschutz
Berlin, den 13. Juni 2018, 16:16 Uhr
Berlin, Paul-Löbe-Haus, Saal 2.600

Vorsitz: Stephan Brandner, MdB

Tagesordnung - Öffentliche Anhörung

Einziger Tagesordnungspunkt **Seite 13**

Öffentliche Anhörung zu den Artikeln 1, 2, 3 und 6 (Themenkomplex Vorratsdatenspeicherung)

des Gesetzentwurfs der Abgeordneten Christian Lindner, Stephan Thomae, Dr. Marco Buschmann, weiterer Abgeordneter und der Fraktion der FDP

Entwurf eines Gesetzes zur Stärkung der Bürgerrechte (Bürgerrechtestärkungs-Gesetz – BüStärG)

BT-Drucksache 19/204

Federführend:
Ausschuss für Recht und Verbraucherschutz

Mitberatend:
Innenausschuss
Ausschuss für Wirtschaft und Energie
Ausschuss für Menschenrechte und humanitäre Hilfe
Ausschuss für Kultur und Medien
Ausschuss Digitale Agenda

Berichterstatter/in:
Abg. Axel Müller [CDU/CSU]
Abg. Dr. Johannes Fechner [SPD]
Abg. Roman Johannes Reusch [AfD]
Abg. Dr. Jürgen Martens [FDP]
Abg. Niema Movassat [DIE LINKE.]
Abg. Tabea Rößner [BÜNDNIS 90/DIE GRÜNEN]

Sitzung des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss)

Mittwoch, 13. Juni 2018, 15:00 Uhr

Ordentliche Mitglieder des Ausschusses	Unterschrift	Stellvertretende Mitglieder des Ausschusses	Unterschrift
CDU/CSU		**CDU/CSU**	
Frieser, Michael		Amthor, Philipp	
Heil, Mechthild		Gutting, Olav	
Heveling, Ansgar		Harbarth Dr., Stephan	
Hirte Dr., Heribert		Hauer, Matthias	
Hoffmann, Alexander		Launert Dr., Silke	
Jung, Ingmar		Lindholz, Andrea	
Luczak Dr., Jan-Marco		Maag, Karin	
Monstadt, Dietrich		Middelberg Dr., Mathias	
Müller, Axel		Nicolaisen, Petra	
Müller (Braunschweig), Carsten		Noll, Michaela	
Sensburg Dr., Patrick		Schipanski, Tankred	
Steineke, Sebastian		Thies, Hans-Jürgen	
Ullrich Dr., Volker		Throm, Alexander	
Wellenreuther, Ingo		Vries, Kees de	
Winkelmeier-Becker, Elisabeth		Weisgerber Dr., Anja	

8. Juni 2018 — **Anwesenheitsliste** — Seite 1 von 3

Referat ZT 4 - Zentrale Assistenzdienste, Tagungsbüro
Luisenstr. 32-34, Telefon: +49 30 227-32251, Fax: +49 30 227-36339

19. Wahlperiode

Sitzung des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss)
Mittwoch, 13. Juni 2018, 15:00 Uhr

Ordentliche Mitglieder des Ausschusses	Unterschrift	Stellvertretende Mitglieder des Ausschusses	Unterschrift
SPD		**SPD**	
Brunner Dr., Karl-Heinz		Esken, Saskia	
Dilcher, Esther		Högl Dr., Eva	
Fechner Dr., Johannes		Lischka, Burkhard	
Groß, Michael		Miersch Dr., Matthias	
Heidenblut, Dirk		Müller, Bettina	
Ryglewski, Sarah		Nissen, Ulli	
Scheer Dr., Nina		Özdemir (Duisburg), Mahmut	
Schieder, Marianne		Rix, Sönke	
Steffen, Sonja Amalie		Vogt, Ute	
AfD		**AfD**	
Brandner, Stephan		Curio Dr., Gottfried	
Jacobi, Fabian		Hartwig Dr., Roland	
Maier, Jens		Haug, Jochen	
Maier Dr., Lothar		Seitz, Thomas	
Peterka, Tobias Matthias		Storch, Beatrix von	
Reusch, Roman Johannes		Wirth Dr., Christian	

8. Juni 2018

Anwesenheitsliste
Referat ZT 4 - Zentrale Assistenzdienste, Tagungsbüro
Luisenstr. 32-34, Telefon: +49 30 227-32251, Fax: +49 30 227-36339

Seite 2 von 3

61

19. Wahlperiode

Sitzung des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss)
Mittwoch, 13. Juni 2018, 15:00 Uhr

Ordentliche Mitglieder des Ausschusses	Unterschrift	Stellvertretende Mitglieder des Ausschusses	Unterschrift
FDP		**FDP**	
Buschmann Dr., Marco		Fricke, Otto	
Helling-Plahr, Katrin		Ihnen, Ulla	
Kloke, Katharina		Schinnenburg Dr., Wieland	
Martens Dr., Jürgen		Skudelny, Judith	
Müller-Böhm, Roman		Thomae, Stephan	
Höferlin, Manuel			
DIE LINKE.		**DIE LINKE.**	
Akbulut, Gökay		Jelpke, Ulla	
Mohamed Ali, Amira		Lay, Caren	
Movassat, Niema		Möhring, Cornelia	
Straetmanns, Friedrich		Renner, Martina	
BÜ90/GR		**BÜ90/GR**	
Bayram, Canan		Kühn (Tübingen), Christian	
Keul, Katja		Künast, Renate	
Rößner, Tabea		Mihalic, Irene	
Rottmann Dr., Manuela		Schauws, Ulle	

8. Juni 2018

Anwesenheitsliste
Referat ZT 4 - Zentrale Assistenzdienste, Tagungsbüro
Luisenstr. 32-34, Telefon: +49 30 227-32251, Fax: +49 30 227-36339

Seite 3 von 3

Sitzung des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss)

Mittwoch, 13. Juni 2018, 15:00 Uhr

	Fraktionsvorsitz	Vertreter
CDU/CSU		
SPD		
AFD		
FDP		
DIE LINKE.		
BÜNDNIS 90/DIE GRÜNEN		

Fraktionsmitarbeiter

Name (Bitte in Druckschrift)	Fraktion	Unterschrift
SINNOKROT, CARMEN	SPD	
ALBERS, KARSTEN	B'90/Grüne	
Dr. [illegible]	AfD	
Hage Kraft	B90/Grüne	
Krüger, Ilka	CDU/CSU	
Tanne	FDP	
Elif Eralp	LINKE	
Hannah Klein	Grüne	
Dr. Leonhardt	CDU/CSU	

Stand: 23. Februar 2015
Referat ZT 4 – Zentrale Assistenzdienste, Luisenstr. 32-34, Telefon: +49 30 227-32659, Fax: +49 30 227-36339

Tagungsbüro

Sitzung des Ausschusses für Recht und Verbraucherschutz
(6. Ausschuss)
Mittwoch, 13. Juni 2018, 15:00 Uhr

Fraktionsmitarbeiter

Name (bitte in Druckschrift)	**Fraktion**	Unterschrift
SCHAWTE	FDP	
Jörn Pohl	Grüne	

Stand: 23. Februar 2015
Referat ZT 4 – Zentrale Assistenzdienste, Luisenstr. 32-34, Telefon: +49 30 227-32659, Fax: +49 30 227-36339

Tagungsbüro

Sitzung des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss)
Mittwoch, 13. Juni 2018, 15:00 Uhr

Bundesrat

Land	**Name** (bitte in Druckschrift)	Unterschrift	**Amtsbezeichnung**
Baden-Württemberg	TRAA		Ri
Bayern	Bauer M		MR
Berlin			
Brandenburg			
Bremen			
Hamburg			
Hessen	Stuhlrath		RD
Mecklenburg-Vorpommern			
Niedersachsen			
Nordrhein-Westfalen	RIEM		RiLG
Rheinland-Pfalz			
Saarland			
Sachsen	SCHNEIDER		Ri
Sachsen-Anhalt			
Schleswig-Holstein			
Thüringen	Bieder		RiLG

Stand: 23. Februar 2015
Referat ZT 4 – Zentrale Assistenzdienste, Luisenstr. 32-34, Telefon: +49 30 227-32659, Fax: +49 30 227-36339

Tagungsbüro

Sitzung des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss)
Mittwoch, 13. Juni 2018, 15:00 Uhr

Ministerium bzw. Dienststelle (bitte in Druckschrift)	**Name** (bitte in Druckschrift)	**Unterschrift**	**Amtsbezeichnung**
BMJV	SPRENGER		RDn
BMI	Dr. FÜLLING		ORRn
BMI	Sperlich		RD

Stand: 23. Februar 2015
Referat ZT 4 – Zentrale Assistenzdienste, Luisenstr. 32-34, Telefon: +49 30 227-32659, Fax: +49 30 227-36339

Anwesenheitsliste der Sachverständigen

zur Anhörung des Ausschusses für Recht und Verbraucherschutz
am Mittwoch, 13. Juni 2018, 15.00 Uhr

Name	Unterschrift
Prof. Dr. Mark Cole Universität Luxemburg Professor für Medien- und Telekommunikationsrecht	
Jens Gnisa Vorsitzender des Deutschen Richterbund e. V. (DRB), Berlin	
Alfred Huber Generalstaatsanwaltschaft Nürnberg Leitender Oberstaatsanwalt als ständiger Vertreter des Generalstaatsanwalts	
Marcus Köhler Richter am Bundesgerichtshof, Leipzig 5. Strafsenat	
Dr. Constanze Kurz Sprecherin Chaos Computer Club e. V., Berlin Informatikerin/Autorin	
Petra Leister Staatsanwaltschaft Berlin Oberstaatsanwältin	
Dr. Heide Sandkuhl Deutscher Anwaltverein e. V., Berlin Fachanwältin für Strafrecht	
Marc Wenske Richter am Oberlandesgericht Hamburg	
Prof. Dr. Ferdinand Wollenschläger Universität Augsburg Juristische Fakultät Lehrstuhl für Öffentliches Recht, Europarecht und Öffentliches Wirtschaftsrecht	

Sprechregister Abgeordnete

Sprechregister Sachverständige

Der Vorsitzende **Stephan Brandner:** Meine Damen und Herren, wir beginnen mit der 17. Sitzung unseres Rechtsausschusses. Die 16. Sitzung war vor allem zum Ende hin recht turbulent. Ich begrüße die noch anwesenden Abgeordneten, ich begrüße die Zuschauer auf der Tribüne und nicht zuletzt begrüße ich natürlich die neun Sachverständigen sehr herzlich und bitte im Namen des Ausschusses – für den ich ja sprechen darf – um Verzeihung für die Verzögerung, wobei ich darauf hinweisen darf, dass das Verschulden der Opposition an dieser Verzögerung eher marginal ist. Meine Damen und Herren, wir führen heute eine öffentliche Anhörung zum Gesetzentwurf der FDP auf Drucksache 19/204 durch. Dort allerdings nur zu den Art. 1, 2, 3 und 6, also nur zu den Artikeln, die die Vorratsdatenspeicherung betreffen. Nicht Gegenstand dieser Anhörung ist das Netzwerkdurchsetzungsgesetz, mit dem wir uns möglicherweise später noch einmal im Rahmen einer weiteren Anhörung befassen werden. Zum Ablauf: Zunächst erhält jeder Sachverständige die Gelegenheit zu einer Eingangsstellungnahme, die nicht länger als vier Minuten dauern sollte. Wir beginnen dabei in alphabetischer Reihenfolge mit Herrn Cole auf der linken Seite und fahren fort bis zu Herrn Wollenschläger. Hieran schließt sich eine Fragerunde an, wobei die Beantwortung in der entgegengesetzten Reihenfolge erfolgt, beginnend bei Herrn Wollenschläger und endend bei Herrn Cole. Die Kolleginnen und Kollegen Abgeordneten wissen, dass in jeder Fragerunde maximal zwei Fragen von jedem gestellt werden dürfen, also jeweils eine Frage an zwei Sachverständige oder zwei Fragen an einen Sachverständigen. Die Uhr, die Sie dort sehen, läuft rückwärts. Nach drei Minuten und dreißig Sekunden ertönt ein Gong. Sie haben dann noch dreißig Sekunden Zeit für Ihre Eingangsstellungnahme. Wir haben trotz der fortgeschrittenen Zeit darauf verzichtet, die Uhr schneller laufen zu lassen. Ich bitte Sie, sich an die Zeit zu halten. Allerdings haben Sie einen kleinen Kredit bei uns, weil Sie lange warten mussten. Gegebenenfalls schließen sich weitere Fragerunden an – Das werden wir dann sehen. Es wird eine Tonaufzeichnung der Anhörung sowie ein Wortprotokoll geben. Bild- und Tonaufnahmen von der Tribüne sind nicht gestattet. Wir hatten vereinbart, dass die Anhörung von 15 Uhr bis etwa 17 Uhr andauern soll. Jetzt sind wir etwas in Verzug. Das hat keinen Einfluss auf Ihre Eingangsstellungnahmen, aber die Fragesteller sollten sich am Ende überlegen, ob wir noch eine zweite oder dritte Fragerunde durchführen und die zwei Stunden voll ausschöpfen wollen. Aber das sehen wir dann. Das war es von meiner Seite. Herr Cole, bitte schön.

SV **Prof. Dr. Mark Cole:** Sehr geehrter Herr Vorsitzender, sehr geehrte Parlamentarier und Parlamentarierinnen. Vielen Dank für die Möglichkeit, kurz Stellung zum Gesetzentwurf zu nehmen. Ich will mich auf einige wesentliche Kernthemen und Thesen beschränken und das Ganze unter einem europarechtlichen Blickwinkel betrachten, und zwar aus folgendem Grund:
Es gibt eine lange Diskussion um die Regelungen zur Vorratsdatenspeicherung in den Mitgliedstaaten. Wie Sie alle wissen, hat der Europäische Gerichtshof (EuGH) 2014 die damalige Richtlinie zur Vorratsdatenspeicherung gekippt. Das ist deshalb sehr wichtig in Erinnerung zu rufen, weil er dabei an der grundsätzlichen Möglichkeit, eine solche Vorratsdatenspeicherung vorzusehen, umfassend Kritik geübt hat. Jetzt ist das Urteil von 2014 nicht das letzte gewesen. Es ist eine ganze Reihe von Urteilen ergangen, insbesondere die Tele 2-Entscheidung vom Dezember 2016 hat das ursprüngliche Urteil noch einmal präzisiert.
Für die Frage der Beurteilung des deutschen Vorratsdatenspeicherungsrechts ist das deshalb relevant, weil das Europarecht in diesem Fall die nationale Entscheidung vorprägt. Warum? Es gibt eine Richtlinie über den Datenschutz in elektronischer Kommunikation, die in Art. 15 sagt, dass Mitgliedstaaten nur ausnahmsweise vom Grundsatz der Vertraulichkeit der Kommunikation abweichen dürfen, und sie für den Fall eines Abweichens die Vorgaben des Europarechts zu beachten haben, insbesondere eine Grundrechtsprüfung am Maßstab der EU-Grundrechtecharta durchführen müssen. Der EuGH hat damit in seinen Urteilen im Prinzip eine Modellprüfung vorgegeben, an der sich auch eine Prüfung des deutschen Rechts orientieren sollte. Zwar sind diese Urteile, jedes für sich genommen, auf einen bestimmten Sachverhalt und auf bestimmte Regelungen bezogen, beispielsweise auf die schwedischen oder die englischen Regelungen im Tele 2- bzw. Watson-Urteil. Aber die grundsätzliche Linie, die der EuGH entwickelt hat, hilft uns, auch andere – zum Beispiel

deutsche – Regelungen der Vorratsdatenspeicherung zu verstehen. Darin sagt der EuGH zusammengefasst Folgendes: Grundsätzlich steht die Idee einer anlasslosen, allgemeinen und umfassenden Speicherung von Kommunikationsdaten mit dem Grundrechtseingriff nicht in einem angemessenen Verhältnis, geht also zu weit. Wenn überhaupt eine solche Vorratsdatenspeicherung möglich ist, dann muss sie sehr viel gezielter sein, muss sie beschränkt sein. Beispielsweise gibt der EuGH Ideen vor, dass man die Vorratsdatenspeicherung territorial bzw. zeitlich begrenzen oder auf einen bestimmten Satz von Daten beschränken könnte. Die umfassende Speicherung von Kommunikationsdaten – zwar keine Inhaltsdaten, aber Verkehrsdaten und Standortdaten – ist schon vom Ansatz her im Blick auf die Grundrechte problematisch. Dann öffnet der EuGH einen Korridor, in dem er bestimmte Kriterien vorgibt, innerhalb dessen sich eine solche Lösung bewegen müsste und meine Einschätzung dieser Kriterien ist es, dass es kaum möglich ist, eine umfassende Vorratsdatenspeicherung auf dieser Basis zu entwickeln. Bislang hat noch keine der Lösungen eines Mitgliedstaates vor dem EuGH gehalten und meine Prognose ist, dass auch für die bestehenden Lösungen dasselbe Schicksal gelten würde.

Deshalb muss man sich fragen, ob nationale Regelungen weitergeführt werden sollen – die entweder schon nach dem Recht der alten Richtlinie zur Vorratsdatenspeicherung problematisch waren oder jedenfalls im Nachgang zu diesen beiden Urteilen weitergeführt werden sollen – oder ob es nicht sinnvoller wäre, einen Ansatz auf der europäischen Ebene zu verfolgen. Die Frage, warum das sinnvoll ist, können wir vielleicht später noch einmal vertiefen. Der Ansatz, eine nationale Regelung – wie hier mit dem Gesetzentwurf – zu hinterfragen, halte ich deshalb für sinnvoll, weil die Intensität eines solchen Eingriffs so erheblich ist, dass die Angemessenheit im Blick auf das zu erreichende Ziel bislang jedenfalls noch nicht belegt werden konnte. Danke schön.

Der **Vorsitzende:** Vielen Dank, Herr Cole. Sie haben aber eine Punktlandung hingelegt. Vielen Dank. Herr Gnisa, bitte.

SV **Jens Gnisa:** Sehr geehrter Herr Vorsitzender, meine sehr geehrten Damen und Herren Abgeordneten, meine Damen und Herren. Ich sehe mich eher als Vertreter der juristischen Praxis der Strafverfolgungsorgane, die hier auch in meinem Verband organisiert sind. Eine effektive Strafjustiz muss auf der Höhe der Zeit handeln können, wenn sie nicht zu einem Feigenblatt werden soll, und das muss auch in technischer Hinsicht gelten. Natürlich müssen unsere Strafverfolgungsorgane auch in technischer Hinsicht mithalten können, damit keine rechtsfreien Räume entstehen.
Mit Vorschriften, wie zum Beispiel dem § 99 Strafprozessordnung (StPO), in dem es heißt: „Zulässig ist die Beschlagnahme der an den Beschuldigten gerichteten Postsendungen und Telegramme […]“, kommen wir in einer digitalen Welt nicht mehr weiter. Straftäter nutzen moderne Telekommunikationsmethoden. Also müssen die Strafverfolgungsbehörden auch hier effektive Ermittlungsmethoden an die Hand bekommen und dazu zählt aus Sicht der Praxis auch die Vorratsdatenspeicherung. Warum ist das notwendig? Genannt seien folgende Fallbeispiele aus der Praxis: Kinderpornografie und Volksverhetzung im Internet – Die IP-Adresse ist regelmäßig der einzige Ermittlungsansatz. Enkeltrickbetrug – Hier ist es erforderlich, die Verbindungsdaten des eingehenden Anrufes zu ermitteln. Kapitaldelikte – Hier ist es bezogen auf den Tatzeitpunkt und auf den Tatort oft erforderlich, Verkehrsgeodaten zu ermitteln, die Rückschlüsse auf bestimmte Personen zulassen. Bandendelikte – Hier ist der Zugriff auf Funkzellendaten in der Vergangenheit sehr nützlich gewesen, weil dann eben Tatzusammenhänge aufgedeckt werden konnten. Richtig ist, dass nach wie vor unter bestimmten Voraussetzungen Abrechnungsdaten nach § 96 Telekommunikationsgesetz (TKG) gespeichert und auch abgerufen werden können. Allerdings ist hier aus der Praxis anzumerken, dass die Anbieter immer häufiger sich weigern, derartige Daten herauszugeben. Es müssen immer häufiger Durchsuchungs- und Beschlagnahmebeschlüsse ergehen, gegen die dann wieder Beschwerden eingelegt werden. Das heißt, es ist auch hier Sand im Getriebe. Darüber hinaus ist zu bedenken, dass der § 96 TKG nicht wesentlich weiterhilft, weil er eben nur sehr eingeschränkt Daten freigibt.
Ich nenne als Beispiel nur, dass Prepaid-Handys nicht gespeichert werden, weil letztendlich hier gar keine Kosten ausgelöst werden. Zu der

Entscheidung des EuGH kann man sicherlich eine Menge sagen. Ich denke, dass es aber meine Aufgabe sein sollte, hier noch einmal klar zu machen, dass nach der gerichtlichen und staatsanwaltschaftlichen Praxis unbedingt an der Vorratsdatenspeicherung festgehalten werden sollte. Wir sehen auch keine Alternativen.
Im Gegenteil sehen wir eigentlich sogar das Erfordernis, noch einmal Lücken zu schließen. Darauf haben wir früher schon einmal hingewiesen. Ich nenne noch einmal ganz kurz drei Punkte. Der Straftatenkatalog des § 100g StPO ist aus unserer Sicht so nicht schlüssig. Wir regen an, hier auf § 100a StPO zurückzugreifen. Die Art der zu erhebenden Daten ist unzureichend. Beispiel: Verkehrsdaten von E-Mails werden ebenso wenig erfasst, wie Daten über aufgerufene Internetseiten, und die Speicherfristen von zehn und vier Wochen sind für die gerichtliche Praxis auch sehr sportlich. Zusammengefasst möchte ich noch einmal sagen, dass die Strafverfolgungsbehörden dringend die Vorratsdatenspeicherung benötigen. Das ist die Rückmeldung der gesamten Praxis, die ich bekomme. Sie darf nicht fallen, vielmehr müssen umgekehrte Überlegungen angestrengt werden, wie das Urteil des EuGH umgesetzt werden kann, ohne unsere Regelungen einzuschränken. Mittelfristig müssen auch die von mir genannten Schwachstellen beseitigt werden. Herzlichen Dank.

Der **Vorsitzende:** Vielen Dank, Herr Gnisa. Der Nächste ist dann Herr Huber.

SV **Alfred Huber:** Sehr geehrter Herr Vorsitzender, sehr geehrte Damen und Herren Abgeordnete.
Ich kann mich zunächst meinem Vorredner anschließen, was die Bedeutung der Vorratsdatenspeicherung für die Strafverfolgung in der Praxis angeht. Die Frage ist hier: Ist der bislang bestehende § 100g Abs. 2 StPO verfassungswidrig oder europarechtswidrig? Da bin ich erst einmal ganz entspannt, weil ich sage, das ist nichts, was ein Sachverständiger entscheiden muss. Das ist aus meiner Sicht auch nichts, was der Deutsche Bundestag entscheiden muss. Da werden wir zu gegebener Zeit eine Entscheidung des Bundesverfassungsgerichts bekommen und daran werden wir uns selbstverständlich alle halten müssen. Sie können sich das mit der Bedeutung der Vorratsdatenspeicherung für die Praxis ein bisschen so vorstellen wie die Situation eines Handwerksmeisters, der seine Handwerker zur Arbeit schickt und ihnen Werkzeuge mitgibt. Wenn der Handwerker das passende Werkzeug nicht hat, kann er die Aufgabe – in unserem Fall ist die Aufgabe der Strafverfolgungsbehörden eben die Aufklärung von Straftaten – schlicht und einfach nicht erfüllen. Das ist die ganze Problematik. Ich denke, dass derjenige, der hier für die Abschaffung der Vorratsdatenspeicherung plädiert, auch ganz klar sagen muss, dass er die Verantwortung dafür trägt, dass Straftaten – und zwar schwere – nicht aufgeklärt werden können. Es geht ja hier in der Regel und im Kern um die sogenannten retrograden Standortdaten, das heißt, die Daten, die uns sagen, wo sich denn ein Tatverdächtiger in der Vergangenheit aufgehalten hat, also um das berühmte Bewegungsprofil. Ich möchte Ihnen zwei Fallgestaltungen schildern und ich verspreche, dass es bei der zweiten sogar eine Überraschung für den Einen oder den Anderen gibt. Die erste Fallgestaltung: Unser Opfer stirbt nach einem Gewaltverbrechen und die Leiche wird zwei Wochen nach der Tat im Wald aufgefunden. Der Tatverdacht richtet sich gegen eine bestimmte Person und wir haben eine – allerdings nicht eindeutige – Beweislage. Die retrograden Standortdaten – das Bewegungsprofil des Tatverdächtigen zur Tatzeit, war er am Tatort, hat er sich in Richtung dieses Ablageortes der Leiche bewegt? – sind ein ganz zentrales Beweismittel, das uns derzeit nicht zur Verfügung steht.

Man kann einen Fall trotzdem lösen, wenn wir eine Zeugenaussage bekommen oder etwas anderes, aber das ist eben nicht garantiert. Ein weiterer Fall, der aus meiner Sicht mindestens genauso dramatisch ist, ist der folgende, den wir derzeit ebenfalls nicht mit Hilfe der Daten lösen können. Nehmen Sie an, eine Joggerin joggt am Abend irgendwo im Wald im Wiesengrund, legt eine Strecke von fünf Kilometern zurück, denkt sich „Komisch, ich werde verfolgt!“, und es passiert natürlich das, was uns als Strafverfolgungsbehörden auf den Plan ruft. Sie wird nach fünf, nach sechs, nach zehn – völlig egal – Kilometern überfallen, vergewaltigt, ausgeraubt. Wir reden immer von schweren Straftaten. Es ist nicht gesagt, dass dieses Opfer am nächsten Tag zur Polizei geht und den Sachverhalt sofort anzeigt. Wir hätten die Möglichkeit, über diese Bewegungsdaten – weil sie sich in diesen fünf Kilometern in ganz vielen Funkzellen aufgehalten

hat – herauszubekommen, wer sich denn in denselben Funkzellen bewegt hat. Wir hätten einen ganz starken Ermittlungsansatz.
Nachdem die Vergewaltigung – und da sehe ich ein ganz großes Problem – derzeit im Katalog des § 100g Abs. 2 StPO nicht enthalten ist und über § 100g Abs. 1 StPO keine retrograden Standortdaten erhoben werden können, können wir in diesem Fall keinerlei Standortdaten erheben. Wir haben Beweismittel – wir reden jetzt nicht über Vorratsdatenspeicherung, wir reden über die Daten nach § 96 TKG – wir können aber nicht auf sie zugreifen. Aus dem Grund ist aus meiner Sicht dringend eine Änderung des § 100g Abs. 1 Satz 3 StPO erforderlich. Ich bitte um Nachsicht für das Überziehen.

Der **Vorsitzende:** Herr Köhler ist der Nächste.

SV **Marcus Köhler:** Herr Vorsitzender, meine sehr geehrten Damen und Herren Abgeordnete. Ich will mich ein bisschen auf den Sinn und Zweck des Gesetzentwurfs konzentrieren und der zielt ab auf Folgendes, ich zitiere: „Abschaffung der verfassungswidrigen und europarechtswidrigen Vorratsdatenspeicherung“. Dazu lässt sich aus meiner Sicht Folgendes sagen: Erstens – Mir scheint es nicht ausgeschlossen zu sein, dass der Entwurf einem Missverständnis hinsichtlich der Frage unterliegt, was das Konzept der Vorratsdatenspeicherung eigentlich ist, denn sie wird hier scheinbar verstanden als – ich zitiere erneut aus der Begründung – „staatliche Befugnis zu einer anlasslosen Verarbeitung der Daten der Bürgerinnen und Bürger“. Wenn das der Fall wäre, wäre das eine glatte Fehlvorstellung, die auch in der Öffentlichkeit weit verbreitet ist, denn tatsächlich trennt das geltende Konzept der Vorratsdatenspeicherung eindeutig und strikt zwischen der Speicherung einerseits und der Verwendung – die der Verarbeitung im Sinne des Gesetzentwurfs entspricht – andererseits. Die Speicherung findet nicht beim Staat statt. Sie findet bei den Telekommunikationsunternehmen statt. Die bloße Speicherung ist anlasslos. Die Verwendung der Daten ist von einem konkreten Anlass abhängig und zwar im Fall der Strafverfolgung von einem tatsachenbasierten Verdacht schwerer Straftaten, wie etwa Mord oder gemeinschaftlicher Vergewaltigung oder – auch das halte ich für eine schwere Straftat – Einbruchsdiebstahl in einer Privatwohnung. Die Verwendung steht zudem unter einem strikten Richtervorbehalt. Es gibt noch nicht einmal eine Eilkompetenz, in dem Fall für die Staatsanwaltschaft. Insofern bitte ich um Nachsicht, weil mir da in der schriftlichen Stellungnahme ein Fehler unterlaufen ist. Das heißt der Zugriff der Strafverfolgungsbehörden auf gespeicherte Daten unterliegt höheren Hürden als die Überwachung von Telefongesprächen.
Da kann man, glaube ich, nicht mehr davon sprechen, dass es sich um eine staatliche Befugnis für anlasslose Verarbeitung von Daten handelt.
Zweitens – Verkehrsdaten sind ohne Zweifel für eine effektive Aufklärung schwerer Straftaten unerlässlich. Ich will das nicht weiter ausführen. In der juristischen Fachwelt – was die Strafjustiz angeht – ist das im Grunde unumstritten. Herr Gnisa und Herr Huber haben etwas dazu gesagt. Ich kenne jedenfalls keine Stimme aus meiner Praxis, die das bestreiten würde. Wir hatten auch in der letzten Legislatur einen Sachverständigen, den Herrn Dr. Berger, der hatte eine Fallsammlung vorgelegt, die das eindeutig belegt. Ich habe sie deshalb meiner Stellungnahme noch einmal beigefügt. Jetzt muss man mal den Schluss ziehen: Die wirksame Aufklärung schwerer Straftaten ist wiederum etwas, was das Bundesverfassungsgericht als einen wesentlichen Auftrag des rechtstaatlichen Gemeinwesens sieht. Nehme ich das jetzt zusammen, komme ich aus meiner Sicht dazu, dass es ein Gebot des Rechtsstaates ist, es im rechtlich zulässigen Rahmen zu ermöglichen, Verkehrsdaten zu erheben. Eine aus meiner Sicht verfassungs- oder europarechtlich nicht gebotene Selbstbeschränkung des Gesetzgebers, nach meinem Verständnis durch den Entwurf intendiert, liefe diesem Gebot entgegen. Das möchte ich hier einmal in den Raum stellen. Das führt drittens zur Frage, wann ich das als Gesetzgeber aufheben müsste. Dann, wenn ich eine offensichtliche Verfassungswidrigkeit oder Europarechtswidrigkeit habe. Da schließe ich mich Herrn Huber an. Diese Frage kann im Grunde niemand seriös beantworten bzw. im Rechtsstaat beantworten solche Fragen die Verfassungsgerichte oder der EuGH. Was wir bisher haben, ist eine Entscheidung des Oberverwaltungsgerichts (OVG) Münster in einem einstweiligen Rechtsschutzverfahren. Die Ausgangsentscheidung des Verwaltungsgerichts (VG) Köln erging mit einer vertretbaren Begründung anders. Ob das jetzt der Maßstab ist,

zu handeln? Ich würde sagen, diese Frage soll bei den Verfassungsgerichten bleiben. Bleibt viertens die Frage: Gibt es Handlungsbedarf? Nach meiner Auffassung – was die Abschaffung der Vorratsdatenspeicherung und der entsprechenden Regelungen angeht – ein klares „Nein“, denn seit dem Beschluss des OVG Münster gibt es faktisch keine Speicherpflicht mehr. Die Vorratsdatenspeicherung existiert momentan nicht, insofern gibt es auch keinen Eingriff in Bürgerrechte durch diese Speicherung. Andererseits gibt es – und darauf will ich auch einmal hinweisen – aus meiner Sicht einen gesetzgeberischen Handlungsbedarf, der die retrograden Standortdaten betrifft. Es gilt nämlich Folgendes: Die Strafverfolgungsbehörden dürfen nicht zugreifen auf Standortdaten, die bei den Telekommunikationsunternehmen aus geschäftlichen Gründen gespeichert sind. Das ist die gesetzliche Lage. Das bedeutet, dass selbst der Generalbundesanwalt beim Verdacht von terroristischen Straftaten rückwirkend keine Standortdaten erheben darf. Ich meine, dass das eine gesetzliche Lücke ist – die sich aus dieser faktischen Abschaffung der Speicherfrist ergibt –, bei der der Gesetzgeber aus meiner Sicht – aus der Praxis der Strafjustiz – zum Handeln aufgefordert ist. Ich bedanke mich.

Der **Vorsitzende:** Ich mich auch, Herr Köhler. Die nächste ist Frau Kurz, bitte.

SVe **Dr. Constanze Kurz:** Vielen Dank. Sehr geehrter Herr Vorsitzender, sehr geehrte Damen und Herren. Ich möchte keine Argumente wiederholen, die bereits in der zehnjährigen Debatte über die Vorratsdatenspeicherung diskutiert worden sind. Ich verweise in technischen Fragen auf die Stellungnahme, die wir 2010 beim Bundesverfassungsgericht abgegeben haben. In technischer Hinsicht gilt sozusagen immer noch dieselbe Argumentation. Ich will darauf eingehen, was sich neben diesen beiden EuGH-Urteilen und dem Urteil aus Karlsruhe geändert hat. Generell nimmt das Volumen der Daten, die hier betroffen sind, stark zu. Das lässt sich messen und aus den jährlichen Berichten der Bundesnetzagentur auch sehr klar ablesen, was gleichzeitig bedeutet, dass diese Form des anlasslosen Festhaltens der Daten immer mehr Menschen, aber auch mehr Geräte betrifft. Denn die Zahl an GSM-Modulen in Geräten oder auch Fahrzeugen ist natürlich in den letzten zehn Jahren enorm gestiegen. Wir haben noch eine – aus meiner Sicht sehr wichtige – technische Änderung, die wir nicht mehr ignorieren können. Das wurde auch in anderen nationalen Regelungen schon besprochen. Wir haben eine fundamentale Änderung in Fragen der IT-Sicherheit. Auch hier im Bundestag ist uns sehr klar geworden, dass das anlasslose Festhalten von Daten ein Sicherheitsproblem darstellt. Aus meiner Sicht ist es eine Tatsache, dass die privaten Unternehmen, trotz des Umstandes, dass sie die schriftlich festgehaltenen Regeln der Bundesnetzagentur einzuhalten haben, mit dem Problem der Wirtschaftsspionage konfrontiert sind. Ich sehe es als problematisch an, dass man diese Daten aufhäuft, unabhängig davon, wer sie später verarbeitet. Ich würde dazu raten, das zu überdenken, denn ich glaube, in den letzten Jahren haben wir mit einer fast an Sicherheit grenzenden Wahrscheinlichkeit gelernt, dass diese Unternehmen – insbesondere auch Telekommunikationsunternehmen – in hohem Maße Ziel von Wirtschaftsspionage sind. Ich will darauf hinweisen, dass sich in technischer Hinsicht noch eine dritte Sache ändert, die mir sehr wichtig erscheint. Gerade jetzt startet die Deutsche Telekom AG eine neue Initiative, mit der die Funkzellen, in die sich unsere mobilen Telefone einbuchen, strukturell kleiner werden.

Das ist seit Jahren schon so, aber damit erhöht sich natürlich auch die Profilierung in dem Sinne, dass die Lokationsdaten, die dabei anfallen, sehr viel genauer werden. Das kann man auch sehr gut messen. Für die Zukunft kann man schon voraussagen, dass dies aufgrund der neuen Funkzellen, die heute verbaut werden, weiter zunehmen wird. Ich möchte noch einen anderen Aspekt ansprechen, der mir wichtig erscheint, der sich verändert hat gegenüber den Debatten, die wir seit zehn Jahren führen. Ich möchte auf die Gesamtüberwachungsrechnung, die wir aus Karlsruhe kennen, hinweisen. Wir haben in der Zeit, in der wir debattieren, ganz neue Möglichkeiten der technischen Überwachung hinzubekommen, namentlich die Funkzellenauswertung. Ich denke, dass die gesamte Überwachungsrechnung neu durchdacht werden sollte, wenn man über die Vorratsdatenspeicherung debattiert. Sie ist nicht unverzichtbar und nicht wegzudenken, denn sie ist ja derzeit überhaupt nicht vorhanden. Und ich

glaube auch, die seit zehn Jahren immer wieder zu hörenden Fallbeispiele und Einzelfälle überzeugen nicht angesichts der Tatsache, dass wir keinen evidenzbasierten Ansatz haben, der tatsächlich diese Unverzichtbarkeit zeigen würde. Insofern freut es mich sehr, dass mit diesem Bürgerrechtestärkungsgesetz die Trendwende – die wir in der Politik in Bezug auf anlasslose Speicherung dringend mal bräuchten – auch angegangen wird. Ich unterstütze daher diesen Gesetzentwurf.

Der **Vorsitzende:** Danke, Frau Kurz. Sie haben gemerkt, sobald der Chaos Computer Club e.V. spricht, funktioniert auch die Technik. Es kann kein Zufall sein. Frau Leister ist die Nächste, bitte.

SVe **Petra Leister:** Ich bin als Oberstaatsanwältin bei der Staatsanwaltschaft Berlin tätig, und zwar im Bereich der organisierten Kriminalität. Das ist wichtig, weil ich in dem Bereich natürlich sehr viel mit den Vorratsdaten und den retrograden Verkehrsdaten zu tun habe. Es wird Sie nicht wundern, wenn ich sage, dass ich mich gegen die Abschaffung der Vorratsdatenspeicherung und natürlich der daran anknüpfenden Zugriffsmöglichkeit der Strafverfolgungsbehörden auf retrograde Verkehrsdaten nach § 100g Abs. 2 StPO ausspreche, wie sie das Bürgerrechtestärkungsgesetz vorsieht. Ja, ich bin der Meinung, wir brauchen die Vorratsdatenspeicherung zur Bekämpfung schwerer Kriminalität, denn es gibt nun einmal spurenarme Taten, bei denen der Abgleich von Verkehrsdaten erforderlich ist, um zu verhindern, dass das Verfahren mangels ermittelten Täters gleich eingestellt wird. Um welche Fälle handelt es sich hierbei? Beispiel: Es werden zum Beispiel Funkzellendaten bei Serientaten abgeglichen, wenn wir uns im Bereich der KfZ-Verschiebung bewegen, also wenn Fahrzeuge desselben Typs in zeitlicher und örtlicher Nähe entwendet werden und wir von einer banden- und gewerbsmäßigen Verschiebung in das östliche Ausland ausgehen. Oder wenn von Gruppierungen nach demselben modus operandi hochkarätige Einbruchs-, aber auch Raubtaten, etwa bei Banken oder bei Juwelieren, begangen oder Geldautomaten gesprengt werden. Was wäre die Alternative in diesen Fällen? Ganz einfach: Eine sofortige Einstellung und überhaupt gar keine Maßnahme, keinerlei Ermittlung der Täter, die natürlich weiter ihr Unwesen treiben würden. Tut die Staatsanwaltschaft das leichtfertig? Nein, natürlich nicht. Es ist tatsächlich so, dass wir die Freiheitsrechte der Bürger ernst nehmen und von der Vorratsdatenspeicherung sind natürlich alle betroffen, auch wir selbst als Mitglieder der Strafverfolgungsbehörden. Wir begrüßen auch grundsätzlich die Kontrolle jeglicher repressiver Eingriffe in einem Rechtsstaat. Das ist erforderlich. Deswegen ist natürlich auch diese Runde heute hier erforderlich. Aber das in der Begründung des Gesetzentwurfs vorgetragene „Aus-der-Balance-Geraten“ von Freiheit und Sicherheit durch die Vorratsdatenspeicherung kann ich nicht erkennen. Staatsanwälte überlegen sehr genau, ob sie Beschlüsse beantragen und sehr zeitaufwendige Benachrichtigungspflichten nach Abschluss der Maßnahmen auf sich nehmen, anstatt den einfachen und durchaus bequemen Weg über eine sofortige Verfahrenseinstellung zu gehen. Natürlich fragt man sich, wie schwerwiegend eigentlich der Eingriff durch die Abfrage von bestimmten Vorratsdaten ist. Dazu muss man sich vor Augen führen, dass es sich nicht – das behauptet hier auch keiner – um Inhaltsdaten handelt, sondern im Wesentlichen um Daten darüber, welche Telefonnummern wann und wo miteinander in Verbindung standen. Erst im Falle von Überschneidungen findet ein Einzelabgleich statt, so wie Herr Köhler es auch erwähnt hat, erst dann, wenn schon ein Verdacht entstanden ist. Dann kommen wir im allerbesten Fall zu ein oder zwei übereinstimmenden Nummern, die wir weiter hinterfragen. Meist handelt es sich ohnehin um fiktive Personalien, auf die diese Nummern zugelassen sind. Wenn wir Glück haben, ist tatsächlich mal in einem Einzelfall eine Identifizierung möglich. Mehr erfahren wir dann auch nicht. Alles andere sind Sonderbände, die aus nichts als einzelnen Nummern bestehen, die für uns quasi anonym sind. Die Voraussetzungen sind meines Erachtens auch sehr eng gefasst. Es gibt eine Speicherfrist von nur zehn Wochen für Verkehrsdaten, vier Wochen für Standortdaten, keine Speicherung von Daten bevorrechtigter Personenkreise, Richtervorbehalt immer, keine Ausnahmen, einen sehr strengen Deliktskatalog, Benachrichtigungspflichten und Rechtsmittel. Weder das Bundesverfassungsgericht noch der EuGH haben die Vorratsdatenspeicherung per se für unzulässig erachtet. Deswegen meine Forderung: Wem die Voraussetzungen nicht

engmaschig genug sind, mag diese anpassen. Die vollständige Abschaffung der Vorratsdatenspeicherung aber beseitigt den einzigen Ermittlungsanhalt zur Verfolgung schwerer Straftaten – und deren Bekämpfung ist ebenso ein Bürgerrecht wie das Recht auf die informationelle Selbstbestimmung. Danke.

Der **Vorsitzende:** Vielen Dank. Die Nächste ist Frau Sandkuhl. Bitte.

SVe **Dr. Heide Sandkuhl:** Vielen Dank. Meine Damen und Herren, der Deutsche Anwaltverein e.V., für den ich hier heute sprechen darf, begrüßt die Abschaffung der Vorratsdatenspeicherung insbesondere aus drei Gründen. Erster Punkt: Unsere nationalen Regelungen verstoßen gegen Unionsrecht. Sie sind nach wie vor so ausgestaltet, dass auf einer ersten Stufe sämtliche Daten von 80 Millionen Bürgerinnen und Bürgern anlasslos, das heißt, ohne Verdacht einer konkreten Gefahr, ohne Verdacht einer schweren Straftat, gespeichert werden. Erst auf einer zweiten Stufe erfolgen Einschränkungen, unter denen die Daten abgerufen werden. Dies aber steht im diametralen Widerspruch zu der Rechtsprechung des EuGH, die Herr Professor Cole heute schon angesprochen hat. Der EuGH hat in seiner Entscheidung aus 2014 gesagt, dass die Speicherung – wohlgemerkt die Speicherung und nicht der Abruf – auf das absolut Notwendige zu beschränken sei. In seiner Entscheidung aus 2016 hat der EuGH das wiederholt und festgestellt, dass die anlasslose Speicherung, so wie sie in Deutschland geregelt ist, gegen Art. 7 und 8 EU-Grundrechtecharta verstößt. Das bedeutet, dass dieser Unionsrechtsverstoß meines Erachtens nicht mehr von der Hand gewiesen werden kann. Nur als Hinweis: Die Wissenschaftlichen Dienste des Deutschen Bundestages haben bereits genau die Punkte herausgearbeitet, die die nationalen Vorschriften nicht erfüllen. Zweiter Punkt: Die Untätigkeit des Gesetzgebers nach der EuGH-Entscheidung von 2016 führt in Deutschland zu einer Rechtsunsicherheit. Warum? Auf der einen Seite – Herr Köhler, Sie haben es schon angesprochen – haben Verwaltungsgerichte – und zwar das OVG Münster und dann im Nachgang das VG Köln – festgestellt, dass Telekommunikationsdiensteanbieter – in dem Fall war es, glaube ich, die SpaceNet AG – nicht verpflichtet seien, die hier in Rede stehenden Daten zu speichern. Und warum? Weil die entsprechenden Vorschriften des Telekommunikationsgesetzes gegen Unionsrecht verstoßen. Daraufhin hat die Bundesnetzagentur die Speicherpflicht erst einmal ausgesetzt. Die Literatur zog daraus den Schluss, dass wir erstmal keine Vorratsdatenspeicherung befürchten müssen, solange diese Speicherpflicht ausgesetzt ist, musste sich aber dann vom Landgericht Mannheim eines Besseren belehren lassen. Warum? Dieses Landgericht sah überhaupt kein Problem mit dem Unionsrecht. Blendete völlig aus, dass Daten anlasslos gespeichert werden und griff dann – weil die Speicherfrist ausgesetzt war und nach §§ 113a ff. TKG nichts gespeichert war – auf die Verkehrs-daten nach § 96 TKG zurück und erklärte eine analoge Anwendung dieser Vorschrift in Verbindung mit § 100g StPO für zulässig. Dritter Punkt: Unseres Erachtens sind die Legislativ-organe aufgerufen, den Rechten, die den EU-Bürgerinnen und Bürgern aus dem Unionsrecht erwachsen, auch zur Geltung zu verhelfen. Nimmt man den Grundsatz der Europafreundlichkeit ernst und will ihm auch rechtspolitisch Geltung verschaffen, dann ist es unseres Erachtens angezeigt, hier auch tätig zu werden. Tut man das nicht und nimmt Verstöße gegen das Unionsrecht hin, dann muss man sich nicht wundern, wenn andere EU-Mitgliedstaaten Forderungen, EU-Recht einzuhalten, unerfüllt lassen. Vielen Dank.

Der **Vorsitzende:** Frau Sandkuhl, vielen Dank. Der Nächste ist der Herr Wenske.

SV **Marc Wenske:** Sehr geehrte Damen und Herren Abgeordnete, sehr geehrte Kolleginnen und Kollegen. Ich danke Ihnen zunächst für die Einladung und die Möglichkeit, die Sicht eines weiteren Strafrechtspraktikers auf das in Rede stehende Ermittlungsinstrument heute in diesem hohen Hause zu Gehör bringen zu dürfen. Erlauben Sie mir zunächst, mit Ihnen in einen Verhandlungssaal des Landgerichts Hamburg zu blicken. Verhandelt wurde im Sommer 2013 ein besonders schwerer Raub, ein Indizienprozess. Die Staatsanwaltschaft hatte bereits neun Jahre Freiheitsstrafe beantragt. In seinem Plädoyer stellte der Verteidiger damals den Hilfsbeweisantrag für den Fall eines Schuldspruchs, noch eine bestimmte Funkzelle im Norden Schleswig-Holsteins auszulesen. Dies werde ergeben, dass

sich das Täterhandy, mit dem das Tatopfer in den Hinterhalt gelockt worden war, dort zu einem bestimmten Zeitpunkt aufgehalten habe. Dem Antrag kamen wir nach, denn es war klar, dass wenn die Behauptung zutrifft, der Angeklagte als Täter ausscheiden müsste. Die Funkzelle wurde nachträglich ausgelesen und es stellte sich heraus, dass das Handy tatsächlich dort eingeloggt war. Wir sprachen den Angeklagten frei. Als Richter bin ich dankbar dafür, dass ein sehr engagierter Verteidiger diesen Antrag gestellt und möglicherweise ein Fehlurteil zu einer langjährigen Freiheitsstrafe verhindert hat. Schon deshalb kann ich als Richter einen der Ausgangspunkte des Gesetzentwurfes, nämlich dass die Regelung über die kurzfristige Speicherung von Verkehrsdaten „verfassungspolitisch nicht klug“ sei, nicht zustimmen. Ist die Möglichkeit, für einen Angeklagten mit Hilfe seines elektronischen Fingerabdrucks auch entlastende Umstände zu Gehör zu bringen, nicht auch Ausdruck eines hohen Anspruchs des Rechtsstaates an den Schutz seiner Bürger? Kein leidenschaftlicher Vertreter des Rechtsstaats kann hierauf voreilig verzichten. Ich möchte Sie weiter einladen, in meine tägliche Arbeit als Ermittlungsrichter in Staatsschutzsachen beim Oberlandesgericht zu blicken. Liegen zureichende Verdachtsmomente für eine Mitgliedschaft etwa beim sogenannten Islamischen Staat nach der Einreise eines Beschuldigten in das Bundesgebiet vor, so gehört es zu dem Standardermittlungsprogramm, die Telekommunikationsverbindungsdaten des Beschuldigten, ich zitiere aus einem Beschluss, „zu potentiellen früheren Mitkämpfern, weiteren Mitgliedern oder Gesinnungsgenossen abzuklären“, um auf diese Weise weitere Erkenntnisse über die frühere oder gar noch fortbestehende Betätigung für die Terrororganisation aufzuklären. Auf andere Art und Weise wäre das nicht möglich. Könnte der Rechtsstaat aber bei absehbar ausbleibenden Ermittlungserfolgen wegen nicht vorhandener Daten noch auf dasselbe Vertrauen seiner Bürger hoffen oder würde nicht vielmehr auf lange Sicht das berechtigte und wichtige Anliegen des Datenschutzes desavouiert? Hiermit korrespondiert eine Stellungnahme des Präsidenten des Bundeskriminalamtes aus der vergangenen Woche. Danach seien im Jahr 2017 bei 8.400 Hinweisen auf Kinderpornographie die Ermittlungen eingestellt worden, weil retrograde Abfragen von IP-Adressen derzeit mangels der Erfüllung gesetzlicher Speicherpflichten durch die Internetdienstleister nicht möglich seien. Die vom Gesetzentwurf angesprochenen verfassungs- und europarechtlichen Fragen sind derzeit nicht eindeutig zu beantworten, sondern bedürfen besonders sorgsamer Prüfung. Die mit Augenmaß ausgestaltete und die widerstreitende Interessen, aus meiner Sicht, ausgleichende geltende Rechtslage berücksichtigt bereits die bisherigen verfassungsgerichtlichen Vorgaben. Sie bleibt in ihrer Eingriffstiefe überdies hinter den durch den EuGH überprüften Regelungen aus Schweden und Großbritannien zurück, sodass ein Schluss auf eine Unionsrechtswidrigkeit nicht zwingend ist. Und in nunmehr absehbarer Zeit wird das Bundesverfassungsgericht über die bei ihm anhängigen Verfassungsbeschwerdeverfahren entscheiden. Sollten wider Erwarten durchgreifende Bedenken aufgezeigt werden, kann der Gesetzgeber darauf konkret und zügig reagieren. Eine Bewertung des Gesetzentwurfs kann schließlich nicht ohne Auseinandersetzung mit den drei noch immer verbreiteten Missverständnissen erfolgen, so auch Herr Köhler soeben. Verkehrsdaten sind sensibel, aber nicht ebenso sensibel wie der Inhalt der Kommunikation. Sie lassen keine Inhalte erkennen, sondern nur, wer, wann, wie lange, von wo, mit wem auf welche Weise kommuniziert hat. Der Staat erhebt keine Informationen. Die Speicherung erfolgt bei den privaten Anbietern unter strengen Sicherheitsvorgaben. Der staatliche Abruf steht unter dem Vorbehalt eines unabhängigen Richters. Dieser muss von den Ermittlungsbehörden voll informiert und überzeugt werden. Erst dann, beschränkt auf die konkret zu benennenden Daten, gibt es eine staatliche Erhebungsbefugnis. Lassen Sie mich schließen: Der Entscheidung des Bundesverfassungsgerichts durch einen vollständigen Verzicht auf das Ermittlungsinstrument, aber auch das Mittel der Gefahrenabwehr, vorzugreifen, wäre nicht nur übereilt, sondern trüge der erheblichen Bedeutung der Speicherpflicht als Mittel moderner Kriminaltechnik für eine effektive Strafverfolgung, vergleichbar mit den Errungenschaften der Daktyloskopie, nicht angemessen Rechnung. Danke schön.

Der **Vorsitzende:** Danke, Herr Wenske. Die Eingangsrunde beendet Herr Wollenschläger.

SV **Prof. Dr. Ferdinand Wollenschläger:** Vielen Dank Herr Vorsitzender, meine sehr geehrten Damen und Herren Abgeordnete. In meiner Stellungnahme möchte ich mich auf die verfassungs- und europarechtliche Dimension konzentrieren. Zunächst kurz zum Gesetzentwurf: Der Gesetzentwurf fordert die vollständige Aufhebung der deutschen Regelung zur Vorratsdatenspeicherung. Hierzu lässt sich relativ kurz sagen – und insoweit auch in Übereinstimmung mit der Rechtsprechung, sowohl der des Bundesverfassungsgerichts, als auch der des EuGH –, dass eine vollständige Aufhebung keinesfalls geboten sein kann. Unabhängig davon stellt sich natürlich angesichts der restriktiven Rechtsprechung des EuGH, die heute schon angeklungen ist, die Frage, ob die im deutschen Telekommunikationsgesetz vorgesehene allgemeine Vorratsdatenspeicherung von Daten noch aufrechterhalten werden kann, oder ob nicht vielmehr nur eine Speicherung von Daten solcher Personenkreise zulässig ist, die in einem zumindest mittelbaren, etwa geografischen, Bezug zu Gefahren, respektive Straftaten, stehen. Meines Erachtens besteht keine solche Pflicht des deutschen Gesetzgebers und ich möchte das im Folgenden anhand eines differenzierten Blicks auf die einschlägige Rechtsprechung begründen. Erstens: Richtig ist, dass der EuGH in den schon erwähnten beiden Urteilen aus den Jahren 2014 und 2016 Regelungen der Vorratsdatenspeicherung für unverhältnismäßig erklärt hat. Hierbei ist allerdings zu berücksichtigen, dass die deutsche Regelung, über die wir reden, deutlich grundrechtsschonender als die beanstandeten Regelungen ausgestaltet ist. Das hat bei einer Gesamtabwägung, die natürlich für jede einzelne konkrete Regelung anzustellen ist, einzufließen, sodass man insoweit aus den beiden EuGH-Urteilen nicht auf die Europarechtswidrigkeit der deutschen Regelung schließen kann. Ich weise nur ganz kurz darauf hin: Das Telekommunikationsgesetz mit seinem Konzept der restriktiven allgemeinen Verkehrsdatenspeicherung differenziert nach Datenart, sieht eine differenzierte Speicherdauer vor, speichert keine Daten von Diensten der elektronischen Post, speichert keine Daten von besonderer Vertraulichkeit unterliegenden Verbindungen und sieht auch nur eine kurze Speicherungsfrist von vier bzw. zehn Wochen vor und nicht von sechs Monaten, wie die beanstandeten Regelungen. Zweiter ganz wichtiger Punkt: Das Tele2-Urteil, also das Urteil aus dem Jahr 2016, erschöpft sich nicht darin, eine konkrete nationale Regelung zu beanstanden, sondern enthält weitere Ausführungen, aus denen sich in der Tat die Europarechtswidrigkeit einer allgemeinen Verbindungsdatenspeicherung schließen lässt. Diese Urteilspassage darf man aus drei Gründen jetzt allerdings nicht missverstehen. Erstens handelt es sich hierbei lediglich um ein den deutschen Gesetzgeber nicht unmittelbar bindendes obiter dictum. Zweitens, verbleibt auch eine Rechtsunsicherheit, ob diese Passage abschließend gemeint ist. Drittens: In seinem Urteil zur Fluggastdatenverarbeitung – das heute noch nicht zur Sprache gekommen ist und nach dem Tele2-Urteil ergangen ist – hat der EuGH jedenfalls einem unbedingten unionsrechtlichen Verbot einer anlasslosen Vorratsdatenspeicherung der Fluggastdaten eine Absage erteilt, was natürlich eine deutliche Lockerung gegenüber dem Tele2-Urteil darstellt. Fazit: Natürlich muss sich der deutsche Gesetzgeber europarechtsfreundlich, wie das angeklungen ist, verhalten. Es ist auch gut, dass jetzt im Rahmen der Anhörung dieses Gesetzentwurfs die Regelung erneut reflektiert wird. Aus den von mir genannten Gründen ist es aber nach wie vor so, dass es unionsgrundrechtlich vertretbar ist, am aktuellen Telekommunikationsgesetz mit seinem Konzept einer restriktiven allgemeinen Verkehrsdatenspeicherung festzuhalten und eine weitere Entscheidung des EuGH abzuwarten. Vielen Dank.

Der **Vorsitzende:** Perfekt, Herr Wollenschläger. Vielen Dank Ihnen allen für die Eingangsrunde. Ich habe jetzt zwei Wortmeldungen notiert: Zum einen von Herrn Martens und zum anderen von Frau Winkelmeier-Becker. Herr Martens, bitte.

Abg. **Dr. Jürgen Martens** (FDP): Vielen Dank, Herr Vorsitzender. Zunächst darf ich mich für die den Gesetzentwurf vorlegende FDP-Fraktion im Bundestag recht herzlich bedanken, dass Sie sich die Zeit genommen haben – vor allem auch die Wartezeit durchgehalten haben –, um hier als Sachverständige zur Verfügung zu stehen. Vielen Dank auch für Ihre Ausführungen. Ich entnehme jetzt den Ausführungen, dass es auf der einen Seite den Wunsch der Praxis – der Strafverfolger – gibt, dieses Instrument einer Vorratsdaten-

speicherung vorzuhalten, auf der anderen Seite hingegen Bedenken sowohl verfassungsrechtlicher wie auch europarechtlicher Art bestehen. Herr Professor Wollenschläger hat zum Schluss noch einmal ausgeführt, der EuGH habe festgestellt, dass nach der EU-Grundrechtecharta erhebliche Bedenken hinsichtlich einer anlasslosen, generellen Datenspeicherung bestünden, wobei wohl weniger die Dauer der Speicherung, sondern vielmehr der Eingriff als Solches im Fokus gestanden habe. Dazu meine Frage an Herrn Professor Cole und vielleicht auch an Frau Dr. Sandkuhl: Gehe ich recht in der Annahme, dass es nach der Rechtsprechung des EuGH gar nicht auf die Dauer der Datenspeicherung ankommt, sondern alleine auf den Umstand der Anlasslosigkeit der Erhebung? Einen anderen Punkt betrifft die Frage, wie man denn jetzt weiter vorgehen soll. Frau Leister, Sie haben gesagt, dass Sie gern die Daten aus der Vorratsdaten-speicherung nutzen würden. Sie haben Beispiele genannt, bei denen Sie am Schluss selbst sagen, dass nur ein oder zwei erfolgversprechende Treffer bleiben. Da stellt sich die Frage der Verhältnismäßigkeit bei der Speicherung von Millionen oder Milliarden Daten, wenn am Ende dann nur zwei Treffer herauskommen. In Berlin ging es meiner Kenntnis nach um Delikte, wie zum Beispiel das Anzünden von Autos. Da sind aus Funkzellenabfragen zwei Millionen Daten erhoben worden. Auch hier stellt sich die Frage der Verhältnismäßigkeit. Die Bundesnetzagentur schreibt – unter Bezugnahme auf das Urteil des OVG Münster –, dass die Telekommunikations-diensteanbieter bis zum Ausgang des Hauptsacheverfahrens nicht verpflichtet seien, die TKG-Daten nach § 113b Abs. 3 TKG zu speichern. Das ist die faktische Aussetzung der Vorratsdaten-speicherung. Trotzdem, so jedenfalls Presse-berichte, möchte die Staatsanwaltschaft Detmold Ermittlungen gegen Telekommunikationsanbieter prüfen, weil diese ihre Speicherpflicht nicht erfüllten und die Daten nun nicht für Ermittlungs-zwecke zur Verfügung stünden. Jetzt folgt die Frage an Frau Leister: Was gilt denn nun nach Ihrer Ansicht? Die Aussage der Bundesnetz-agentur bezüglich der Aussetzung oder machen sich die Unternehmen, die keine Daten speichern, jetzt strafbar?

Der **Vorsitzende:** Ihre Fragen sind mir jetzt nicht ganz klar. Wir haben drei Fragen notiert, an Herrn Cole, Frau Leister und Frau Sandkuhl. An wen wollten Sie die Fragen jetzt eigentlich stellen?

Abg. **Dr. Jürgen Martens** (FDP): Die erste Frage ging an Herrn Professor Cole und Frau Dr. Sandkuhl und die zweite Frage richtete sich nur an Frau Leister.

Der **Vorsitzende:** Also stellen Sie insgesamt drei Fragen?

Abg. **Dr. Jürgen Martens** (FDP): Ich habe die erste Frage an zwei Sachverständige und die zweite Frage an eine Sachverständige gerichtet.

Der **Vorsitzende:** Wir hatten uns aber darauf verständigt, eine Frage an zwei Sachverständige oder zwei Fragen an einen Sachverständigen zu richten – alternativ, nicht kumulativ. Aber wir belassen es hier dabei und halten uns in Zukunft an diese Vereinbarung. Die Nächste ist Frau Winkelmeier-Becker und danach hat Herr Fechner das Wort.

Abg. **Elisabeth Winkelmeier-Becker** (CDU/CSU): Ich hätte auch ein paar mehr Fragen, so ist es jetzt nicht. Ich möchte zunächst eine Frage an Herrn Gnisa und an Herrn Huber richten und möchte das auch mit einem Dank an die gesamte Riege der Sachverständigen verbinden. Sie beide haben – wie auch andere Kollegen – sehr anschaulich geschildert, welche Verbrechen hier im Raum stehen, die verhindert bzw. aufgeklärt werden sollen, beispielsweise Kinderpornografie oder schwere Kapitalverbrechen. Es steht ja immer zweierlei zur Abwägung. Und wir wissen hier sehr konkret, was wir alles nicht verhindern bzw. aufklären können, obwohl der Staat – aus meiner Sicht jedenfalls – die Pflicht dazu hätte, denn wer soll sonst die Bürger in diesen Fällen schützen? Ich würde Sie aber bitten, auch noch einmal den Blick auf die Gefahr des Missbrauchs, die hier immer im Raum steht, zu werfen und zu erklären, was denn der „worst case“ für einen unbescholtenen Bürger ist, von dem Daten erhoben wurden, weil er telefoniert hat. Was kann denn diesem passieren, wenn er in die Fänge der „bösen“ Strafermittlungsbehörden gerät? Was kann da über ihn herausgefunden werden? Was ist der belastende Faktor für den Bürger? Es geht also darum, was auf der anderen Seite in der Waag-schale liegt. Muss man sich beobachtet fühlen oder sind nicht die Vorkehrungen, die im

Verfahren dann vorgesehen sind, so hoch, dass man hier vor einem Missbrauch doch recht sicher ist? Oder im Nachhinein erklärt bekommen würde, warum man betroffen war? Auch im Blick auf das von Frau Dr. Kurz angesprochene Gefahrenpotential hinsichtlich der Spionage. Sind die Daten, um die es hier geht, für irgendeinen Spion, etwa einen Wirtschaftsspion, interessant? Gibt es irgendjemanden, der ein Interesse daran hätte, zu erfahren, wer wann mit dem Pizzaservice telefoniert hat? Wenn Sie das noch einmal darlegen könnten, wäre ich Ihnen sehr dankbar.

Der **Vorsitzende:** Danke, Frau Winkelmeier-Becker. Danach Herr Fechner und dann Frau Rößner.

Abg. **Dr. Johannes Fechner** (SPD): Ich hätte zwei Fragen an Herrn Wenske. Von Herrn Münch war ja vor kurzem in ziemlich dramatischen Ausführungen zu lesen, welche Defizite er aufgrund des Umstandes sieht, dass dieses Instrument der Vorratsdatenspeicherung nicht zur Verfügung steht. Teilen Sie diese Einschätzung auch in dieser Dramatik? Das wäre meine erste Frage. Und daran anschließend: Soll man als Gesetzgeber nun handeln, wie es die FDP hier vorschlägt, oder erst einmal in Ruhe die Verfassungsgerichtsentscheidung abwarten?

Der **Vorsitzende:** Danke schön. Frau Rößner und dann Herr Movassat.

Abg. **Tabea Rößner** (BÜNDNIS 90/DIE GRÜNEN): Von meiner Seite ganz herzlichen Dank für die Ausführungen. Ich habe zwei Fragen an Frau Dr. Kurz. Hier wurde eben schon von verschiedener Seite die Bedeutung des Instruments im Hinblick auf sexuelle Gewalt, Missbrauch und Kinderpornografie angesprochen. Wir kennen ja diese Diskussion schon seit über zehn Jahren, in der es immer heißt, dass die Vorratsdatenspeicherung das einzige Mittel ist, um diese Straftaten richtig zu verfolgen – verhindern wird man sie nicht können. Dabei haben wir doch eigentlich eine sehr hohe Aufklärungsquote. Soweit ich weiß, ist die gegenüber der Vergangenheit auch gestiegen. Ist denn jetzt die Vorratsdatenspeicherung Ihrer Ansicht nach insoweit der einzige Ansatz? Die zweite Frage betrifft alle Berufsgeheimnisträger. Gibt es denn eigentlich eine technische Lösung für die geforderte Nichterfassung von Berufsgeheimnisträgern? Und falls nicht, was taugen die diskutierten Ausweichlösungen, die seitens der Befürworter und Sicherheitsbehörden immer wieder angeboten werden?

Der **Vorsitzende:** Danke, Frau Rößner. Bitte, Herr Movassat.

Abg. **Niema Movassat** (DIE LINKE.): Ich hätte zwei Fragen an Frau Dr. Sandkuhl. Zum einen würde mich interessieren, ob nach der derzeitigen Studienlage nachgewiesen ist, dass ohne die Vorratsdatenspeicherung Ermittlungserfolge bei der Strafverfolgung ausgeblieben sind? Das ist ja ein ganz häufig genanntes Argument. Mich würde interessieren, wie sich aus Ihrer Sicht insoweit die Studienlage darstellt. Zweitens würde mich das gesamte Thema der Berufsgeheimnisträger interessieren. Es werden auch die Daten von Ärzten, Anwälten, Seelsorgern, Abgeordneten usw. erhoben. Bei Journalisten besteht zusätzlich die besondere Problematik des Quellenschutzes, weil man so herausfinden kann, welcher Journalist mit welchem Informanten zu welcher Zeit gesprochen hat. Das kann tatsächlich gravierende Folgen für die Arbeitsweise von Journalisten haben. Wie sehen Sie die derzeitige Rechtslage nach der Rechtsprechung des EuGH, insbesondere zum zwingenden Schutz von Berufsgeheimnisträgern? Danke schön.

Der **Vorsitzende:** Vielen Dank, die erste Fragerunde ist damit aus meiner Sicht abgeschlossen. Wir haben keine weiteren Fragesteller. Dann kommen wir zu den Antworten und beginnen auf der rechten Seite im Alphabet rückwärts. Herr Wollenschläger ist diesmal hinsichtlich der Fragen leider leer ausgegangen. Deshalb beginnt Herr Wenske mit zwei Fragen von Herrn Fechner.

SV **Marc Wenske:** Vielen Dank. Ich versuche, die Frage, ob ich mich der Einschätzung des Präsidenten des Bundeskriminalamts, Herrn Münch, bezüglich der Kinderpornographie anschließen kann, kurz zu beantworten. Ich kann mich dem anschließen. Kinderpornographie ist das eine, damit habe ich am Oberlandesgericht nur im Revisionsrecht ab und zu zu tun. Mich treiben eher die Gewalttaten und – eben als Ermittlungsrichter – die Staatsschutzdelikte um, bei denen ich einen ähnlichen Ausfall an Erkenntnismitteln besorge und deswegen befürchten muss, dass, wenn der Staat an diesen Stellen seine – für die Wahrnehmung in der

Öffentlichkeit und bei den Bürgern entscheidende – Handlungsfähigkeit einbüßt, er – bzw. die Funktionstüchtigkeit der Strafrechtspflege – möglicherweise an Vertrauen verliert. Und deswegen – jetzt komme ich zum zweiten Punkt – bin ich natürlich nicht dafür, dieses bedeutsame Instrument sofort abzuschaffen. Dafür wäre ich nur bei einer evidenten Verfassungswidrigkeit oder Unionsrechtswidrigkeit. Die kann ich nicht sehen. Als Richter würde ich deswegen die Regeln weiterhin anwenden und nicht wie das OVG Münster wegen der Europarechtswidrigkeit stoppen. Deswegen plädiere ich dafür, mit Augenmaß – entsprechend der Abfassung der jetzigen Regelungen, die auch mit Augenmaß abgefasst sind – abzuwarten und zu schauen, ob und wie das Bundesverfassungsgericht entscheidet. Es wird sicher in absehbarer Zeit entscheiden, denn auf der Homepage des Bundesverfassungsgerichts steht das Verfahren schon im Jahresplan für dieses Jahr, um abgearbeitet zu werden. Und dann mit Augenmaß zu reagieren. Eine komplette Nichtigerklärung durch das Bundesverfassungsgericht steht meines Erachtens auch nicht zu besorgen, sondern eher – wenn überhaupt – eine punktuelle Nachsteuerung, weil die deutsche Regelung eben nicht umfassend erfolgt, sondern differenziert und – es wurde schon gesagt, durch die Kolleginnen und Kollegen – E-Mail-Verkehr außen vor lässt. Deswegen ist sie auch nicht vergleichbar mit den schwedischen Regelungen – das sei auch noch erwähnt –, die zulassen, dass die Ermittlungsbehörden unmittelbar selbst die Daten abgreifen. Wir haben mit dem Zwei-Türen-Modell eine formale Sicherung. Erst wird gespeichert und dann durch den Ermittlungsrichter der rechtmäßige Abruf gewährleistet. Diese ausdifferenzierte Regelung lässt mich weiter dafür plädieren, abzuwarten und mit Augenmaß punktuell nachzusteuern, wenn es erforderlich sein sollte. Danke.

Der **Vorsitzende:** Danke, Herr Wenske.
Frau Sandkuhl mit insgesamt drei Fragen, das heißt mit zwei Fragen von Herrn Movassat und einer der vielen von Herrn Martens.

SVe **Dr. Heide Sandkuhl:** Die ersten Fragen gingen ja ein bisschen ineinander über, insofern passt es jetzt ganz gut. Herr Wenske, Sie werden sich nicht wundern, dass ich Ihnen jetzt widersprechen werde. Denn nach wie vor ist – und das muss man einfach auch hier bei der Beantwortung der ersten Frage festhalten – die deutsche Rechtslage so ausgestaltet, dass die Daten von 80 Millionen Bürgerinnen und Bürgern ohne Anlass gespeichert werden, das heißt, ohne einen Verdachtsgrad. Der EuGH sagt dazu – wenn ich mal zitieren darf – in der Entscheidung aus 2016: „Zudem kann zwar die Wirksamkeit der Bekämpfung schwerer Kriminalität, insbesondere der organisierten Kriminalität und des Terrorismus, in hohem Maß von der Nutzung moderner Ermittlungstechniken abhängen. Eine solche dem Gemeinwohl dienende Zielsetzung kann jedoch, so grundlegend sie auch sein mag, für sich genommen die Erforderlichkeit einer nationalen Regelung, die die allgemeine und unterschiedslose Vorratsdatenspeicherung sämtlicher Verkehrs- und Standortdaten vorsieht, für die Kriminalitätsbekämpfung nicht rechtfertigen.“ Die Wissenschaftlichen Dienste – und jetzt komme ich, Herr Movassat, zu Ihrer Frage gleich im Anschluss – haben dieses Urteil des EuGH von 2016 bereits analysiert und – wie ich finde – völlig zu Recht, die Defizite, unter denen die nationalen Regelungen leiden, zusammengefasst – oder anders gesagt: die Vorgaben zusammengefasst, die die nationalen Regelungen mit Blick auf die Rechtsprechung des EuGH aus dem Jahr 2016 nicht erfüllen. Nämlich, dass bereits die Speicherung von Vorratsdaten nur bei Vorliegen des Verdachts einer schweren Straftat zulässig ist, oder auch nur Vorratsdaten solcher Personen gespeichert werden, die Anlass zur Strafverfolgung geben. Und das von Ihnen angesprochene Berufsgeheimnis – was diese Frage angeht – wie folgt zutreffend zusammengefasst: Die Vorratsdaten solcher Personen dürfen nicht gespeichert werden, deren davon betroffene Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen. Das haben wir gerade. Das ist eindeutig. Dann noch zu Ihrer zweite Frage: Herr Huber ist ja so weit gegangen und hat gesagt, wer sich gegen die Abschaffung der Vorratsdatenspeicherung ausspricht, müsse die Verantwortung dafür übernehmen, dass bestimmte Straftaten nicht verfolgt werden können. Wer die Vorratsdatenspeicherung will, muss umgekehrt die Verantwortung dafür übernehmen, dass Daten von 80 Millionen Bürgerinnen und Bürger gespeichert werden, ohne dass diese auch nur irgendeinen

Anlass dafür gegeben haben. Jetzt wird oft mit Fallgestaltungen aus der Praxis argumentiert. Aber nach wie vor bleibt doch festzuhalten, dass wir gesicherte Rechtstatsachen, die eine Erforderlichkeit einer Vorratsdatenspeicherung belegen, doch überhaupt nicht haben. Ich glaube, Frau Dr. Kurz kann da noch viel mehr zu sagen als ich. Es wird uns mit Fällen begegnet, aber der Deutsche Anwaltverein e.V. hat schon in der Stellungnahme von 2015 auf die Studie des Max-Planck-Instituts hingewiesen. Und das Ergebnis ist immer wieder, dass wir keine empirisch gesicherten Erkenntnisse haben. Die Frage, ob es mildere Mittel gibt, das Ziel zu erreichen, kann doch nicht einfach mit drei Fällen beantwortet werden, in denen es jetzt ganz wichtig ist. Und deswegen dürfen wir diese Maßnahme nicht einfach so ergreifen und – ohne dass es empirisch unterlegt ist – sagen, dass wir das jetzt brauchen. Das steht ja in keinem Verhältnis zu der Eingriffsintensität. Danke.

Der **Vorsitzende:** Danke, Frau Sandkuhl. Dann sind wir bei der Frau Leister angelangt, die eine Frage von Herrn Martens gestellt bekommen hat.

SVe **Petra Leister:** Im Prinzip habe ich zwei Fragen erhalten. Die erste Frage betraf ja die Frage, ob überhaupt eine Verhältnismäßigkeit gegeben ist, wenn nur ein Treffer bei den Vorratsdaten vorliegt, beispielsweise bei den Funkzellen. Das erschließt sich mir nicht wirklich, denn auch wenn ich 100 Treffer hätte, hätte ich im Grunde Treffer. Wenn ich tatsächlich nur einen bis fünf Täter suche, wird es mir nichts nützen, wenn ich 400 verschiedene Nummern angezeigt bekomme. Die Verhältnismäßigkeit ergibt sich ja daraus, dass ich tatsächlich irgendwas Werthaltiges angezeigt bekomme und natürlich der Abgleich solange erfolgt, bis ich zum Ergebnis gelange, dass diese Nummer tatsächlich aussagekräftig ist. Sie wird natürlich desto aussagekräftiger, je mehr Beschlüsse ich für die Taten mit demselben modus operandi einhole, bei denen ich der festen Überzeugung bin, dass hier bandenmäßig immer dieselben Täter vorgehen. Wenn ich dann feststelle, dass eigentlich an allen Tatorten irgendwann um 3:23 Uhr nachts immer wieder dieselbe Nummer vorkommt und nur diese eine Nummer ständig vorkommt, dann kann ich mir relativ sicher sein, dass es wahrscheinlich kein Zufall ist. Das hat meines Erachtens mit Verhältnismäßigkeit nicht so viel zu tun. Natürlich speichere ich auch andere Nummern und rufe diese ab, und in anderen Fällen habe ich andere Treffer, aber ich halte es für verhältnismäßig, insbesondere aufgrund des Umstandes, dass es in den Fällen, in denen wir die Beschlüsse beantragen, wirklich keine andere Möglichkeit gibt, es also gar keinen anderen Ermittlungsanhalt gibt, als den, dass wir eine Funkzelle abfragen. Alles andere würde bedeuten, dass wir die Verfahren sofort einstellen. Die zweite Frage habe ich so verstanden, dass ich überlegen solle, ob es tatsächlich möglich oder sinnvoll oder überhaupt zulässig sein kann, gegen die Bundesnetzagentur vorzugehen, wenn die sagt, dass sie ihrerseits keine Bußgeldverfahren wegen der Nichtumsetzung der Vorratsdatenspeicherung verfolgt, falls ich es so richtig gehört habe. Das finde ich problematisch, weil meines Erachtens etwa das OVG Münster gesagt hat, dass nicht nur die Speicherpflicht an sich rechtswidrig sei, sondern darauf dann auch kein Bußgeld gestützt werden dürfe. Das wird ja ausdrücklich im Urteil erwähnt. Aber ich glaube, insofern sind wir schon von den tatsächlichen Gegebenheiten überholt worden. Es ist inzwischen Ende April eine Vereinbarung getroffen worden mit den für uns hinsichtlich dieser Daten relevanten drei Betreibern, Telefónica, Vodafone und Deutsche Telekom AG, dass tatsächlich eine Erfassung erfolgt. Die ist zwar – finde ich – von der Begründung hinterfragenswert, allerdings sicher zulässig. Es wurde vereinbart, dass wenn in einer ganz bestimmten Form seitens der Staatsanwaltschaften angefragt wird, nämlich durch einen Beschluss nach § 100g Abs. 1 und 2 StPO in Verbindung mit § 96 TKG – richtigerweise müsste es § 113b TKG heißen –, wir dann auch die Daten erhalten. Wobei die Deutsche Telekom AG sich ausgebeten hat, dass sie uns auch nur dann retrograde Daten geben werde, wenn wir darauf hinweisen, dass ein Bußgeld erhoben werden könne, also quasi ein Ordnungsgeld angedroht werden muss. Wenn wir uns auf die tatsächlich zutreffende Rechtsgrundlage stützen würden, nämlich § 113b TKG, wird uns keiner der Betreiber die Daten geben, sodass wir uns natürlich fragen müssen, was tun wir nun? Wir sind jetzt noch nicht in diese Situation gekommen. Möglicherweise wäre eine Lösung, dass wir zwei Beschlüsse einholen. Der eine gemäß der tatsächlich bestehenden Rechtslage.

Wir fordern Vorratsdaten ab, so wie es im Gesetz geregelt ist, und holen möglicherweise – ich weiß noch nicht einmal, ob ein Ermittlungsrichter das machen würde – auch einen Beschluss hinsichtlich der Daten nach § 96 TKG ein. Und beide Beschlüsse senden wir dann den Anbietern in der Hoffnung, dass sie uns dann die retrograden Daten aushändigen. Aber wie gesagt, die Anbieter haben sich entschlossen, den Strafverfolgungsbehörden nunmehr die retrograden Daten zur Verfügung zu stellen. Danke.

Der **Vorsitzende:** Danke, Frau Leister. Die Nächste ist Frau Kurz mit zwei Antworten auf Fragen von Frau Rößner.

SVe **Dr. Constanze Kurz:** Ich glaube, ich hatte noch eine dritte Frage, zu der Wirtschaftsspionage.

Der **Vorsitzende:** Tatsächlich? Es ist heute hier alles ein wenig aus dem Ruder gelaufen. Na dann, bitte. Herr Martens ist übrigens schon bei vier Fragen.

SVe **Dr. Constanze Kurz:** Ich will nicht auf die Vorfrage eingehen, sondern nur auf diese Frage der Wirtschaftsspionage. Wir haben in den letzten vier, fünf Jahren einige sehr umfangreiche Fälle gehabt, in denen Telekommunikationsmetadaten und auch Telekommunikationsinhaltsdaten, aber aufgrund der leichteren Verarbeitbarkeit meistens die Metadaten, komplett abgegriffen worden sind. Ich darf an den griechischen Fall erinnern, bei dem übrigens auch die gesamte Regierung betroffen war. Attraktiv sind diese Daten deswegen, weil man in technisch sehr einfacher Form ein Gesamt-Sozialprofil inklusive Bewegungsdaten von denjenigen, die bei diesem Provider sind, erhalten kann. Es gibt auf der Welt ohnehin einige Staaten, die das sowieso machen. Das sind in der Regel natürlich keine Demokratien, zumindest nicht von denen ich wüsste. Aber technisch ist es natürlich möglich. Die Möglichkeit, solche großen Datenhaufen mit vorbereiteten Auswertungswerkzeugen zu bearbeiten, ist natürlich vorhanden. Vergleichbares leisten natürlich auch die Massenüberwachungsdaten der geheimdienstlichen Systeme, die ja auch Metadaten betreffen. Soweit zur Wirtschaftsspionage. Es ist, glaube ich, nachvollziehbar, dass diese Daten attraktiv sind, weil sie eben einen sehr großen Teil der Bevölkerung betreffen. Nicht jeder hat ein Telefon, aber doch sehr viele. Und weil sie sowohl machtpolitisch, als auch für die Wirtschaftsspionage attraktiv sind. Und sie bilden auch sozusagen eine Art Kommunikationsgraph. Das kann man sich mal ansehen, wenn man solche Daten auswertet für andere Länder. So etwas gibt es ja.

Zu der Frage der Unverzichtbarkeit: Für mich ist sie in mehrerer Hinsicht interessant. Sie wird ja auch schon immer, sagen wir seit zehn Jahren, debattiert. Ich halte natürlich die Unverzichtbarkeit für praktisch gegeben. Es liegt natürlich in Deutschland an den verwaltungsgerichtlichen Entscheidungen. Mich überzeugen die stets vorgebrachten Fallbeispiele nicht, denn sie sind immer auf eine bestimmte Weise konstruiert. Das haben wir schon damals 2010, als wir Sachverständige in Karlsruhe waren, erlebt. Zum einen sind die Fallbeispiele immer so konstruiert, dass die Täter so blöd sind, ein Telefon mitzunehmen, wenn ich es mal so offen sagen darf. Was natürlich nicht immer der Fall ist, aber so ist es in der Regel konstruiert. Zum anderen sind die einzelnen Fallbeispiele – die auch stimmen können und bei denen sich auch niemand darüber freut, dass dort eine Ermittlung nicht weiterkommt – für mich einfach nicht in irgendeiner Weise ins Equilibrium zu bringen mit der Tatsache des anlasslosen Festhaltens. Das überzeugt mich nach wie vor nicht. Da schwingt immer mit, als wenn ansonsten – wenn die Vorratsdatenspeicherung nicht wäre, die faktisch jetzt auch gerade nicht passiert – alle Telekommunikationsdaten sakrosankt wären. Das ist natürlich Unsinn. Und wenn ich höre, was die Herren Juristen gesagt haben über die gesetzlichen Lücken, die heute bestehen – Sie haben ein eindrucksvolles Beispiel dafür gebracht –, dann finde ich schon, dass der Gesetzgeber hier tätig werden muss. Und ich finde nach wie vor – und das sage ich aber auch schon seit zehn Jahren –, dass die Ermittlungsbehörden in den Fällen, in denen wir als Chaos Computer Club e.V. damit zu tun haben, oft eben sehr langsam agieren. Denn das Kennzeichen der digitalen Welt ist doch, dass die Daten erst einmal anfallen. Wir sollten nur dafür sorgen, dass wir sie nicht anlasslos weiterspeichern. Wir sollten aber wohl dafür sorgen, dass die Ermittlungsbehörden in der Lage sind,

wenn es notwendig ist, im Rahmen des geltenden Rechts und mit Richterbeschlüssen schnell darauf zuzugreifen.

Zu der letzten Frage, der technischen Lösung für Berufsgeheimnisträger. Technisch sehe ich dafür insofern keine Lösung. Sie könnte eigentlich denklogisch und vom Technischen her nur aus Zweierlei bestehen: Entweder Sie führen eine Liste der Berufsgeheimnisträger, aber hierzu brauche ich als Nichtjurist, glaube ich, nichts weiter zu sagen. Das ist natürlich inakzeptabel. Oder aber Sie versuchen es über die Analyse der Inhalte. Das halte ich aber auch sowohl juristisch, als auch technisch für schwierig. Sie müssen eine Form von einer Deep Packet Inspection durchführen, um irgendwie leicht entscheiden zu können, wie man die Daten aussortiert, um sie nicht zu speichern. Was ich eigentlich auch nicht für möglich halte.

Ich möchte eine letzte Tatsache anmerken, weil jetzt sehr viel über die beiden EuGH-Urteile und Karlsruhe berichtet wird. Ich möchte darauf hinweisen, dass es nicht nur um die EU-Grundrechtecharta und unsere Verfassung, sondern auch um die Europäische Menschenrechtskonvention geht. Wie Sie wissen, bin ich selber Beschwerdeführerin in einem Fall. Da geht es um Metadaten. Wir hatten bereits die Anhörung in Straßburg und die Richter haben durch ihre Fragen sehr deutlich erkennen lassen, dass es auch für die Massenüberwachung von Metadaten – und zwar geht es da auch um deren Festhalten, in diesem Fall von unseren britischen Partnern – sehr problematisch wird bezüglich grundlegender europäischer Menschenrechte. Ich bin eben ein bisschen abgebogen von der Frage der technischen Lösung und bitte um Verzeihung.

Der **Vorsitzende:** Danke, Frau Kurz. Herr Köhler hatte in der Eingangsrunde umfassend ausgeführt und keine Fragen offen gelassen. Herr Huber ist dann der Nächste mit einer Antwort auf eine Frage von Frau Winkelmeier-Becker.

SV **Alfred Huber:** Es geht wohl um zwei Punkte, wenn ich es richtig verstanden habe. Zum einen geht es um den Gesichtspunkt der Spionage und zum anderen geht es um die Frage des Missbrauchs. Was kann denn eigentlich dem Bürger draußen passieren? Ich möchte auf den Gesichtspunkt der Spionage als erstes eingehen. Ich glaube, wir müssen da zuallererst – nachdem das in der Diskussion aus meiner Sicht ein bisschen durcheinander geht – eines ganz klar feststellen: Es gibt natürlich bereits heute eine Speicherung aller 80 Millionen Handys – oder wie viel wir tatsächlich haben – durch die Provider. Nicht veranlasst durch den Gesetzgeber – keine Vorratsdatenspeicherung –, sondern eine Speicherung, die den Providern nach § 96 TKG erlaubt ist. Sie können sich das vorstellen, wie zwei große Töpfe. In den einen Topf fließen heute bereits diese ganzen Daten rein. Die darf der Provider speichern, weil er das zur Störungsbehebung braucht, weil er das braucht, um den Betrieb aufrechtzuerhalten und weil er das aus Abrechnungsgesichtspunkten braucht. Ich bin mir natürlich darüber im Klaren, dass man sich vor Spionage nie 100%ig schützen kann. Aber wir müssen uns doch auch darüber im Klaren sein, dass dieser Topf – der heute schon besteht – ebenso ausspioniert werden kann. Das ist doch völlig klar. Wir machen doch kein extra Fass auf, wenn wir jetzt einen zweiten Topf daneben stellen und sagen, dass dort jetzt verpflichtend diese Daten reingesteckt werden sollen. In dem „§§ 113a ff. TKG-Topf“ sind keine anderen Daten als in dem „§ 96 TKG-Topf“. Ich hoffe, dass unsere Provider sich dagegen entsprechend rüsten. Es gibt ja auch viele Personen aus dem Chaos Computer Club e.V., die da mittlerweile – glaube ich – beratend tätig sind. Das ist der übliche Wettlauf, den wir immer haben. Den Wettlauf – ich möchte etwas knacken bzw. ich schütze mich –, den werden wir nie und auch nicht bei der Vorratsdatenspeicherung und bei keinem anderen Punkt, wo es um Datenspeicherung geht, ausschließen können. Ich möchte nur klarstellen, dass die Vorratsdatenspeicherung mit Spionage zunächst einmal nichts zu tun hat, weil diese ganzen Daten schon jetzt bei den Providern im Rahmen der Speicherung nach § 96 TKG vorliegen.

Zur Frage, wie es denn mit dem Missbrauch aussieht: Es stellt sich doch erstmal die Frage, was mit diesen Daten denn jetzt passiert. Die Daten werden gespeichert. Da wird nicht ein Name, sondern nur eine Telefonnummer gespeichert. Es wird gespeichert, dass die Telefonnummer sich an einem bestimmten Tag in einer bestimmten Funkzelle befunden hat usw. – das gilt selbst-verständlich bezüglich aller Daten,

sowohl im „§§ 113a ff. TKG-Topf“, als auch im „§ 96 TKG-Topf“. Auch hier haben wir die gleichen Daten. Wir brauchen den § 113a TKG – die Vorratsdatenspeicherung – nur deshalb, weil die Provider in der Regel – auch da mag es vielleicht die eine oder andere Ausnahme geben – die Daten nach sieben Tagen löschen und sie damit für uns nicht mehr greifbar sind. Das bedeutet, wenn ich jetzt meinen vorherigen Vergewaltigungs- oder Totschlagsfall noch einmal zitiere: Wenn das Opfer bzw. die Leiche erst nach zwei Wochen entdeckt wird oder wenn das Opfer erst nach zwei Wochen die Anzeige erstattet, dann muss ich davon ausgehen, dass ich keine Daten mehr kriege. Und nur das wollen die §§ 113a ff. TKG: Die Verfügbarkeit dieser Daten, soweit es um Standortdaten geht, für vier Wochen sicherzustellen oder, soweit es um Verbindungsdaten geht, für zehn Wochen sicherzustellen. Das ist das Einzige, was passiert. Ansonsten werden diese Daten gelöscht. Die interessante Frage ist jetzt – weil Sie auch den Missbrauch angesprochen haben –, wie verantwortungsvoll denn die Strafverfolgungsbehörden damit umgehen. Also zunächst einmal ist doch klar, dass wir keine Namen haben. Wir haben nur eine Nummer. Wir können aufgrund dieser Nummer – wenn wir einen zusätzlichen Ermittlungsschritt gehen würden, nämlich eine Bestandsdatenanfrage bei dem Provider – herausbekommen, welche Person sich tatsächlich dahinter verbirgt. Das funktioniert nicht automatisiert. Das muss konkret nachgefragt werden, also in einer konkreten Situation angestoßen werden. Ich habe mir mal die Zahlen für das Jahr 2016 herausgesucht und mitgebracht. Das Bundesamt für Justiz hat insoweit eine Statistik. Danach haben wir hier im gesamten Jahr 2016 in insgesamt 16.000 Verfahren derartige Kommunikationsüberwachungsmaßnahmen nach § 100g StPO beantragt und dann – davon gehe ich jetzt mal aus – auch entsprechend die Daten bekommen. Jetzt kann man natürlich argumentieren, dass für 16.000 Verfahren die Daten von 80 Millionen Menschen gespeichert werden. Da sind wir wieder an dem Punkt – Frau Dr. Kurz, da bin ich durchaus bei Ihnen –, dass das eine politische Frage ist. Auch hier wieder die Frage an diejenigen, die die politische Verantwortung tragen: Wenn einer sagt, ich lasse einfach diese 16.000 Ermittlungsverfahren sausen – wobei man sagen muss, dass es schwere Straf-taten sind –, dann werden wir als Staatsanwaltschaften schlicht und einfach sagen, dass uns die Hände gebunden sind. Wir können nichts machen. Wir stellen dieses Verfahren ein, genauso wie es die Frau Leister gesagt hat. Mich ärgert massiv – und vielleicht auch schon seit zehn Jahren, das kann ich in diesem Zusammenhang auch gleich mal sagen – der Punkt, dass man immer sagt, man könne doch nicht beweisen, was die Vorratsdatenspeicherung gebracht hätte. Allein aus Gründen der Logik kann es doch nicht funktionieren. Wenn ich eine Maßnahme nicht anwenden darf, dann kann ich doch nicht beweisen, was sie gebracht hätte. Ich kann umgekehrt vielleicht sagen: In einer bestimmten Zahl von Fällen haben wir es eingesetzt und gerade im hochsensiblen Bereich des Wohnungseinbruchsdiebstahls haben wir dabei hervorragende Erfolge erzielt, insbesondere mit retrograden Standortdaten, weil man eben sieht, wo sich die Leute bewegt haben. Wir führen über sehr Vieles Statistiken, darüber jedenfalls derzeit nicht. Ich habe aber überhaupt keine Zweifel aufgrund der vorliegenden Zahlen. Wenn Sie die 16.000 Verfahren in der ganzen Bundesrepublik betrachten – das sind 16.000 schwere Straftaten gewesen. Das wird also verantwortungsvoll genutzt. Ich bin schon fast der Meinung – da bin ich noch einmal bei der Frau Dr. Kurz –, dass vielleicht ja etwas ganz Geniales heute passiert. Wenn Sie sagen, Sie möchten, dass die vorhandenen Daten benutzt werden – da schließe ich mich an. Wir haben nämlich – darauf möchte ich noch einmal hinweisen – bei den retrograden Standortdaten derzeit die ganz schwierige Situation, dass diese Daten im „§ 96 TKG-Topf“ liegen und wir größte Probleme haben, an diese heranzukommen.

Also möchte ich noch einmal nachhaltig dafür plädieren, den § 100g Abs. 1 Satz 3 StPO abzuändern, so dass retrograde Standortdaten, die vorhanden sind und die im „§ 96 TKG-Topf“ liegen, auf alle Fälle von den Strafverfolgungsbehörden genutzt werden können… Ich will jetzt nicht weiter reden, weil ich schon 8:20 Minuten rede und der Herr Vorsitzende bereits äußerst unruhig wird, was ich verstehen kann. Aber das letzte Mal war es auch so. Da saß die Frau Künast da, die hat auch schon etwas gezappelt.

Der **Vorsitzende:** Wir haben eine Datenschutzbeauftragte in Deutschland, die kann das auch ganz gut – umfassende Ausführungen machen.

SV **Alfred Huber:** Jedenfalls ist die ganze Geschichte so, dass wir hier Daten haben und sie nicht benutzen dürfen. Es gibt zurzeit – die Frau Leister hat es ja erklärt – einige Klimmzüge, mit denen man versucht, an die Daten heranzukommen. Da könnte uns der Gesetzgeber massiv helfen, wenn man § 100g Abs. 1 Satz 3 StPO auf seinen alten Rechtsstand von vor 2015 zurückführen würde.

Der **Vorsitzende:** Wenn wir noch dazu kommen, dann machen wir das vielleicht auch irgendwann.

SV **Alfred Huber:** So lange rede ich nicht.

Der **Vorsitzende:** Vielen Dank. Der Herr Gnisa ist der Nächste mit einer Antwort an Frau Winkelmeier-Becker.

SV **Jens Gnisa:** Ja gerne. Ich kann es vielleicht etwas kürzer halten und etwas Zeit herausholen. Es ist so, dass ich noch zwei ergänzende Punkte zu Herrn Huber, also zu denselben Fragen, anbringen möchte. Was könnte passieren? So lautete Ihre Frage. Im schlimmsten Fall gäbe es Missbräuche. Erstens möchte ich darauf hinweisen, dass der EuGH ja in seinen Entscheidungen selbst im Prinzip immer wieder auf eine mögliche Einschränkung hinweist, nämlich die Angst des Bürgers vor Überwachung und damit auf Verhaltenseinschränkungen des Bürgers. Dies sehe ich letztendlich in diesem Fall nicht. Auch gerade in Deutschland sehe ich das nicht, weil wir eben ein zweistufiges Verfahren haben. Es ist mehrfach angesprochen worden. Die erste Stufe betrifft die umfassende Datenerhebung. Und auf der zweiten Stufe ist dann aber nur ein ganz eingeschränktes Abgreifen der Daten möglich. Ich habe auch den Eindruck, dass bei dem Bürger diese Dinge durchaus angekommen sind. Ich weiß jetzt nichts von einer Vertrauenskrise oder derartigem. Also ich denke, der Bürger vertraut auf die Integrität der Daten und das sieht man ja auch bei der Parallelerwägung, dass zum Beispiel so gut wie keine Fälle bekannt sind, in denen sich der Bürger mal darüber beschwert hat, dass seine Daten nach § 96 TKG oder zur Qualitätssicherung gespeichert werden. Also darüber müsste er sich dann ja auch beschweren. Da ist mir zumindest jetzt nichts bekannt.

Das zweite Argument, auf das ich noch eingehen möchte, ist auch von der Frau Dr. Kurz, was ja irgendwie in die Richtung geht, dass wenn Daten vorgehalten werden, sie auch von irgendwem irgendwann in rechtswidriger Weise abgegriffen werden, Stichwort: Wirtschaftsspionage. Ich glaube, das ist letztendlich nicht nur ein Problem der Vorratsdatenspeicherung, sondern der gesamten Datenspeicherung. Es geht um Datensicherheit generell. Wir brauchen natürlich grundsätzlich ein hohes Maß an Datensicherheit, sodass dann das Problem eigentlich viel weitergehender gezogen werden müsste. Da benötigen wir natürlich ausreichende Investitionen, aber auch ein ausreichendes Verständnis für die Datensicherheit. Und vielleicht darf ich noch den Grundsatz der Datensparsamkeit ansprechen, den Sie ja damit, glaube ich, auch meinen. Ein alter datenschutzrechtlicher Grundsatz, wonach möglichst wenig Daten zu erheben sind. Das ist schon richtig, aber auch da darf ich noch einmal die Parallele zu § 96 TKG ziehen und zu den weiteren Speicherungen, etwa aus Qualitätsgründen usw… Inwieweit jetzt nach § 113a TKG mehr Daten gespeichert werden – das kann man sicherlich diskutieren. Sie wollen da sicherlich gleich noch etwas dazu sagen, aber da muss man natürlich dann auch in die Abwägungsfrage kommen. Stichwort: Angst des Bürgers vor Missbrauch. Ich sehe hier – um das noch einmal auf den Punkt zu bringen – eigentlich genau den gegenteiligen Wunsch der Bürger nach Schutz vor Kriminalität. Und deswegen sehe ich auch letztendlich keine Einschränkungen im Verhalten bei den Bürgern. Herzlichen Dank.

Der **Vorsitzende:** Vielen Dank, Herr Gnisa. Eine der vielen Fragen von Herrn Martens hat Herr Cole bekommen. Herr Martens ist aber nicht mehr da. Dafür nimmt Herr Höferlin die Antwort stellvertretend entgegen. Und er hat auch selbst ein Interesse an den Ausführungen. Bitte, Herr Cole.

SV **Prof. Dr. Mark Cole:** Das gibt mir auch die Gelegenheit, die vorhin in der gebotenen Kürze der Zeit sehr knappen Ausführungen insofern zu unterstreichen, als dass in der Tat die Frage, warum der EuGH – um es mal etwas platt auszudrücken – ein Problem mit der Vorratsdatenspeicherung hat, sehr früh ansetzt und nicht erst

bei der Frage, was mit den Daten im Rahmen der Strafverfolgungsbehörden geschieht. Ich glaube, es ist auch kein Misstrauen auf der Seite des EuGH, dass beispielsweise Strafverfolgungsbehörden zu exzessiv Daten abrufen würden. Er trifft seine Feststellungen ganz nüchtern. Und deswegen plädiere ich ja auch dafür, dass man zunächst einmal möglichst nüchtern betrachtet, was bei der Vorratsdatenspeicherung passiert, und nicht einzelne Gegenbeispiele anbringt und argumentiert, dass ohne die Vorratsdatenspeicherung dies und jenes passiert. Bereits die – zwar bei Privaten erfolgende, aber staatlich, nämlich durch eine gesetzliche Pflicht veranlasste – Speicherung der Daten in diesem Volumen ist das Problem. Es geht nicht um die Frage, was in einem zweiten Schritt mit diesen Daten geschieht. Der Zugriff auf die Daten ist nämlich ein weiterer Eingriff, aber bereits den ersten Schritt der anlasslosen massiven Speicherung der Daten sieht der EuGH als ein Problem an. Der EuGH stellt das nicht einfach nur so fest, sondern er präzisiert, warum das so ist. Einerseits sagt er, dass die Möglichkeit, nicht nur mit den Kommunikationsdaten, sondern auch – oder vielleicht sogar noch mehr – mit den Rahmendaten, den Verkehrsdaten oder den Bewegungsdaten Rückschlüsse auf das Verhalten von Personen zu ziehen, eine Gefahr ist, die nicht unterschätzt werden darf. Und natürlich wäre das Speichern aller Kommunikationsinhalte ein Verstoß. Aber dann würde der EuGH so weit gehen und feststellen – das hat er in der Schrems-Entscheidung angedeutet –, dass es sich sogar um einen Eingriff in den Wesensgehalt des Grundrechts handeln würde. Da gäbe es überhaupt keine Abwägung mehr und es läge ganz klar ein Verstoß vor. Darunterliegend – bei den Verkehrsdaten – ist es aber nicht so, dass sie weniger problematisch sind, nur weil entsprechende Maßnahmen vom Datensubjekt weniger stark als Eingriff empfunden werden. Wenn man sagt, dass es nötig ist, von allen Nutzern der Telekommunikationsdienstleistungen diese Daten zu erheben, dann stellt der EuGH fest, dass man eine ganz enge Verbindung zwischen dem legitimen Ziel und der Schwere dieses Eingriffs benötigt. Da wirft er die Frage auf, ob bereits bei der Erhebung diese enge Zweckbindung gegeben ist. Und das wird man wohl bestreiten können, weil in der Tat die Evidenz nicht dafür spricht, zu sagen, dass man die Daten – vielleicht nicht von 80 Millionen, weil nicht jeder eine Telekommunikationsnutzung vornimmt – aber vielleicht von 50 Millionen Bürgern – um das Beispiel Deutschlands zu nehmen – erheben muss, um mit den Daten dann später in der Strafverfolgung arbeiten zu können. Wenn das nicht der Fall ist – auch wenn es möglicherweise nützlich ist, diese Daten zu haben –, genügt das nicht. Die Erhebung der Daten an sich ist ein Problem. Da genügt es nicht, zu sagen, dass es aber mal oder sogar in vielen Fällen helfen kann. Das mag so sein und deswegen ist es auch eine harte Erkenntnis, dass, wenn die Daten wegfallen, vielleicht tatsächlich die eine oder andere Straftat weniger gut aufklärbar ist, aber das genügt nicht. Es muss klar sein, dass die Erhebung der Daten ohne Ausnahme notwendig ist, um überhaupt in diesem Bereich arbeiten zu können. Wenn das nicht der Fall ist, dann sagt der EuGH, dass man schon diese Erhebung nicht durchführen darf.

Nun ist zurecht darauf hingewiesen worden, dass es in der Tat nicht um das deutsche System ging, und man wird auch sagen können, dass die aktuelle deutsche Rechtslage sicherlich weniger einschneidend oder weniger eingreifend ist, als viele der Beispiele von anderen Mitgliedstaaten. Aber daraus kann man aus meiner Sicht umgekehrt nicht ableiten, dass das deutsche System auf jeden Fall zulässig ist.

Weil die Grundaussage dieser beiden Urteile – insbesondere, wenn man sie in größeren Kontext setzt, also mit dem Gutachten zur Fluggastdatenspeicherung und der sogenannten Schrems-Entscheidung – eher darauf hindeutet, dass massenhafte Datenspeicherung ohne Anlass per se ein Problem ist. Jetzt kann man natürlich sagen, dass wir dann noch einmal abwarten, was mit dem deutschen Gesetz passiert und wir dann abwarten, was mit dem französischen Gesetz passiert und dann abwarten, was mit dem italienischen Gesetz passiert. Das kann man machen. Man kann es auf die nationalen Verfassungsgerichte oder den EuGH zurückführen. Man kann aber auch sagen, dass man die Nachricht verstanden hat und das System einmal umdreht und proaktiv möglicherweise hier Korrekturen vornimmt. Vielleicht dazu noch Eines: Das Erfordernis, dass die Vorratsdatenspeicherung zur Bekämpfung schwerer Straftaten genutzt wird, ist ein absolutes Minimum. Der EuGH lässt da auch keinen Interpretationsspielraum und sagt, dass das mindestens

vorliegen muss. Dass die Vorratsdatenspeicherung beispielsweise für kleinere Delikte genutzt werden könnte, steht gar nicht zur Debatte. Aber selbst wenn sie zur Bekämpfung von schweren Straftaten eingesetzt wird, genügt das allein nicht. Und warum ist er sich da relativ sicher? Weil er bereits jetzt – Frau Dr. Kurz hat es angedeutet – in den Verfahren vor dem Gerichtshof in Straßburg, also dem Europäischen Gerichtshof für Menschenrechte (EGMR), wird man das noch deutlicher zu hören bekommen… Aber im Prinzip muss man die gar nicht abwarten. Bereits jetzt ist es so, dass der EuGH in den relevanten Urteilen mit Straßburg im Prinzip Ping Pong spielt. Also sowohl in der Tele2- als auch den Vorgängerentscheidungen wird auf die Rechtsprechung in Straßburg Bezug genommen und umgekehrt. Und zwar auf welche Rechtsprechung? Die Rechtsprechung über geheime Abhörmaßnahmen, also normalerweise geheimdienstliche Abhörtätigkeiten, die hier natürlich nicht einschlägig sind. Aber die Maßstäbe, die dort angewendet werden nach Art. 8 Europäische Menschenrechtskonvention, nutzt der EuGH auch, um zu sagen, dass wir ein Grundsatzproblem haben, wenn man eine anlasslose Verkehrsdatenspeicherung vornimmt. Und in der Tat: Man kann politisch sagen, dass man selbst das nicht entscheiden will – man wartet ab, was die Gerichte sagen. Aber ich halte es für klug, dass hier vorangeschritten wird und möglicherweise darüber nachgedacht wird, ob man einen – wenn überhaupt – harmonisierten Ansatz auf europäischer Ebene findet. Danke.

Der **Vorsitzende:** Danke, Herr Cole. Herr Höferlin, Sie haben alles mitgeschrieben und berichten dann? Prima, danke schön. Dann ist die erste Frage- und Antwortrunde beendet. Wir kommen zur zweiten Fragerunde. Ich habe da vier Wortmeldungen notiert. Herr Müller, Frau Rößner, Frau Winkelmeier-Becker und Herr Movassat. Mit Herrn Müller beginnen wir, bitte.

Abg. **Axel Müller** (CDU/CSU): Ich habe zunächst eine Frage an Sie, Herr Professor Cole. Sie haben die Frage wahrscheinlich auch schon teilweise beantwortet. Es geht um die Entscheidung des EuGH, die Sie zitiert haben. Die letzte stammt nach meinem Kenntnisstand aus dem Jahr 2014. Die Entscheidung des Bundesverfassungsgerichts, die Sie erwähnt haben, stammt aus dem Jahre 2016. Sie war wiederum Grundlage für die Änderungen, die der nationale Gesetzgeber vorgenommen hat. Dabei handelte es sich ja auch um Beschränkungen in zeitlicher Hinsicht – zehn Wochen Speicherdauer für die Verbindungsdaten und vier Wochen Speicherdauer für die Standortdaten –, während die Entscheidung des EuGH immer noch von einer sechsmonatigen Speicherung ausgegangen ist. Wenn Sie jetzt die beiden Entscheidungen nebeneinander legen und die Entscheidung des EuGH mit den dort aufgestellten Maßstäben noch einmal in Verbindung bringen mit der Entscheidung des Bundesverfassungsgerichts, die zur aktuellen Gesetzeslage geführt hat – Kommt man dann nicht zu der Überzeugung oder der Auffassung, dass die Entscheidung des EuGH im Grunde genommen überholt ist, bzw. der nationale Gesetzgeber den Anforderungen, die der EuGH gestellt hat, in ausreichendem Maße Rechnung getragen hat? Zumal ja genau das, was der EuGH in seiner Entscheidung gefordert hat, nämlich eine Differenzierung, eine Einschränkung und eine Zielbestimmung, was die Bekämpfung schwerer Straftaten betrifft, durch das hier gewählte zweistufige Verfahren – das jetzt auch schon mehrfach vorgestellt wurde – in ausreichendem Maße verwirklicht wurde. Das ist meine erste Frage.

Die zweite Frage richtet sich an die Frau Rechtsanwältin Dr. Sandkuhl und zwar in ihrer Eigenschaft als Organ der Rechtspflege. Da schildere ich Ihnen jetzt mal einen Fall aus meiner Praxis als Vorsitzender Richter einer Strafkammer, der ist vielleicht auch ganz interessant für Sie, Frau Dr. Kurz. Es findet eine Motorradmesse statt. Eine friedliche Gruppe Messebesucher begibt sich auf die Messe und gleichzeitig begibt sich eine Rocker-Gruppe auf die Messe. Die Rocker-Gruppe fühlt sich in irgendeiner Form durch die friedlichen Messebesucher gestört. Da beschließt die Rocker-Gruppe, die friedlichen Messebesucher zu verprügeln. Die Opfer erleiden schwerste Verletzungen. Als es zum Strafverfahren kommt, sagt der Haupttäter, dass er doch gar nicht am Tatort gewesen sei. Er belegt es mit einer Alibi-Zeugin, die bezeugt, dass er in einer Rocker-Kneipe ungefähr 30 Kilometer vom Tatort entfernt gewesen sei. Stichwort: Alibi-Zeugen – das zur Frage, welche Möglichkeiten wir sonst noch

besitzen. Wir können durch einen Funkzellenabgleich nachweisen, dass er sich im Bereich der Messe befunden hat. Dass es also nicht sein kann, dass er sich zur Tatzeit 30 Kilometer entfernt aufgehalten hat. Das war letztendlich …

(Unverständliche Zwischenrufe)

Das Handy war dort. Es war nachgewiesen, dass er sein Handy nicht aus den Augen lässt. Das ist so, wie bei den meisten von uns – wir tragen es ständig mit uns herum. Die Einlassung, man habe sein Handy mal kurz verliehen, kommt zwar immer wieder vor, aber wenn Sie sich alle mal an die eigene Nase fassen – Wie oft verleihen Sie ihr Handy? Jedenfalls hat das letztendlich dazu geführt, dass ein Freispruch vermieden werden konnte. Mit der Alibi-Zeugin wäre dieser Täter sonst definitiv nicht zu überführen gewesen. Gegen die Alibi-Zeugin wurde ein Verfahren wegen Falschaussage eröffnet. Sie ist rechtskräftig verurteilt worden und hat in ihrem eigenen Verfahren – um eine mildere Strafe zu bekommen – die Tat gestanden. Dies zur Frage des empirischen Nachweises. Und jetzt die Frage an Sie als Organ der Rechtspflege: Was wäre Ihnen denn lieber gewesen als Strafverteidigerin? Dass man den Haupttäter freigesprochen hätte oder wäre es Ihnen doch lieber gewesen, ihn rechtskräftig verurteilen zu können?

Der **Vorsitzende:** Danke, Herr Müller. Frau Rößner, bitte schön. Und danach Frau Winkelmeier-Becker.

Abg. **Tabea Rößner** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank nochmals. Das ist ein spannender Fall. Ich kann Ihnen versichern, dass ich mein Handy regelmäßig irgendwo vergesse, ob im Taxi oder sonst wo. Das kann immer mal passieren. Ich würde nie meine Hand dafür ins Feuer legen, dass ich mein Handy immer bei mir habe. Ich habe noch einmal zwei Fragen an Frau Dr. Kurz: Es gab ja vor kurzem die polizeiliche Kriminalstatistik, nach der wir im Jahr 2017 so wenige Straftaten hatten, wie seit 25 Jahren nicht mehr. Das Bundeskriminalamt stellt sich nun aber hin und veröffentlicht eine Sammlung an Einzelfällen, mit deren Hilfe es beweisen will, dass die Vorratsdatenspeicherung so dringend erforderlich sei. Es gab jetzt auch eine Analyse, über die Netzpolitik.org berichtet hat. Vielleicht können Sie hierzu einmal Ihre Einschätzung deutlich machen. Und die zweite Frage bzw. Bitte wäre, noch einmal ganz pointiert und zugespitzt zu erläutern, welches der bürgerrechtliche Preis ist, den wir mit der Einführung der Vorratsdatenspeicherung zahlen, und welches die gesellschaftlichen, demokratischen und rechtsstaatlichen Folgen sind. Vielen Dank.

Der **Vorsitzende:** Danke schön. Frau Winkelmeier-Becker bitte und dann Herr Movassat.

Abg. **Elisabeth Winkelmeier-Becker** (CDU/CSU): Vielen Dank. Ich möchte eine Frage an Herrn Professor Wollenschläger richten und darum bitten, noch einmal die Unterschiede zwischen der aktuellen deutschen Rechtslage und den jeweils den EuGH-Entscheidungen zugrunde liegenden nationalen Regelungen herauszuarbeiten. Wenn Sie da noch einmal deutlich machen könnten, welche zusätzlichen Einschränkungen und Missbrauchshürden im deutschen Recht vorgesehen sind. Meine These ist, dass der EuGH in nachvollziehbarer Weise natürlich damit rechnet, dass seine Aussagen europaweit gelesen und interpretiert werden. Und dass sich etwa eine Aussage, dass bestimmte Daten gespeichert werden dürfen, möglicherweise aus bulgarischer Sicht und nach dortigem rechtsstaatlichem Niveau anders anhört und auch auswirkt als nach deutschem Recht, wo eben der Vorbehalt der Entscheidung eines unabhängigen Richters vorgesehen ist. Könnte das möglicherweise mit einer der Gründe dafür sein, weshalb die Haltung des EuGH insoweit so restriktiv ist? Weil er immer auch mit in Rechnung stellt, dass bei einem Staat, der sich auf eine Vorratsdatenspeicherung stützt, die rechtsstaatlichen Absicherungen möglicherweise nicht so hoch sind, wie bei uns.

Dann würde ich doch gern auch noch einmal an Sie die kurze Frage nach dem Missbrauchspotential stellen. Weil mir hier bei den Antworten auffällt, dass wenn es um die Missbrauchsmöglichkeiten geht, immer sehr abstrakt argumentiert wird. Dass das informationelle Selbstbestimmungsrecht abstrakt irgendwie beeinträchtigt sein könnte, während die Nachteile von Opfern von Straftaten immer sehr konkret sind. Und da scheint mir ein Missverhältnis zu bestehen. Deshalb auch noch einmal an Sie die Frage: Gibt es aus Ihrer Erkenntnis heraus irgendwo einen konkreten Missbrauchsfall? In

dem eine konkrete Person erpresst oder unterdrückt worden ist? Politisch irgendwelchen Repressalien unterlag? In dem irgendetwas passiert ist, bei dem man sagt, dass das der Nachteil der Vorratsdatenspeicherung ist? Gibt es da irgendeinen ganz konkreten individuellen Nachteil, der nicht in die Richtung von dem geht, was Frau Dr. Kurz angesprochen hat? Insoweit würde ich vermuten, dass es sich eher um eine Art Data-Mining handelt. Man kann die Daten insgesamt auswerten, aber kann man wirklich eine konkrete Person aufgrund dieser erpressen? Etwa: „Ich habe gesehen, Du hast mit einem bestimmten Terroristen oder einem bestimmten Schwerverbrecher telefoniert, und daraus kann ich jetzt irgendwelche Dinge ableiten.“ Gibt es da einen konkreten Fall, wo eine Person einen Nachteil hatte?

Der **Vorsitzende:** Danke schön, Frau Winkelmeier-Becker. An wen haben Sie die zweite Frage gerichtet?

Abg. **Elisabeth Winkelmeier-Becker** (CDU/CSU): Alle Fragen gingen an Herrn Professor Wollenschläger.

Der **Vorsitzende:** Alles klar. Dann hören wir jetzt die Fragen von Herrn Movassat und danach die von Herrn Reusch.

Abg. **Niema Movassat** (DIE LINKE.): Ich will zumindest festhalten, Frau Kollegin Winkelmeier-Becker, dass die Entscheidung des EuGH vom 21. Dezember 2016 zu Schweden und zu Großbritannien erging. Ich glaube, wir sind uns einig, dass es sich dabei um Rechtsstaaten handelt und dass es damit keine Entscheidung zu Staaten war, bei denen der EuGH vermutet, dass die Rechtsstaatlichkeit nicht ausreichend gewahrt ist. Und er muss harte Grenzen setzen. Ich glaube auch, dass der EuGH versucht, einheitliche Standards zu setzen. Das ist ja das Ziel. Und ich muss auch sagen, dass mich viele Argumente heute in der Anhörung nicht überzeugt haben. Ich finde, es wurde sehr monokausal auf die Ermittlungen geschaut, in dem Sinne: „Man braucht die Vorratsdatenspeicherung, sonst kann man bestimmte Ermittlungen gar nicht durchführen.“ Ich glaube, Ermittlungen finden auf vielen Schienen statt und sind nicht auf eine Ermittlungsmaßnahme beschränkt. Das kam jedoch heute teilweise hier so rüber, als die Fälle geschildert wurden. Zweitens wurde hier immer wieder der Fall des ermordeten Menschen im Waldstück genannt, bei dem ohne die Vorratsdatenspeicherung innerhalb von sieben Tagen die relevanten Daten gelöscht werden. Und was tun Sie, wenn Sie nach vier Wochen und einem Tag die Leiche finden? Dann sind die Daten auch weg. Also ich meine, diese Argumentationskette führt dann letztlich dazu, eine immer längere Datenspeicherung zu fordern. Ich will das nur mal als Feedback erwähnen.

Eine Frage habe ich aber tatsächlich an Herrn Köhler. Sie haben ja auch in Ihrer schriftlichen Stellungnahme ausgeführt, dass die EuGH-Entscheidung zur Vorratsdatenspeicherung nicht unmittelbar auf Deutschland anwendbar ist. Mich würde schon noch einmal genauer interessieren, wie Sie darauf kommen. Und mich würde eine Einschätzung von Ihnen zu der Frage interessieren, wie der EuGH entscheiden würde, wenn er die deutsche Regelung zur Vorratsdatenspeicherung auf den Tisch bekäme. Da ja der EuGH die anlasslose Datenspeicherung an sich und nicht erst die Ebene der Verwertung kritisiert hat. Danke schön.

Der **Vorsitzende:** Der Nächste ist Herr Reusch. Bitte.

Abg. **Roman Reusch** (AfD): Drei unserer Sachverständigen, nämlich Herr Professor Cole, Frau Dr. Kurz und Frau Dr. Sandkuhl, haben – wenn ich richtig mitgeschrieben habe – das Fehlen empirischer Untersuchungen zur Frage der Effizienz und Notwendigkeit von solchen Maßnahmen beklagt. Ich würde gerne von allen Dreien wissen, wie Sie sich solche Untersuchungen vorstellen und weshalb Sie meinen, dass die Auffassungen und die Erfahrungen der Praktiker, die tagtäglich damit zu tun haben, nicht ausreichen. Wenn Ihnen Leute, die wirklich jeden Tag die entsprechenden Akten auf dem Tisch haben, sagen, dass wir ohne diese Maßnahmen relativ „blank“ sind – weshalb reicht das nicht? Weshalb meinen Sie, muss man zu weiteren Maßnahmen greifen, um sich hierzu eine Meinung zu bilden?

Der **Vorsitzende:** Danke schön. Wobei ich noch einmal darauf hinweisen möchte, dass wir

eigentlich eine Frage an zwei Sachverständige oder zwei Fragen an einen Sachverständigen stellen wollten.

(Unverständlicher Zwischenruf)

Der **Vorsitzende:** Ich denke, angesichts der Tatsache, dass die Rednerliste in der zweiten Fragerunde jetzt auch erschöpft scheint, können wir diese Ausnahme noch einmal machen. Wir gehen in die Antwortrunde und beginnen diesmal wieder alphabetisch von vorn, also mit Herrn Cole, bitte.

SV **Prof. Dr. Mark Cole:** Zunächst einmal zur Situation beim EuGH. Also das letzte Urteil, was ich zunächst einmal angeführt habe, Herr Müller, ist das vom Dezember 2016. Ich bin sogar noch einen Schritt weitergegangen und habe gesagt, dass man auch das Gutachten zum Passenger-Name-Record-Abkommen EU-Kanada vom Folgejahr, das keine Entscheidung zur Vorratsdatenspeicherung darstellt, mit heranziehen muss, um die Rechtsprechungslinie des EuGH zu sehen. Bislang liegt die deutsche Regelung zur Vorratsdatenspeicherung nicht auf dem Tisch des EuGH. Man kann sich also ganz weit zurücklehnen und sagen: Solange das nicht entschieden ist, weiß man nicht, wie die Regelung europarechtlich zu bewerten ist. Man kann sich aber auch diese Reihe an Urteilen anschauen – unabhängig davon, dass zwischenzeitlich das Bundesverfassungsgericht sich dazu geäußert hat, ob im Eilrechtsschutz etwas gegen die Anwendung der derzeitigen deutschen Rechtslage zu unternehmen ist – und sich fragen, ob es eine Linie in der EuGH-Rechtsprechung gibt, die sogar über die enge Frage der Kommunikationsvorratsdatenspeicherung hinausgeht. Und ich hoffe, es ist mir gelungen, zu zeigen, dass der EuGH eine Liste an Kriterien aufgebaut hat, die eine hohe Hürde darstellt, die man überspringen muss. Das mag man bedauern, aber die Hürde ist relativ hoch. Und die sieht zum Beispiel nicht so aus, zu sagen, dass eine anlasslose allgemeine Speicherung möglich ist, aber beispielweise, er nennt das Targeted Retention – zielgerichtet, um es mal ganz platt auszudrücken – … Es wäre wohl denkbar – beispielsweise jetzt im Rahmen des anstehenden Fußballfestes – eine Gegend einzubeziehen, in der im Rahmen von Public-Viewing-Angeboten die Gefahr eines Anstiegs von Kriminalität gegeben ist. Das wäre denkbar. Das wäre vielleicht etwas, was der EuGH als zielgerichtet oder geografisch eingeschränkt ansieht. Auch das ist übrigens Kritik begegnet, weil man gesagt hat: Nehmen wir mal keinen bestimmten Anlass, sondern eine Gegend mit einer höheren Kriminalitätsrate. Da gibt es beispielsweise in Brüssel bestimmte Stadteile, die vielleicht davon erfasst würden. Auch da gilt natürlich dann die Frage, ob es andere Erwägungen gibt, die möglicherweise dagegen sprechen. Etwa eine Art diskriminierenden Faktor? Das ist auch als Kritik am Tele2-Urteil geäußert worden. Aber tatsächlich würde das eher dem Bild des EuGH entsprechen. Die Mitgliedstaaten übrigens – um auch das mal einzubringen – haben das aus meiner Sicht als Gedanken aufgegriffen. Es wird aktuell im Rat diskutiert. Die nennen das einen Repeated Retention Warrant (RRW). Wo man sagt: OK, wir akzeptieren, dass es grundsätzlich keine solche Vorratsdatenspeicherung geben kann. Also wenn wir sie gezielt für bestimmte Zeiträume schaffen – und ich meine jetzt nicht damit, dass die Speicherung zeitlich limitiert ist. Im Moment haben wir ein Kriminalitätsproblem. Das ist statistisch im Laufe der letzten Jahre ersichtlich. Der Typ des „schweren Verbrechens“ wird verstärkt begangen. Mit den Verkehrsdaten haben wir die Möglichkeit, insoweit besser vorzugehen. Dass dann eine limitierte Vorratsdatenspeicherung eingeführt wird und dieser RRW soll dann dazu führen, dass man das ohne allzu großen argumentativen Aufwand mehrfach verlängern kann. Es ist erkennbar, dass die Mitgliedstaaten im Moment am Suchen sind, was der beste Weg ist, diese Targeted Retention zu erreichen. Die Tatsache, dass das Bundesverfassungsgericht sich in der Zwischenzeit hierzu geäußert hat, ändert am Befund zunächst einmal nichts, weil es nicht um die Frage ging, ob die deutsche Rechtslage allgemein mit dem Europarecht vereinbar ist oder nicht, sondern es um die Frage ging, wie im Rahmen von Eilrechtsschutz damit umzugehen ist. Ich bin zwar nicht gefragt worden, ob ich prognostisch tätig sein will, aber ich möchte es, weil es im Grunde genommen in Ihre Frage hineinspielt. Hat nicht die deutsche Rechtslage eine wesentlich differenziertere Herangehensweise als die schwedische, englische oder auch andere, die bereits diskutiert worden sind? Da wäre meine Antwort: ja. Aber auch diese differenzierte

Herangehensweise beseitigt das Grundproblem nicht. Also deswegen kann man abwarten, ob der EuGH sagt: Das ist sozusagen der Spalt in der Tür, den die Deutschen richtig genutzt haben, das kann man machen. Oder er sagt: Das Grundsatzproblem ist, dass die Tür aufgemacht wird. Zu Ihrer Frage: Es geht weniger darum, ob ich es für richtig halte, dass eine Evidenz aufgebracht wird. Aber der EuGH spricht von objektiven Belegen, die dafür sprechen, dass diese Form des Eingriffs als einzige Möglichkeit notwendig ist, um dem geplanten Ziel besserer Strafverfolgung und Strafvereitelung für diese bestimmten Straftaten zu genügen. Und es hat nichts mit der Bezweifelung der Kompetenz der Strafverfolgungsbehörden zu tun, wenn man sagt, dass es nicht genügt, wenn einer aus der Praxis sagt, dass er dieses Werkzeug benötigt. Sondern es hat eher etwas damit zu tun, glaube ich, dass in dem ursprünglichen Verfahren zur Richtlinie zur Vorratsdatenspeicherung sich alle statistischen Daten nicht mit den Aussagen der Praktiker gedeckt haben. In dem Sinne, dass also gesagt wurde, wir hatten so und so viele Verfahren, dann gab es so und so viele Beweismittel, eines davon waren auch die erhobenen Verkehrsdaten und das war der Ausgang. Es war nicht so, dass eine Linie gezeichnet werden konnte, nach der eine bestimmte Anzahl von Straftaten nicht aufgeklärt worden wäre ohne die Verkehrsdaten. Was dazu geführt hat, dass die Richtlinie zur Vorratsdatenspeicherung vom EuGH gekippt wurde. Seither verfolgt er diesen Ansatz, wonach man wegen der Schwere des Eingriffs zuerst Belege benötigt, die diesen Eingriff rechtfertigen. Mir ist schon klar, dass wir hier sozusagen in zwei verschiedenen Lagern stehen. Aber man muss es aus meiner Sicht andersherum angehen. Man kann nicht fragen, ob es denn schlimm wäre, wenn diese Daten missbraucht würden. Ist es denn problematisch? Ist der Eingriff wirklich so schmerzhaft für das Individuum? Das ist gar nicht die Frage, die gestellt wird. Es ist umgekehrt die Frage, ob der Staat eine Regelung vorsehen darf, bei der es zu diesem Eingriff kommt. Und das darf er nur dann, wenn klar ist, dass ohne diese Daten – und zwar nicht im Einzelfall, sondern ganz prinzipiell – das Ziel der Strafverfolgung schwerer Straftaten nicht erreicht werden kann.

Der **Vorsitzende**: Danke, Herr Cole. Herr Gnisa und Herr Huber sind in dieser Runde leer ausgegangen. Herrn Köhler wurde von Herrn Movassat eine Frage gestellt.

SV **Marcus Köhler:** Vielen Dank für die Frage. Es ist nicht die klassische „Wie würden Sie entscheiden?“-Frage. Ich habe zwar als Wahlfach Europarecht belegt, aber als Praktiker mache ich es mal wie Karl Valentin, dem großen Philosophen, und sage: Prognosen sind schwierig, vor allem wenn sie die Zukunft betreffen. Jetzt mal im Ernst. Wenn ich mir das hier alles anhöre, geht es aus meiner Sicht wild durcheinander mit den Begriffen wie Erhebung, Festhalten und Überwachung. Von was sprechen wir? Also zum Beispiel, wenn es heißt: Erhebung braucht einen Anlass. Dann schaue ich in das Gesetz und dort heißt es: „[…] so dürfen Verkehrsdaten erhoben werden bei einem Tatverdacht“. Das wäre also nach dem EuGH gar kein Problem. Wenn ich frage, was denn die Eingriffstiefe der Speicherung ist: Nehmen wir das Bundesverfassungsgericht, dass dabei – das war ein Urteil mit Gesetzeskraft – auf das diffuse Gefühl des Überwachtseins abstellt. Man muss mal dabei bleiben. Deswegen gibt es für mich eigentlich nur eine Sache und da haben Sie völlig Recht: Beim EuGH liegt die deutsche Regelung momentan nicht. Das ist das, was ich gesagt habe – nicht mehr und nicht weniger. Beim Bundesverfassungsgericht liegt die Regelung hingegen. Das Bundesverfassungsgericht – da habe ich großes Vertrauen und stimme, glaube ich, mit Ihnen allen hier überein, auch mit der Bevölkerung – wird die Rechtsprechung des EuGH analysieren – der nämlich ein guter Kenner des deutschen Rechtes ist, dieses möglicherweise sogar besser kennt, als manch anderer. Wir haben das beim Europäischen Stabilitätsmechanismus erlebt. Wir haben das erlebt in arbeitsrechtlichen Fällen, wie sehr das Bundesverfassungsgericht die Rechtsprechung des EGMR und des EuGH miteinbezieht. Deshalb – wenn Sie mich so fragen – mein Petitum: Warten wir doch am besten einfach ab, was das Bundesverfassungsgericht sagt. Daraus können wir vielleicht Schlüsse ziehen. Das ist schlicht und ergreifend nicht abzusehen. Das ist, wie Sie es gesagt haben, ganz schwierig. Die deutsche Regelung – das habe ich, glaube ich, auch geschrieben – ist aus meiner Sicht ein wirklich gelungener Ausgleich in dem Rahmen, der verfassungsrechtlich und europarechtlich vorgegeben ist. Wie das am Ende ausgeht? Ich bitte um Nachsicht – das wäre für

mich unseriös, solche Prognosen abzugeben. Das erwarten Sie hoffentlich auch nicht von mir. Aber ich habe aus der Sicht der Praxis darauf hingewiesen, wo momentan die kleine Lücke ist, hinsichtlich der man etwas tun sollte: die retrograden Standortdaten. Und das Zweite wäre der Punkt, dass man abwartet, was das Bundesverfassungsgericht macht und auf dieser Grundlage weiter überlegt. Ich bin mir sicher, dass da die Fragen des Europarechts eine große Rolle spielen werden. Vielen Dank.

Der **Vorsitzende:** Danke, Herr Köhler. Nun bitte Frau Kurz mit drei Antworten.

SVe **Dr. Constanze Kurz:** Ich will nur ganz kurz auf die Frage zur Pressemitteilung des Bundeskriminalamts bezüglich der Notwendigkeit der Vorratsdatenspeicherung eingehen. Dazu könnte man zwar eine Menge sagen. Das will ich aber mit Blick auf die vorangeschrittene Zeit nicht im Detail tun. Ich möchte aber darauf hinweisen, dass die Analyse von Netzpolitik.org ergibt, dass das Bundeskriminalamt seinen eigenen Daten widerspricht, dass das Bundeskriminalamt Einzelfälle herausnimmt, die bereits widerlegt sind. Ich halte es für eine ausgesprochen unredliche Pressearbeit einer angesehenen Behörde. Sie können das gern im Einzelnen nachlesen. Einer unserer Redakteure hat es mal auseinander genommen. Es ist für mich ein neuer Tiefpunkt, dass sich eine Behörde, die Verbrecher ergreifen soll, mit falschen Zahlen in einen politischen Diskurs einmischt. Das finde ich unerhört. Ich denke, die Behörde sollte das korrigieren, denn es ist belegbar und auch ziemlich gut auseinander genommen. Ich kann es aber nicht im Einzelnen darlegen. Ich bitte Sie jedoch, es zu lesen und wahrzunehmen. Ich darf auch daran erinnern – ich will mir das Wort nicht zu Eigen machen –, dass es hier um Bilder und Filme geht, die den Missbrauch von Kindern zeigen. Auch die Art, wie es dargestellt ist, mit diesem doch sehr emotionalisierenden Bild. Aber lesen Sie es nach. Das würde ich Ihnen sehr empfehlen. Zu der Frage der Grundrechte: Ich glaube, Herr Professor Cole hat es schon sehr deutlich gemacht. Man muss sich natürlich nicht dafür rechtfertigen, wenn man ein Grundrecht – und die informationelle Selbstbestimmung ist ein Grundrecht – wahrnehmen möchte. Es muss kein Schaden eintreten, auch kein konkreter, sondern der Gesetzgeber muss begründen, warum er dieses Grundrecht beschneiden will. Die Verdrehung, die Sie zweimal in Ihren Fragen bringen, finde ich bemerkenswert. Der Preis ist aus meiner Sicht hoch. Der ist deshalb hoch, weil wir bereits vor zehn Jahren in Karlsruhe vor der Frage standen, welche anderen anlasslosen Datenspeicherungen folgen werden, wenn wir diese anlasslose Datenspeicherung zulassen. Wir hatten mittlerweile eine Menge. Ich darf daran erinnern, dass unsere Körperdaten, also Biometrie-Daten, etwa das Gesicht und Fingerabdrücke, bereits in hohem Maße anlasslos festgehalten werden und wir darauf automatisierte Zugriffe haben. Wir haben auch das Festhalten der Flugdaten. Also da zieht so in gewisser Weise die Digitalisierung auf den Einzelnen zu. Und aus meiner technischen Sicht besteht überhaupt kein Zweifel, dass dieses Zusammenziehen sehr viel enger wird. Ich trage heute schon mehrere elektronische Geräte permanent bei mir. Und sie werden natürlich auch an unsere Körper wachsen und das haben wir im Prinzip auch schon vor zehn Jahren angebracht. Ich denke, wir müssen als eine freiheitliche Demokratie auch ein gewisses Vorbild sein. Ich darf daran erinnern, was mit genau diesen Telekommunikationsmetadaten in repressiven Staaten, wie etwa China, gemacht wird, mit denselben Techniken übrigens. Und ich möchte noch einmal darauf hinweisen, dass die Aussage falsch ist und durch Wiederholungen nicht besser wird, dass die Daten, die technisch bei den Providern anfallen, dieselben seien, wie die, die bei der Vorratsdatenspeicherung anfallen. Das können Sie auch gerne bei der Bundesnetzagentur, die ja die Anforderungen für die Datensicherheit festhält, noch einmal nachlesen. Die häufige Wiederholung macht das nicht wahrer. Und der Unterschied ist ja vor allen Dingen, dass bei den Vorratsdatenspeicherungsdaten in der Regel vorgesehen ist, dass man auf sie zugreifen kann, indem man die Schnittstellen baut. Und dass sehr viele kommerzielle Anbieter diese Daten gar nicht selbst speichern, sondern das als Dienstleistungsauftrag an Dritte weitergeben. Wofür die Bundesnetzagentur auch sehr konkrete Regeln gemacht hat, um sich zu schützen. Ich glaube, dass diese Trendwende, die in dem Bürgerrechtestärkungsgesetz enthalten ist, enorm wichtig für eine digitale Zukunft wäre, in die wir

ja gehen werden. Sonst werden wir sehr viel mehr andere anlasslose Datenspeicherungen haben.

Ein letztes Wort noch zu Ihrer Frage. Sie sagten, man müsse das ja verstehen, dass die Praktiker diesen Ermittlungsansatz benötigen. Und dass die Praktiker ansonsten „blank“ seien. Das ist natürlich ein hanebüchenes Argument angesichts der Tatsache, dass heute sehr viel mehr digitalisierte Daten vorliegen. Es besteht ein ganz anderer Ermittlungsansatz, als der, den wir vor 15 Jahren hatten, als wir nicht unsere gesamte Kommunikation – sozusagen unser Leben – digital organisiert haben. Sie haben ganz andere Ansätze, die es früher so nicht gab. Und es gibt sehr wenige Ermittler, die sagen, dass sie „blank“ wären, wenn sie keine Vorratsdatenspeicherung mehr hätten. Ich will noch einmal darauf zurückkommen, was ich vorhin ausgeführt habe. Selbstverständlich bin ich der Meinung, dass man Telekommunikationsdaten für Ermittlungen nutzen sollte, und zwar in effizienter Weise. Aber man sollte nicht die gesamte Bevölkerung dafür sozusagen in Mithaft nehmen. Und ein letztes Wort zur Evidenz: Ich glaube, Sie waren das, die sagten: „Wie sollen wir denn belegen, was wir nicht belegen können, weil die Vorratsdatenspeicherung ja gar nicht durchgeführt wird?“ Zum einen haben wir eine 200-seitige wissenschaftliche Studie des Max-Planck-Instituts, die sich immer noch zu lesen lohnt. Zum anderen haben wir sehr wohl einige Länder in Europa, die mehrere Jahre lang die Vorratsdatenspeicherung durchgeführt haben und auch Daten erhoben haben. Und ich darf Sie daran erinnern, dass vonseiten der Europäischen Union diese Daten auch abgefragt wurden. Man hat also die Länder um die Übermittlung der Ergebnisse gebeten, um zu schauen, ob es tatsächlich zu einer Verbesserung der Aufklärung kommt. Und jetzt raten Sie, was das Ergebnis war! Es heißt, wir haben sehr wohl Evidenz. Wir müssen sie nur mal zur Kenntnis nehmen. Es ist nicht so, dass wir Verbrechen nicht aufklären könnten, wenn wir keine Vorratsdatenspeicherung haben. Wir haben dafür auch praktische Daten. Wir haben sie zwar nicht aus Deutschland, aber so unterschiedlich sind die europäischen Nationalstaaten auch nicht.

Der **Vorsitzende:** Frau Kurz, vielen Dank. Frau Sandkuhl mit zwei Antworten. Herr Müller und Herr Reusch hatten Fragen an Sie gerichtet.

SVe **Dr. Heide Sandkuhl:** Gleich mal am Ende beginnend, in Ergänzung zu dem, was Frau Dr. Kurz gerade ausgeführt hat, darf ich vielleicht noch einmal daran erinnern, dass gerade nach der Rechtsprechung des Bundesverfassungsgerichts bereits die Speicherung der Daten „einen irreversiblen Eingriff in das Grundrecht aus Art. 10 Abs. 1 Grundgesetz“ darstellt. Und ich darf vielleicht auch noch einmal daran erinnern, was eigentlich eine anlasslose Speicherung bedeutet. Da werden Daten von Menschen gespeichert, die nicht den geringsten Anlass gegeben haben, oder überhaupt nicht im Verdacht stehen, eine Straftat begangen zu haben oder irgendwie eine konkrete Gefahr verursacht zu haben. Das ist die Ausgangssituation. Dann möchte ich noch einmal an den auch vom Bundesverfassungsgericht in vergangenen Entscheidungen angesprochenen Gedanken der Prozeduralisierung erinnern. Mit anderen Worten: Auch den Gesetzgeber trifft im Gesetzgebungsverfahren eine bestimmte Darlegungslast, nach der er zu erläutern hat, warum er eine bestimmte Maßnahme, die er gesetzlich geregelt haben will, braucht. Das ist auch ein Grundrechtsschutz durch Verfahren. Da brauch ich jetzt nicht wiederholen, was Frau Dr. Kurz und Herr Professor Cole gesagt haben, aber das darf nicht verdreht werden. Das ist ein ganz massiver grundrechtlicher Eingriff. Und wenn die dafür erforderliche Rechtstatsache fehlt, dann bedeutet das nicht, dass der Grundrechtseingriff trotzdem gerechtfertigt ist. Also daran will ich nur erinnern, weil Sie sagten, Sie ärgerten sich, dass diejenigen immer kommen und das behaupten – das sei ja schon denklogisch, das wäre überhaupt nicht schlüssig. Dann darf ich mal an die Prozeduralisierung erinnern. Ich meine: Ist das zu viel verlangt, bei einem so massiven Grundrechtseingriff auch Rechtstatsachen zu verlangen? Und wenn ich das höre, was Frau Dr. Kurz gerade ausgeführt hat – Sie haben verwiesen auf Netzpolitik.org, wo nachzulesen ist, wie da mit den Fällen umgegangen wird –, dann denke ich, dass dem nichts hinzuzufügen ist.

Dann wurde ich als Organ der Rechtspflege angesprochen. Darauf will ich auch gerne eingehen. Zunächst muss ich die von Ihnen geschilderte Chronologie ein wenig korrigieren. 2014: EuGH-Urteil, in dem die Richtlinie zur Vorratsdatenspeicherung gekippt, nämlich für

nichtig und ungültig erklärt wurde. Damit hatte sich das Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland erledigt und es bestand keine Verpflichtung für die Bundesrepublik Deutschland, Regelungen zur Vorratsdatenspeicherung einzuführen. Dennoch tat es die Bundesrepublik Deutschland. Und das war deswegen erstaunlich, weil der damalige Bundesminister für Justiz noch erklärt hatte, dass eine anlasslose Speicherung von Daten rechtswidrig sei. Gleichwohl wurde sie im Jahr 2015 eingeführt. Und dann erging im Jahr 2016 diese Entscheidung vom EuGH, die hier schon vielerorts angesprochen wurde. Wenn ich mich nach dieser Entscheidung richte, ist die anlasslose Speicherung rechtswidrig. Da kann ich mich nur wiederholen. Insofern als Antwort auf Ihre Frage nach dem Recht der Europäischen Union: Diese Speicherung ist unionsrechtswidrig. Deswegen darf sie hier nicht erfolgen.

(Unverständlicher Zwischenruf)

Ja, aber was ist das für eine Argumentation? So können Sie doch nicht argumentieren!

Der **Vorsitzende:** Frau Sandkuhl, vielen Dank. Herr Wollenschläger bitte mit der Beantwortung zweier Fragen von Frau Winkelmeier-Becker.

SV **Prof. Dr. Ferdinand Wollenschläger:** Vielen Dank. Vielleicht noch einmal um die Grundfrage, die der Frage von Frau Winkelmeier-Becker zugrunde liegt, in den Raum zu stellen: Letztlich geht es um eine Abwägung des Grundrechts auf informationelle Selbstbestimmung auf der einen Seite mit den staatlichen Schutzpflichten – rechtsstaatlichen, grundrechtlichen Schutzpflichten – auf der anderen Seite. Und dass insoweit viele Antworten denkbar sind, hat die heutige Diskussion gezeigt. Das zeigen aber natürlich auch die Kontrastierungen der Rechtsprechung des Bundesverfassungsgerichts einerseits, das ja insoweit 2010 keine der vom EuGH verbalisierten Bedenken geteilt hat, sowie die Rechtsprechung des EuGH andererseits. Vor diesem Hintergrund kann der deutsche Gesetzgeber oder auch jeder andere Grundrechtsinterpret ohne Weiteres zum Ergebnis kommen, dass auch die anlasslose allgemeine Verkehrsdatenspeicherung unionsrechtskonform ist, ebenso wie man natürlich zum gegenteiligen Ergebnis kommen kann. Die Frage, die für Sie als Gesetzgeber jetzt relevant ist, lautet: Sind sie europarechtlich aufgrund dieser Rechtsprechung verpflichtet, das deutsche Gesetz zu modifizieren? Und da muss man –das ist jetzt auch in der vorherigen Antwort nicht ganz deutlich zum Ausdruck gekommen, der Herr Cole hat es aber differenziert dargestellt – zwei Fragen unterscheiden. Nämlich einmal die Frage, welche Regelungen konkret beanstandet wurden. Das ist letztlich eine Abwägung, in die natürlich alle Gesichtspunkte, die die Eingriffsschärfe, aber natürlich auch die Eingriffsintensität mildern, einzustellen sind. Und da ist nach wie vor festzuhalten, dass die deutsche Regelung deutlich grundrechtsschonender als die beanstandeten Regelungen ausgefallen ist. Frau Winkelmeier-Becker, Sie hatten mich gebeten, das noch einmal ganz kurz anzusprechen. Das tue ich gerne. In dem Urteil des EuGH wurde eine unterschiedslose und ausnahmslose sechsmonatige Vorratsdatenspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer in Bezug auf alle elektronischen Kommunikationsmittel beanstandet. Die deutsche Regelung bleibt natürlich in fast jedem dieser Merkmale dahinter zurück: Nach Datenart differenzierende Speicherungsdauer, keine Speicherung von Daten von Diensten der elektronischen Post, keine Speicherung von Verbindungen, die einer besonderen Vertraulichkeit unterliegen sowie eine Speicherfrist von vier bis maximal zehn Wochen, und nicht von sechs Monaten wie in dem beanstandeten Fall. Der Ehrlichkeit halber muss man natürlich auch erwähnen, dass das Urteil neben der Beanstandung der konkreten Regelung noch ein obiter dictum enthält, aus dem sich die Unionsgrundrechtswidrigkeit dieser allgemeinen anlasslosen Verkehrsdatenspeicherung ableiten lässt. Erster Punkt: Das obiter dictum besitzt keine verpflichtende Wirkung für den deutschen Gesetzgeber – es gehört nicht zum Tenor der Entscheidung. Zweiter Punkt: Selbst dieses obiter dictum, würde ich sagen, lässt noch eine gewisse Restunschärfe. Es heißt dort „hingegen untersagt das Unionsrecht nicht“ und es ist nicht wie folgt formuliert: „hingegen ist eine Telekommunikationsverbindungsdatenspeicherung nur dann zulässig, wenn 1. ..., 2. …, 3. …“. Also ist da auch sprachlich noch eine gewisse Restunschärfe vorhanden, abgesehen davon, dass es nur ein obiter dictum ist. Und das wird man auch

bedenken müssen. Daher habe ich gesagt, dass der deutsche Gesetzgeber sich nicht europarechtsfeindlich verhält, wenn er aufgrund einer natürlich zu vertretenden Abwägung mit den Gesichtspunkten, die ja heute alle zur Sprache gekommen sind, zu dem Ergebnis gelangt, dass er an der deutschen Regelung festhält bis sie eben konkret beanstandet wird, sei es vom Bundesverfassungsgericht, sei es vom EuGH. Und ich glaube, dass man das festhalten muss. Ich würde auch davor warnen – nachdem das vorhin geschehen ist –, dass man jetzt irgendwelche Teile aus diesem Urteil heranzieht und sagt, dass damit die deutsche Regelung nicht übereinstimmt, wie zum Beispiel in Bezug auf die Frage der Berufsgeheimnisträger. Insoweit ist die Sache ganz klar. Die Frage der Speicherung von Daten von Berufsgeheimnisträgern wird nicht im obiter dictum angesprochen, sondern sie findet sich im Rahmen der Beanstandung der schwedischen und englischen Regelung, sodass sich der EuGH zu der Frage, ob man diese Daten speichern darf, anders als das vorhin dargestellt wurde, nicht allgemein geäußert hat. In dem Urteil muss man unterscheiden, zwischen den Ausführungen vor der Randnummer 108 und den Ausführungen ab der Randnummer 108. Das ist ganz wichtig. Ein Punkt, der schon teilweise beantwortet wurde: Natürlich ging es um schwedische bzw. englische Regelungen. Der EuGH hat jedoch natürlich immer die ganze Europäische Union im Blick. Vielleicht noch etwas zum Thema des Missbrauchspotentials: Auch wenn ich da jetzt, was die Empirie betrifft, der falsche Ansprechpartner bin, besteht das in zweierlei Hinsicht. Natürlich einmal auf der Seite der Telekommunikationsunternehmen, weil dort diese Datenmasse gespeichert wird. Das ist das eine. Und das andere ist natürlich der Punkt, der jedenfalls mit Blick auf die deutsche Praxis kaum thematisiert wird, dass natürlich auch Strafverfolgungsbehörden beim Zugriff auf diese Daten missbräuchlich vorgehen können.

Letzter Punkt: Herr Cole, wir waren uns eigentlich in sehr Vielem einig. Bei einem Punkt würde ich widersprechen. Bei dieser Linie, die Sie hinsichtlich der EuGH-Rechtsprechung aufgemacht haben. Ich würde sagen, dass das Fluggastdaten-Urteil, das ja das letzte Urteil in dieser Linie war, in gewisser Weise zurückrudert, auch im Vergleich zum Schrems-Urteil. Weil der EuGH dort ja eigentlich nicht, wie man es vielleicht erwartet hätte, eine Vorratsdatenspeicherung für grundsätzlich unionsgrundrechtswidrig erklärt hat, sondern in dem Urteil für Passagierdaten entschieden hat, dass die Daten von jedem, der nach Kanada einreist – egal ob mit guten oder bösen Absichten – für den Aufenthalt in Kanada vorratsgespeichert werden dürfen. Das ist im Einklang mit den Unionsgrundrechten. Da kann man natürlich auch wieder diskutieren, welche Schlüsse daraus zu ziehen sind. Aber jedenfalls erachte ich diese Linie, die gezogen wurde, für nicht ganz so eindeutig. Das sollte man bedenken. Danke schön.

Der **Vorsitzende:** Danke, Herr Wollenschläger. Damit ist die zweite Frage- und Antwortrunde beendet. Die Anhörung dauert nun ziemlich genau zwei Stunden. Wenn das gewünscht ist, können wir natürlich auch noch eine dritte Frage- und Antwortrunde abhalten. Gibt es noch Fragesteller unter den anwesenden Abgeordneten? Ich sehe keine Fragesteller mehr. Möchten Sie noch etwas loswerden, aus der Mitte der Sachverständigen? Das ist auch nicht der Fall. Dann bedanke ich mich herzlich. Ich bitte noch einmal um Entschuldigung für den verzögerten Beginn. Ich denke, es war eine sehr erhellende Anhörung. Es gab ja auch konträre Ansichten, die hoffentlich im Gesetzgebungsverfahren dann auch Berücksichtigung finden. Ich wünsche Ihnen noch einen schönen Abend und eine schöne Woche. Vielen Dank, damit ist die Sitzung geschlossen.

Schluss der Sitzung: 18:19 Uhr

Stephan Brandner, MdB
Vorsitzender

Anlagen: Stellungnahmen der Sachverständigen

Professor Dr. Mark D. Cole
Medien- und Telekommunikationsrecht
Universität Luxemburg
4, rue Alphonse Weicker
L-2721 Luxemburg
T.: +352 46 66 44 6824
mark.cole@uni.lu
www.medialaw.lu

Wissenschaftlicher Direktor
Institut für Europäisches Medienrecht
Franz-Mai-Straße 6
D-66121 Saarbrücken
T.: +49/681/99275-11
m.cole@emr-sb.de
www.europaeisches-medienrecht.de

Sachverständigenanhörung

Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages

zu den Artikeln 1, 2, 3 und 6 (- Themenkomplex Vorratsdatenspeicherung -) des Entwurfs eines Gesetzes zur Stärkung der Bürgerrechte (Bürgerrechtestärkungs-Gesetz – BüStärG), BT-Drucksache 19/204

am Mittwoch, dem 13. Juni 2018, 15.00 Uhr in Berlin

Der vorgenannte Gesetzesentwurf hat in dem hier relevanten Auszug die Abschaffung der telekommunikationsbezogenen sog. Vorratsdatenspeicherung zum Ziel. Im Folgenden werden fünf Kernthesen vorgestellt, die einen Änderungsbedarf gegenüber der aktuellen Gesetzeslage bestätigen. Eine ausführlichere Erörterung der Thesen ist im Rahmen der Anhörung vorgesehen.

1. Die mitgliedstaatliche Regelung einer Vorratsdatenspeicherung unterfällt den Vorgaben des Europarechts und ist mit diesem in Einklang zu bringen.

2. Es existiert eine umfassende und konsistente Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH), die die Vorgaben der Europäischen Menschenrechtskonvention (EMRK) in ihrer Auslegung durch den Europäischen Gerichtshof für Menschenrechte (EGMR) intensiv einbezieht und weitreichende Vorgaben für Datenspeicherungsregelungen macht.

3. Die anlasslose und generelle Speicherung von Verkehrsdaten ist schon vom Ansatz her grundrechtlich problematisch. Jede Form solcher Speicherpflichten ist nur unter engen Voraussetzungen und als Ausnahme zur Regel überhaupt denkbar.

4. Die umfassenden Vorgaben der einschlägigen Rechtsprechung des EuGH sind nur schwer erfüllbar und jedenfalls nicht in Form eines allgemeinen Speicherregimes umsetzbar. Dies wird letztlich auch auf Ebene der Mitgliedstaaten im Rahmen der Verhandlungen in der EU um mögliche neue gemeinsame Instrumente deutlich.

5. Eine grundrechtsschonende und im Blick auf die divergierenden Ansätze auf mitgliedstaatlicher Ebene und den grenzüberschreitenden Wirtschaftraum, in dem sich die entsprechenden Unternehmen bewegen, gebotene einheitliche Herangehensweise spricht für die Abschaffung nationaler Vorratsdatenspeicherungsregelungen in der bisherigen Gestalt. Ob und wie eine harmonisierter Ansatz auf EU-Ebene verfolgt werden sollte, hängt maßgeblich davon ab, ob die Notwendigkeit des intensiven Grundrechtseingriffs durch entsprechende Erreichung legitimer Ziele belegt werden kann.

Stellungnahme

zum Entwurf eines Gesetzes zur Stärkung der Bürgerrechte (Bürgerrechtestärkungs-Gesetz – BüStärG)[1]

Verfasser: Richter am Bundesgerichtshof Marcus Köhler, Leipzig/Berlin

I. Vorbemerkung:

Der Verfasser ist Mitglied des 5. Strafsenats des Bundesgerichtshofs. Er war zuvor u. a. beim Generalbundesanwalt in Karlsruhe und der Generalstaatsanwaltschaft Frankfurt am Main tätig. Aufgrund des Schwerpunkts seiner beruflichen Tätigkeit im Straf- und Strafverfahrensrecht wird sich die Stellungnahme auf die mit der im Entwurf eines Gesetzes zur Stärkung der Bürgerrechte (BüStärGE) beabsichtigte Abschaffung der „Vorratsdatenspeicherung“ beschränken (Artikel 1 bis 3 des BüStärGE).

II. Inhalt und Ziel der Artikel 1 bis 3 des BüStärGE

Artikel 1 Nummer 2 des BüStärGE bestimmt die Aufhebung der §§ 113a bis 113g des Telekommunikationsgesetzes (TKG). Artikel 2 sieht im Wesentlichen vor, § 100g Absatz 2 und Absatz 3 Satz 2 Strafprozessordnung (StPO) ersatzlos zu streichen. Artikel 3 enthält Änderungen des Justizvergütungs- und entschädigungsgesetzes (JVEG).

Ziel des Gesetzentwurfs ist die „Abschaffung der verfassungswidrigen und europarechtswidrigen Vorratsdatenspeicherung“.[2] Der Gesetzentwurf beabsichtigt mithin, die durch das Gesetz vom 10. Dezember 2015 (BGBl I 2218) eingeführten Regelungen zur Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten zu streichen.

Zur Begründung führt der Entwurf zum einen aus, dass „staatliche Befugnisse zu einer anlasslosen Verarbeitung der Daten der Bürgerinnen und Bürger … abzulehnen“ seien. Zum anderen stützt er sich auf die Rechtsprechung des Bundesverfassungsgerichts (BVerfG) und des Europäischen Gerichtshofs (EuGH) sowie des Oberverwaltungsgerichts (OVG) Münster.[3]

Die Frage der Bedeutung von Verkehrsdaten für eine objektive und effektive Aufklärung schwerwiegender Straftaten erörtert der Entwurf nicht.

[1] BT-Drucksache 19/204
[2] BT-Drucksache 19/204, Seite 1
[3] BT-Drucksache 19/204, Seite 7

III. Das Konzept der „Vorratsdatenspeicherung“ im geltenden Recht

Nach § 113b Absatz 1 TKG sind Telekommunikationsanbieter im Sinne des § 113b TKG verpflichtet, sogenannte Standortdaten für vier Wochen und die übrigen Verkehrsdaten für zehn Wochen zu speichern. Die auf dieser rechtlichen Grundlage gespeicherten Verkehrsdaten dürfen nach § 100g Absatz 2 Satz 1 StPO nur zur Aufklärung und Verfolgung besonders schwerer, in § 100g Absatz 2 Satz 2 abschließend aufgeführter Straftaten erhoben werden. Dabei genügt nicht die abstrakte Schwere der Tat; die Straftat muss vielmehr auch im konkreten Einzelfall besonders schwer wiegen (§ 100g Absatz 2 Satz 1 StPO). Die Erhebung bedarf der gerichtlichen Anordnung, die mit einer Begründung zu versehen ist (§ 101a Absatz 1 Satz 1 in Verbindung mit § 100e Absatz 1 Satz 1, Absatz 4 StPO). Eine Eilkompetenz der Staatsanwaltschaft gibt es nicht. Die Erhebung und Verwertung der Daten durch Strafverfolgungsbehörden ist mithin nur unter engen Voraussetzungen zulässig. Die Hürden sind sogar höher als die für die Überwachung von Telekommunikationsinhalten nach § 100a StPO.

Anders als dies die Entwurfsbegründung nahe legt[4], stellt die „Vorratsdatenspeicherung“ im geltenden Recht mithin keine „staatliche Befugnis zu einer anlasslosen Verarbeitung von Daten“ dar. Ihr liegt vielmehr ein zweistufiges Konzept zugrunde, das Speicherung und „Verarbeitung“ von Verkehrsdaten strikt trennt. Die Speicherung findet nach § 113b TKG (erste Stufe) bei einem Telekommunikationsanbieter statt; einen besonderen Anlass bedarf es dazu nicht. Nur die „Verarbeitung“ (= Erhebung und Verwertung der gespeicherten Verkehrsdaten) findet nach § 100g Absatz 2 StPO (zweite Stufe) in der staatlichen Sphäre statt; sie bedarf eines konkreten Tatverdachts für eine besonders schwerwiegende Straftat und steht unter dem Richtervorbehalt.

IV. Die „Vorratsdatenspeicherung“ im Lichte der Rechtsprechung

1. Rechtsprechung des BVerfG

Die in der Entwurfsbegründung in Bezug genommene Entscheidung des BVerfG vom 2. März 2010 (1 BvR 256/08; 1 BvR 263/08; 1 BvR 586/08)[5] betrifft - worauf die Entwurfsverfasser zutreffend hinweisen[6] – ein früheres Regelungskonzept der „Vorratsdatenspeicherung“. Sie kann allerdings nur schwerlich gegen die Verfassungskonformität der nun geltenden Regelungen ins Feld gezogen werden. Denn die früheren Regelungen unterscheiden sich wesentlich von den Regelungen im geltenden Recht. So sah das frühere Recht eine deutlich längere und unterschiedslose Speicherung von sechs Monaten vor (§ 113a Absatz 1 TKG a. F.); im geltenden Recht ist die Speicherung auf zehn

[4] Vgl. BT-Drucksache 19/204, Seite 7, letzter Satz im ersten Absatz und erster Satz im zweiten Absatz
[5] Der angegebenen Fundstelle (BVerfGE 126, 260) scheint ein Schreibversehen zugrunde zu liegen.
[6] BT-Drucksache 19/204, Seite 7, dritter Absatz

Wochen beschränkt, für Standortdaten ist die Speicherung sogar nur für vier Wochen zulässig (§ 113b Absatz 1 TKG). Zudem war die Erhebung der Verkehrsdaten schon bei erheblichen Straftaten zulässig (§ 100g Absatz 1 StPO a. F.); im geltenden Recht bedarf es hingegen den Verdacht für eine auch im Einzelfall besonders schwerwiegende Straftat (§ 100g Absatz 2 StPO). Vor allen Dingen hat das BVerfG die Regelung einer „Vorratsdatenspeicherung“ nicht an sich für verfassungswidrig erachtet, sondern lediglich deren damalige konkrete Ausgestaltung (BVerfG aaO Rn. 208 ff.).

Die Vorgaben für eine verfassungskonforme Regelung (BVerfG aaO Rn. 220 ff.) hat der Gesetzgeber bei der Neuregelung im Jahr 2015 berücksichtigt. Eilanträge gegen die Neuregelung hat das BVerfG - auch unter Berücksichtigung neuerer Entscheidungen des EuGH - zurückgewiesen (1 BvQ 42/15; 1 BvR 3156/15; 1BvR 229/16, 1 BvR 141/16). Die Entscheidung des BVerfG in der Hauptsache steht noch aus.

2. Rechtsprechung des EuGH

Die im Entwurf zitierten Entscheidungen des EuGH können nicht ohne weiteres als Beleg für die Unvereinbarkeit der Neuregelung der „Vorratsdatenspeicherung“ mit Unionsrecht herangezogen werden. Denn die Entscheidungen betreffen – worauf die Entwurfsverfasser zu Recht hinweisen[7] - nicht das deutsche Recht.

Die Entscheidung des OVG Münster, wonach die Neuregelungen nicht mit dem Unionsrecht vereinbar seien (Beschluss vom 22. Juni 20017 – 13 B 238/17), ist schon mit Blick auf die Vorläufigkeit der Entscheidung nur bedingt als Entscheidungsmaßstab für den Gesetzgeber geeignet – zumal das Verwaltungsgericht (VG) Köln in der Ausgangsentscheidung mit einer ausführlichen Begründung zum gegenteiligen Ergebnis gelangt ist (VG Köln, Beschluss vom 25. Januar 2017 – 9 L 1009/16).

V. Beweisbedeutung von Verkehrsdaten im Strafverfahren

Der Bedeutung von Verkehrsdaten für die Aufklärung von Straftaten war Gegenstand der öffentlichen Anhörung des Ausschuss für Recht und Verbraucherschutz im Rahmen der parlamentarischen Beratungen über das Gesetz zur Einführung einer Pflicht zur Speicherung und Höchstspeicherfrist für Verkehrsdaten am 21. September 2015. Zur hohen beweisrechtlichen Bedeutung von Verkehrsdaten – wenn nicht gar ihrer Unverzichtbarkeit - für die Aufklärung schwerer Straftaten hat der damalige Sachverständige Dr. Nikolaus Berger ein umfassendes Gutachten mit konkreten Einzelfällen vorgelegt. Seine Bewertung entspricht den praktischen Erfahrungen des Verfassers; das Gutachten ist daher als Anlage beigefügt.

VI. Erforderlichkeit gesetzgeberischen Handelns

[7] BT-Drucksache 19/204, Seite 7

Die vom BürStärGE betroffenen Regelungen über die „Vorratsdatenspeicherung“ liegen dem Bundesverfassungsgericht zur Überprüfung ihrer Vereinbarkeit mit dem Grundgesetz vor. Es ist davon auszugehen, dass das BVerfG in der Entscheidung richtungsweisende Aussagen zur Erhebung von Verkehrsdaten für die Strafverfolgung treffen wird. Es erscheint daher sinnvoll, die abschließende Entscheidung des BVerfG abzuwarten. Eine Beeinträchtigung individueller Freiheitsrechte ist nicht zu besorgen, da – worauf der Entwurf zutreffend hinweist[8] – die Netzagentur bis auf weiteres von Maßnahmen zur Durchsetzung der Speicherpflicht nach § 113b Absatz 1 TKG absieht.

VII. Fazit

1. Die Erhebung und Verwertung von Verkehrsdaten ist für eine effektive rechtsstaatliche Verfolgung und Aufklärung schwerer Straftaten notwendig. Da die wirksame Aufklärung gerade schwerer Straftaten aber einen wesentlichen Auftrag des rechtsstaatlichen Gemeinwesens darstellt (vgl. BVerfGE 77, 65, 76; 109, 279, 336) und die Feststellung des wahren historischen Sachverhalts eine Voraussetzung von materieller Strafrechtsgerechtigkeit ist (vgl. BVerfGE 33, 367, 383), ist es ein Gebot des Rechtsstaats, die Erhebung von Verkehrsdaten im Strafverfahren im verfassungs- und unionsrechtlich zulässigen Rahmen zu ermöglichen.

2. Eine eklatante, offensichtliche Unvereinbarkeit der geltenden Regelungen über die „Vorratsdatenspeicherung“ mit Verfassungs- oder Unionsrecht ist nicht ersichtlich. Vielmehr stellt die Neuregelung aus dem Jahr 2015 einen (weitgehend) gelungenen Ausgleich zwischen den individuellen Freiheitsrechten und dem verfassungsrechtlichen Gebot einer effektiven Strafverfolgung dar, der die Vorgaben des Bundesverfassungsgerichts für eine verfassungskonforme „Vorratsdatenspeicherung“ (vgl. BVerfG aaO) restriktiv umsetzt.

3. Eine Notwendigkeit für gesetzgeberisches Handeln besteht derzeit nicht, da eine Beeinträchtigung individueller Freiheitsrechte bis auf weiteres nicht zu besorgen ist. Insofern erscheint es sinnvoll, die anstehende Entscheidung des BVerfG abzuwarten, um auf deren Grundlage eine gegebenenfalls erforderliche Neubewertung vornehmen zu können.

[8] BT-Drucksache 19/204, Seite 7

Stellungnahme zum Bürgerrechtestärkungs-Gesetz – BuStärG unter dem Aspekt der geplanten Abschaffung der Vorratsdatenspeicherung

Für die Anhörungssitzung des Ausschusses für Recht und Verbraucherschutz vom 13. Juni 2018

Die Vorratsdatenspeicherung ist ein heiß umstrittenes Thema. Entsprechend viele Änderungen mit Einfluss auf die Strafverfolgung hat es in den letzten Jahren gegeben.

Die **Richtlinie 2006/24/EG** über die **Vorratsdatenspeicherung** vom 15. März 2006**,** mit der alle EU-Mitgliedstaaten zur Einführung einer Vorratsdatenspeicherung von sechs Monaten bis zwei Jahren verpflichtet wurden, setzte Deutschland mit dem Gesetz zur Neuregelung der Telekommunikationsüberwachung vom 21.12.2007 um. Die Strafverfolgungsbehörden konnten über §100 g StPO Zugriff auf die Daten nehmen.

Bei der ersten Vorratsdatenspeicherung wurde noch nicht zwischen Daten, die der Diensteanbieter zur Leistungserbringung nach § 96 TKG speichern darf und solchen, die er zum Zwecke der Strafverfolgung nach § 113b TKG (damals: § 113a TKG) speichern muss, unterschieden.

Das **Bundesverfassungsgericht** beschloss im Wege der einstweiligen Anordnung vom **11.3.*2008*** (1 BvR 256/08) bis zur Entscheidung in der Hauptsache die nur eingeschränkte Anwendung, nämlich nur bei besonders schweren Straftaten.

Das B**undesverfassungsgericht** entschied am **2.3.2010** (BVerfGE 125, 260), dass die §§ 113a, 113b TKG in der Fassung vom 21.12.2007 und § 100g StPO, soweit danach Verkehrsdaten erhoben werden dürfen – sechsmonatige anlasslose Speicherung – gegen Art. 10 GG, das Brief-, Post- und Fernmeldegeheimnis, verstoßen. Eine maximal sechsmonatige Speicherung sei aber nicht von vornherein unzulässig. Es seien im Rahmen der Verhältnismäßigkeit die Datensicherheit, der Umfang der Datenverwendung sowie Transparenz und Rechtsschutz zu beachten. Voraussetzung für den Abruf von Daten zu Zwecken der Strafverfolgung sei ein abschließender Kreis der umfassten Tatbestände, dass die Straftat im Einzelfall schwer wiege und die Datenverwendung verhältnismäßig sei.

In seiner Entscheidung vom **8.4.2014**, C-293/12, C-594/12 (EuGH NJW 2014, 2169) hat der **Europäische Gerichtshof** die Ungültigkeit der Richtlinie 2006/24/EG zur Vorratsdatenspeicherung, die eine Speicherungsfrist von 6 Monaten bis 2 Jahren vorsah, festgestellt. Denn es gebe keine Einschränkung auf das zur Erreichung des Zieles (öffentliche Sicherheit und Terrorismusbekämpfung) absolut Notwendige. Der Entscheidung liegt keine grundsätzliche Absage an die Vorratsdatenspeicherung zugrunde.

Daraufhin kam es zum **Gesetz zur Einführung einer Speicherfrist und einer Höchstspeicherfrist von Verkehrsdaten vom 10.12.2015**. In § 100g StPO wurden Katalogtaten für Verkehrsdaten nach § 113b TKG, also Vorratsdaten, eingeführt. Verbindungsdaten nach § 113 b Abs. 1 und 2 TKG, z.B. Rufnummer, Datum und Uhrzeit, Internetprotokoll-Adressen und Anschluss- und Benutzerkennungen sollen 10 Wochen und Standortdaten nach § 114b Abs. 4 TKG, sog. Funkzellendaten, vier Wochen gespeichert werden. Der Anbieter kann aber Standortdaten zu Abrechnungszwecken bis zu sechs Monate speichern, § 97 Abs. 3 TKG.

Das **Bundesverfassungsgericht** hat am **8.6.2016** (1 BvQ 42/15 u. 1 BvR 229/16) den Erlass einstweiliger Anordnungen bezüglich des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10.10.2015 und §§ 100g, 101a, 100b StPO abgelehnt. Es entstehe kein schwerwiegender und irreparabler Nachteil durch die Datenspeicherung. Das BVerfG dürfe von seiner Befugnis, den Vollzug eines in Kraft getretenen Gesetzes auszusetzen, nur mit größter

Zurückhaltung Gebrauch machen, da der Erlass einer solchen einstweiligen Anordnung stets ein erheblicher Eingriff in die Gestaltungsfreiheit des Gesetzgebers sei.

Der **Europäische Gerichtshof** hat auf die Vorlage von Großbritannien und Schweden mit Urteil vom **21.12.2016** (C-203/15 und C-698/15) entschieden, dass die von der Richtlinie 2002/58/EG vom 12.7.2002 in der geänderten Fassung der Richtlinie 2009/136/EG vom 25.11.2009 vorgesehene anlasslose Vorratsdatenspeicherung nicht mit den Europäischen Grundrechten vereinbar ist. Eine Verwendung von Vorratsdaten sei nur zur Bekämpfung schwerer Straftaten legitim. Das europäische Recht stehe einer nationalen Regelung entgegen, die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsehe. Es steht einer nationalen Regelung entgegen, die den Schutz und die Sicherheit der Verkehrs- und Standortdaten, insbesondere den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten zum Gegenstand hat, ohne im Rahmen der Bekämpfung von Straftaten diesen Zugang ausschließlich auf die Zwecke einer Bekämpfung schwerer Straftaten zu beschränken, ohne den Zugang einer vorherigen Kontrolle durch ein Gericht oder einer unabhängigen Verwaltungsbehörde zu unterwerfen und ohne vorzusehen, dass die betreffenden im Gebiet der Union auf Vorrat zu speichern sind.

Eine Speicherung sei möglich, sofern die dabei erhobenen Daten in Europa verbleiben und zuvor eine richterliche Genehmigung eingeholt werde.

Das **OVG Münster** hat am **22.6.2017** – 13 B 238/17 -beschlossen, dass die Speicherungspflicht nach § 113a Abs. 1 i.V.m. § 113b Abs. 1 und 3 TKG insgesamt mit Unionsrecht nicht vereinbar sei und das IT-Unternehmen jedenfalls in seiner durch Art. 16 der Charta der Grundrecht der Europäischen Union geschützten unternehmerischen Freiheit verletzt und hat festgestellt, dass bis zum rechtskräftigen Abschluss des Hauptsacheverfahrens des VG Köln keine Speicherpflicht bestehe.

Bis zum 29.7.2017 wurden Verkehrsdaten nach § 100g Abs. 1 StPO a.F. i.V.m. § 12 StPOEG und § 96 Abs .1 S. 1 Nr. 1 TKG sowohl für Straftaten von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 StPO bezeichnete Straftat (= Katalog für Taten, für welche eine Telefonüberwachung beantragt werden kann), als auch für eine mittels Telekommunikation begangene Straftat eingeholt, wenn sie für die Erforschung oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich waren. Bei einer Maßnahme mittels Telekommunikation musste die Maßnahme zu o.g. Zwecken überdies auf andere Weise aussichtslos sein, und die Erhebung der Daten muss in einem angemessenen Verhältnis zur Bedeutung der Sache stehen.

Ab dem 30.7.2017 erfolgt eine Differenzierung wie folgt:

Nach § 100g Abs. 1 StPO können Verkehrsdaten und Standortdaten für die Zukunft oder in Echtzeit nur bei einer mittels Telekommunikation begangenen Straftat eingeholt werden.

Nach § 100g Abs. 2 StPO ist die Einholung von Verkehrsdaten nach § 113b TKG (= Vorratsdaten) möglich

- bei Standortdaten für die Zukunft oder in Echtzeit bei einer Straftat von auch im Einzelfall erheblicher Bedeutung
- bei allen Standortdaten für die Vergangenheit bei besonders schweren Taten = Katalogtaten.

Weiter müssen die Verkehrsdaten zur Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos sein. Die

Erhebung der Daten muss in einem angemessenen Verhältnis zur Bedeutung der Sache stehen. Die Tat muss im Einzelfall schwer wiegen.

Nach § 100g Abs. 3 StPO können Funkzellendaten nur bei besonders schweren Taten = Katalogtaten abgefragt werden. Überdies muss es sich um eine Straftat von auch im Einzelfall erheblicher Bedeutung handeln. Die Erhebung der Daten muss in angemessenem Verhältnis zur Bedeutung der Sache stehen. Die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten wäre auf andere Weise wesentlich erschwert oder aussichtslos. Hinsichtlich Vorratsdaten nach § 113b TKG gelten dieselben Voraussetzungen wie bei § 100g Abs. 2 StPO.

Nach § 113b Abs. 6 TKG dürfen Daten 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 besonderen Verschwiegenheitsverpflichtungen unterliegen, nicht gespeichert werden. Bei weiteren Berufsgeheimnisträgern wie Rechtsanwalt oder Verteidiger greift das Verbot der Erhebung nach § 100 g Abs. 4 StPO.

Wie kommt es zu der unterschiedlichen Handhabung?

Bis zum 29.7.2017 konnten Staatsanwaltschaft und Gerichte sich auf die **Übergangsnorm des § 12 StPOEG** berufen. Zwar gab es das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherpflicht für Verkehrsdaten vom 10.12.2015, gültig ab dem 18.12.2015. Die Speicherverpflichtung galt nach § 150 Abs. 13 TKG aber erst spätestens ab dem 1.7.2017. Da es mangels Speicherfrist noch keine gespeicherten Daten gab, konnte vorübergehend auf Verkehrsdaten nach § 96 Abs. 1 TKG zurückgegriffen werden.

Seitdem diese Übergangsregelung ausgelaufen ist, gibt es z.B. keine retrograden Verbindungsdaten mehr für

- Geldfälschung, § 146 StGB
- Sexuellen Missbrauch von Kindern ohne Eindringen in den Körper, § 176 StGB
- Vergewaltigung durch Alleintäter, § 177 Abs. 6 S. 2 Nr. 2 StGB
- einfachen oder besonders schweren Diebstahl („Einbruch“), §§ 242, 243 StGB
- Raub, § 249 StGB
- Erpressung, § 253 StGB
- Betrug oder Computerbetrug, § 263 (a) StGB
- Urkundenfälschung, § 267 StGB.

Es kommt zu einem Auseinanderfallen von Katalogtaten nach § 100a StPO (Telefonüberwachung) und § 100g StPO (retrograde Standortdaten). Letztere sollen nämlich die Erstellung eines Bewegungsprofils ermöglichen. Anders als bei der Telefonüberwachung gibt es nach § 101a Abs. 1 StPO auch keine Eilkompetenz der Staatsanwaltschaft mehr bei Gefahr im Verzug.

Es ist beispielsweise eine Telefonüberwachung möglich, nicht aber die Einholung von retrograden Standortdaten bei

- Geldfälschung
- Fälschung von Kredit-/Scheckkarten oder Schecks
- Menschenhandel
- Bandendiebstahl
- gewerbsmäßige Hehlerei, Bandenhehlerei

- einfacher Geldwäsche
- gewerbs- und/oder bandenmäßigem (Computer-)Betrug
- gewerbs- und/oder bandenmäßiger Urkundenfälschung
- einfachem Raub oder Erpressung.

Dabei geht es bei der Telefonüberwachung um Inhaltsdaten, während es bei den Vorratsdaten „nur" um Verkehrsdaten geht, also im Wesentlichen Rufnummern, IMSI-und IMEI-Nummern, IP-Adresse, Anfang und Ende der Kommunikation sowie Standortdaten.

Moderne Formen der Tatbegehung im Bereich der Cyberkriminalität wie Carding, Skimming, Phishing, DDOS-Angriffe und Drohung damit sowie Ransomware-Angriffe (außer bei Gewerbsmäßigkeit und/oder bandenmäßiger Begehung) oder verbreitete professionelle Betrugstaten wie die sog. Enkeltrickmasche werden außer acht gelassen.

Es gab aber auch deswegen keine retrograde Daten aufgrund der Vorratsdatenspeicherung mehr, weil zwar seit dem 30.7.2017 die Speicherung gesetzlich verpflichtend war, aber grundsätzlich nicht mehr gespeichert wurde. Das hat folgenden Hintergrund:

Die **Bundesnetzagentur** hat aufgrund der Entscheidung des OVG Münster am **28.6.2017** erklärt, bis zum rechtkräftigen Abschluss eines Hauptsacheverfahrens von Anordnungen und sonstigen Maßnahmen zur Durchsetzung der in § 113b TKG geregelten Speicherverpflichtungen gegenüber allen verpflichteten Unternehmen abzusehen. Bis dahin werden auch keine Bußgeldverfahren wegen einer nicht erfolgten Umsetzung gegen die verpflichteten Unternehmen eingeleitet.

Als neue Entwicklung wurde jedoch jüngst bekannt, dass am **26. April 2018** eine **Besprechung der Mobilfunkprovider, dreier Ministerien, der Sicherheitsbehörden und der Generalstaatanwaltschaft Stuttgart** stattgefunden hat. Die Provider Telefónica, Vodafone und Telekom haben sich nunmehr dazu bereit erklärt, retrograde Standortdaten über die für diesen Zweck eingerichtete „Elektronische Schnittstelle Behörden" in digitaler Form zu beauskunften. Es kann unter Berufung auf § 100g Abs. 1, Abs. 2 StPO i.V.m. § 96 TKG um Übermittlung der gemäß § 96 Abs. 1 TKG erhobenen Verkehrsdaten einschließlich zurückliegender Standortdaten gebeten werden. Die Deutsche Telekom wiederum erteilt nur bei Androhung eines Ordnungsgeldes Auskunft. Andere Abfragen werden unter Hinweis auf die Nichtverfügbarkeit der gemäß § 113b TKG zu speichernden Daten zurückgewiesen bzw. wird eine Nullauskunft erteilt.

Wie sieht ein Funkzellenbeschluss aus?

Er wird auch, wenn nicht überwiegend, bei noch nicht offen gelegten Verfahren beantragt. Er wird nach § 44 Abs .4 StPO und unter Zurückstellung der Benachrichtigung des Betroffenen für 12 Monate nach § 101a Abs .6, 101 Abs. 4 und 6 StPO für die drei Netzbetreiber Telekom Deutschland GmbH (D1), Vodafone D2 GmbH und die Telefónica Deutschland Holding AG (E2) eingeholt, grundsätzlich bis zuletzt noch nur zu den Verkehrsdaten – ohne Standortdaten -. Nach der Einigung vom 26.4.2018 wird sich die Auskunft in Zukunft auch wieder auf die retrograden Standortdaten beziehen. Der Tatvorwurf wird konkret und unter Auflistung der einschlägigen Paragraphen aufgelistet. Es wird ausgeführt, dass und warum es sich um eine Straftat von auch im Einzelfall erheblicher Bedeutung handelt, warum die Maßnahme geeignet, zweckdienlich, erforderlich, angemessen ist. So benutzen erfahrungsgemäß Teilnehmer arbeitsteilig ausgeführter Taten Mobilfunkendgeräte, um miteinander zu kommunizieren. Es liegt nahe, dass sie zumindest mit einem absichernden Mittäter in Tatortnähe über eine Telekommunikations- oder Datenverbindung in Kontakt stehen oder sich zumindest

Datenverbindungen durch mitgeführte Mobiltelefone im Rahmen automatischer Zugriffe von und auf Apps aufbauen und ein Vergleich zu weiteren Tatorten möglich wird.

Dem Beschluss werden als Anlagen Ausmessungsunterlagen zu den Funkzellen beigefügt. Die Ausmessung stellt sicher, dass wirlich nur der betroffene Bereich Gegenstand einer Anfrage ist.

Die Maßnahme ist im verdeckten Bereich häufig Ansatzpunkt für eine Telefonüberwachung, der baldmöglichst eine Observation zur Seite gestellt wird.

Praxisbezug

Retrograde Standortdaten spiele eine wichtige Rolle z.B. bei Geldautomatensprengungen, Einbrüchen in Banken und Sparkassen, Raubtaten, der Kfz-Verschiebung, im Betäubungsmittelhandel und in Erpressungsfällen.

Nun ist es in der Tat so, dass § 113b TKG eine allgemeine Speicherpflicht begründet, ohne dass nach personellen, zeitlichen oder geografischen Merkmalen eine Begrenzung stattfindet. Andererseits beträgt der Speicherzeitraum nicht mehr 6 bis 24 Monate, sondern nur noch 10 Wochen für Verkehrsdaten und 4 Wochen bei Standortdaten. Diese Zeiten sind relativ kurz bemessen und müssen den Zeitraum abdecken, in dem es zu einer Anzeige kommt und eine Reaktion der Strafverfolgungsbehörde samt richterlicher Entscheidung ohne schuldhaftes Zögern möglich ist. Überdies sind Personenkreise nach § 113b Abs. 6 i.V.m. § 99 Abs. 2 S. 1 TKG von der Speicherfrist ausgenommen.

Daten im Sinne eines Quick-Freeze-Verfahrens erst ab einem bestimmten Anlass zu speichern führt grundsätzlich nicht weiter. Denn wenn man die Täter vorab nicht kennt, ist eine solche Einschränkung außer nach Tatort bei gleichem modus operandi nicht möglich.

Weiter speichern die Provider immer weniger Abrechnungsdaten nach § 96 TKG, auf welche Strafverfolgungsbehörden Zugriff nehmen könnten.

Hält man die derzeitige Vorratsdatenspeicherung für unionswidrig, wäre zu überlegen, welche Möglichkeiten der Einschränkung dieser Speicherung möglich ist, die wenigstens teilweise eine Vorratsdatenspeicherung ermöglicht. So sieht das Polizeirecht die Einteilung als sog. kriminalitätsbelasteten Ort nach § 21 Abs. 2 Nr. 1. a) aa) ASOG vor, bei welchem ohne Weiteres Personenkontrollen stattfinden können. Die örtliche Eingrenzung würde aber auch die Aussagekraft erlangter Daten entwerten, da gerade untypische, kleinere Orte mit geringer Bevölkerungszahl aufschlussreich sein können, etwa bei einer Nummer, die sowohl am Tatort als auch nachts in einem entlegenen Dorf, in dem ein amtliches Kennzeichen entwendet wurde, festgestellt wurde, wenn bekannt ist, dass die Täter grundsätzlich für ihre Fluchtfahrzeuge gestohlene Kennzeichen nutzen.

Sensibilität der abgefragten Daten

Zu berücksichtigen ist bei den abgefragten Daten auch, dass hier Telefonnummern abgefragt werden, zu denen grds. keine Nachforschung zum Anschlussinhaber stattfindet. Die aufgelieferten Verkehrsdaten an sich haben keine Aussagekraft und lassen keinen Rückschlüss auf eine Einzelperson zu. Erst wenn z.B. bei mehrfach auftretenden Nummern bei Serientaten klar wird, dass eine Relevanz

in Betracht kommt, erfolgen solche Nachfragen. Die Sonderbände der Ermittlungsbehörden weisen keine Hinweise auf konkrete Personen auf. Bei übereinstimmenden Nummern zu mehreren Tatorten führt ein Abgleich häufig zur Feststellung von fiktiven Personalien der Anschlussinhaber. Überprüfungen zur Benachrichtigung nach durchgeführter Maßnahme erfolgen nicht, da dies den Eingriff in die betroffenen Rechte vertiefen würde.

Die Speicherfristen sind auf 4 bzw. 10 Wochen verkürzt. Es gibt Benachrichtigungspflichten und Rechtsschutzmöglichkeiten gegen die Maßnahme. Für Funkzellendaten gibt es einen abschließenden Katalog von Straftaten, der enger ist als der für eine Telefonüberwachung.

Die Mitteilungspflichten nach § 101 StPO sind sehr zeitaufwendig für Polizei (vorbereitend) und Staatsanwaltschaft. Es kommt grundsätzlich nicht zu Beschwerden von Drittbetroffenen – mir persönlich ist keine einzige bekannt -, dafür aber zu einer ganzen Reihe von Nachfragen Drittbetroffener, welche die Anschreiben inhaltlich nicht verstehen und sich erkundigen, ob sie verpflichtet seien, rechtliche Schritte zu unternehmen oder einen Anwalt zu beauftragen, was nicht der Fall ist.

Auswirkung der Änderung in der Strafverfolgung

Werden dem Bürgerrechtsstärkungs-Gesetz folgend keine Vorratsdaten mehr gespeichert, gibt es im Regelfall, da immer weniger Verkehrsdaten nach § 96 TKG gespeichert werden, auch keine Daten mehr, auf welche Strafverfolgungsbehörden Zugriff nehmen könnten. Gemäß § 100 g Abs. 2 StPO wird auf retrograde Verkehrsdaten ohnehin nur zugegriffen, wenn die Erforschung des Sachverhalts auf andere Weise nicht möglich oder erheblich erschwert wäre, in anderen Worten, wenn im Prinzip diese Datenabfrage der einzige Ermittlungsansatz ist. Als Folge des Gesetzes werden also schwere Straftaten unverfolgt bleiben. Das muss jedem, der das Gesetz befürwortet, klar sein. Dem gegenüber sind die Eingriffe angesichts der starken gesetzlichen Einschränkungen m.E. hinnehmbar und verhältnismäßig.

Berlin, den 9. Juni 2018

Petra Leister, Oberstaatsanwältin

Staatsanwaltschaft Berlin

DeutscherAnwaltVerein

Stellungnahme

des Deutschen Anwaltvereins durch den Ausschuss Gefahrenabwehrrecht

zum Entwurf eines Gesetzes zur Stärkung der Bürgerrechte (Bügerrechtestärkungs-Gesetz - BüStärG) der FDP-Fraktion vom 8.12.2017 (Drs. 19/204)

Stellungnahme Nr.: 24/2018 Berlin, im Juni 2018

Mitglieder des Ausschusses

- Rechtsanwältin Dr. Heide Sandkuhl, Potsdam (Vorsitzende und Berichterstatterin)
- Rechtsanwalt Wilhelm Achelpöhler, Münster
- Rechtsanwalt Dr. Nikolas Gazeas, LL.M., Köln
- Rechtsanwalt Prof. Dr. Björn Gercke, Köln
- Rechtsanwalt Dr. Stefan König, Berlin
- Rechtsanwältin Dr. Regina Michalke, Frankfurt / Main
- Rechtsanwältin Kerstin Oetjen, Freiburg
- Rechtsanwältin Lea Voigt, Bremen

Zuständig in der DAV-Geschäftsführung

- Rechtsanwalt Max Gröning

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
EU-Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Verteiler

Deutschland

Bundesministerium des Innern
Bundesministerium der Justiz und für Verbraucherschutz

Deutscher Bundestag – Ausschuss für Recht und Verbraucherschutz
Deutscher Bundestag – Innenausschuss

Arbeitsgruppen Inneres der im Deutschen Bundestag vertretenen Parteien
Arbeitsgruppen Recht der im Deutschen Bundestag vertretenen Parteien

Justizministerien und -senatsverwaltungen der Länder
Landesministerien und Senatsverwaltungen des Innern
Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Landesdatenschutzbeauftragte
Innenausschüsse der Landtage
Rechtsausschüsse der Landtage

Europäische Kommission – Vertretung in Deutschland
Bundesrechtsanwaltskammer
Deutscher Richterbund
Bundesverband der Freien Berufe
Gewerkschaft der Polizei (Bundesvorstand)
Deutsche Polizeigewerkschaft im DBB
Verd.di, Recht und Politik
stiftung neue verantwortung e.V.
Deutsches Institut für Menschenrechte

Vorstand und Landesverbände des DAV
Vorsitzende der Gesetzgebungs- und Geschäftsführenden Ausschüsse des DAV
Vorsitzende des FORUM Junge Anwaltschaft des DAV

Presse

Redaktion der Frankfurter Allgemeinen Zeitung
Redaktion der Süddeutschen Zeitung
Redaktion der Berliner Zeitung
Redaktion des Juris Newsletter
JurPC

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit derzeit rund 64.500 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

I. Einleitung

Der Entwurf des BüStärG regelt neben der Aufhebung des Netzwerkdurchsetzungsgesetzes in der Fassung der Bekanntmachung vom 1. September 2017 die Abschaffung der Vorratsdatenspeicherung. Zu Letzterem wird nachstehend Stellung genommen.

Art. 1 BüStärG-E sieht die Aufhebung von §§ 113a bis 113g TKG vor, nach Art. 2 BüStärG-E sollen die entsprechenden Vorschriften der StPO geändert und insbesondere § 100g Abs. 2, 4, 5 StPO aufgehoben und § 101a Abs. 1 StPO neu gefasst werden. Zur Begründung führt der Entwurf aus, es müsse eine Trendwende im Umgang mit den Grundrechten der Bürgerinnen und Bürger eingeleitet und gerade mit Blick auf die Rechtsprechung des EuGH[1] und des OVG Münster[2] die Regelungen zur Vorratsdatenspeicherung aufgehoben werden; der Gesetzgeber dürfe die erforderliche Kurskorrektur nicht in die Hände der Gerichte legen, er müsse selbst die Initiative ergreifen und die unverhältnismäßigen Regelungen zur Vorratsdatenspeicherung aufheben[3].

Nach Ansicht des Deutschen Anwaltvereins ist der Vorschlag zu begrüßen. Eine Aufhebung der Regelungen ist dringend geboten. Nach der Rechtsprechung des EuGH steht fest, dass die anlasslose Speicherung von Daten unionsrechtswidrig ist. Dass der Gesetzgeber dies jedoch bislang nicht zum Anlass genommen hat, die nationalen Regelungen über die Vorratsdatenspeicherung aufzuheben und es nach wie vor den Gerichten überlässt, mit dieser Rechtslage umzugehen, schafft Rechtsunsicherheiten: Während Verwaltungsgerichte entschieden haben, die in § 113a Abs. 1 i. V. m. § 113 b TKG angeordnete Speicherpflicht verstoße gegen das Unionsrecht – mit der Folge,

[1] U. v. 8.4.2014, Rs. C-292/12 u. C-594/12 – Digital Rights Ireland; U. v. 21.12.2016, Rs. C-203/15 u. C-698/15, Rn. 106 – Tele 2 Sverige AB u. Watson.
[2] B. v. 22.6.2017, 13 B 238/17.
[3] Drs. 19/204, S. 7 f.

dass die Bundesnetzagentur die seit dem 1. Juli 2017 bestehende Speicherpflicht für Telekommunikationsdienstleister vorerst ausgesetzt hat –, sieht das Landgericht Mannheim keine Zweifel an deren Vereinbarkeit mit Unionsrecht und hält, da die Netzbetreiber die Speicherpflichten zur Zeit nicht umsetzen müssen, eine analoge Anwendung des § 100g Abs. 2 StPO i. V. m. § 96 TKG für zulässig. Das Bundesverfassungsgericht hat die Beschwerdeführer im Verfahren 1 BvR 141/16 u.a. betreffend die Verfassungsbeschwerden gegen die nationalen Regelungen zur Vorratsdatenspeicherung überdies im November 2017 darauf hingewiesen, dass es auch auf die Frage ankommen könne, ob die angegriffenen Vorschriften mit den Anforderungen des EuGH an entsprechende Regelungen zur vorsorglichen Datenspeicherung vereinbar sei und welche Folgen sich hieraus für die verfassungsrechtliche Beurteilung des BVerfG ergeben. Mit anderen Worten: Der Gesetzgeber unterlässt es, den Rechten, die den Bürgerinnen und Bürger aus dem Unionsrecht erwachsen, die volle Wirksamkeit zu verschaffen. Durch seine Untätigkeit zwingt er vielmehr das Bundesverfassungsgericht dazu, sich mit der Frage zu befassen, ob die europäischen Grundrechte nicht nur die Union selbst, sondern auch ihre Mitgliedstaaten binden. Dieser Umweg ist schon deswegen nicht angezeigt, weil bis heute keine gesicherten empirischen Erkenntnisse darüber vorliegen, dass mit einer flächendeckenden Vorratsdatenspeicherung und dem damit verbundenen Eingriff in Art. 10 GG von 80 Millionen Bundesbürgerinnen und Bundesbürger Voraussetzungen geschaffen werden, ohne die eine wirksame Gefahrenabwehr und Strafverfolgung nicht möglich wäre. Dass solche Erkenntnisse nicht vorliegen, dürfte seinen Grund darin haben, dass es sie nicht gibt. Im Einzelnen:

II. Keine Europarechtskonformität der deutschen Regelungen

1. Urteil des EuGH vom 8. April 2014

Mit Urteil vom 8. April 2014 erklärte der EuGH die Richtlinie 2006/24/EG über die Vorratsdatenspeicherung vom 15. März 2006 wegen Verstößen gegen Art. 7 und Art. 8 GRCh für ungültig und nichtig. Der EuGH hielt fest, der Schutz des Grundrechts auf Achtung des Privatlebens verlange, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkung auf das „absolut

Notwendige“ beschränken müssten[4]. Dies aber ist nach der Rspr. des EuGH nicht der Fall, wenn Daten anlasslos und flächendeckend gespeichert werden, weil dadurch Personen betroffen sind, die elektronische Kommunikationsdienste nutzen, bei denen aber keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte[5].

2. Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015

Damit entfiel für die Bundesrepublik Deutschland die unionsrechtliche Verpflichtung, Regelungen zur Vorratsdatenspeicherung zu erlassen. Gleichwohl beschloss der Gesetzgeber das *Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten*, das am 18. Dezember 2015 in Kraft trat. Erstaunlich war dies, da der damalige Bundesminister der Justiz und für Verbraucherschutz nach seinem Amtsantritt im Kalenderjahr 2013 wiederholt und zu Recht (!) darauf hingewiesen hatte, dass „*eine anlasslose Vorratsdatenspeicherung gegen das Recht auf Privatheit und gegen den Datenschutz*“ verstößt[6]. Dennoch sind die nationalen Regelungen in §§ 113 ff. TKG so ausgestaltet worden, dass die Speicherung der Daten nach wie vor anlasslos erfolgt und nicht den Verdacht oder die drohende Gefahr einer schweren Straftat voraussetzt. Einschränkungen werden erst auf einer zweiten Stufe, mithin beim Abruf der Daten, vorgenommen. Nach § 100g Abs. 2 StPO dürfen die nach § 113d TKG gespeicherten Verkehrsdaten nur erhoben werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine der in Satz 2 bezeichneten besonders schweren Straftaten begangen hat oder in Fällen, in denen der Versuch strafbar ist, eine solche Straftat zu begehen versucht hat und die Tat auch im Einzelfall besonders schwer wiegt, soweit die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wären und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht.

[4] EuGH U. v. 8.4.2014, Rs. C-292/12 u. C-594/12 Rn. 52.
[5] Ebenda Rn. 56-60.
[6] DER SPIEGEL 13/2015, S. 34 f.

3. Urteil des EuGH vom 21. Dezember 2016

Dies aber steht nicht nur im diametralen Widerspruch zu der Entscheidung des EuGH vom 8. April 2014[7], sondern auch zum Urteil des EuGH vom 21. Dezember 2016[8]. Denn auch nach dieser Entscheidung ist nicht erst der Datenabruf, sondern bereits die Speicherung von Vorratsdaten auf Ausnahmefälle zu beschränken. Der EuGH hat klargestellt, dass Art. 15 Abs.1 der Richtlinie 2002/58 (= Datenschutzrichtlinie) im Lichte der Art.7, 8 und 11 sowie des Art.52 Abs. 1 GRCh dahingehend auszulegen sei, dass er einer nationalen Regelung entgegenstehe, die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsdatenspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Daten vorsehe. Insoweit führt der EuGH u. a. aus:

> „*Zudem kann zwar die Wirksamkeit der Bekämpfung schwerer Kriminalität, insbesondere der organisierten Kriminalität und des Terrorismus, in hohem Maß von der Nutzung moderner Ermittlungstechniken abhängen; eine solche dem Gemeinwohl dienende Zielsetzung kann jedoch, so grundlegend sie auch sein mag, für sich genommen die Erforderlichkeit einer nationalen Regelung, die die allgemeine und unterschiedslose Vorratsdatenspeicherung sämtlicher Verkehrs- und Standortdaten vorsieht, für die Kriminalitätsbekämpfung nicht rechtfertigen (…)*“[9].

Die Literatur hat hieraus zu Recht den Schluss gezogen, die Entscheidungsgründe seien so zu verstehen, dass eine Vorratsdatenspeicherung von der Kenntnis vom Vorliegen eines Verdachts einer Bedrohung der öffentlichen Sicherheit abhängen soll, was, wenn man diese Anforderung für sich betrachtet, für eine anlasslose Vorratsdatenspeicherung kaum einen Spielraum ließe[10]. Die *Wissenschaftliche Dienste des Deutschen Bundestages* fassen die Vorgaben des EuGH, die die aktuellen nationalen Regelungen nicht erfüllen, so zusammen,

---

[7] Siehe Fn. 1.
[8] Siehe Fn. 1.
[9] EuGH U. v. 21.12.2016, C-203/15 u. C-698/15, juris Rn. 103.
[10] *Kunnert* DuD 2014, 774, 777; *Leutheuser-Schnarrenberger* DuD 2014, 589, 592; *Otto/Seitlinger* MMR 2014, 9, 23; *Moos* K&R 2015, 158, 164; *Petri* ZD 2014, 300, 301; *Roßnagel* NJW 2017, 696, 698.

„*dass*

- *bereits die Speicherung von Vorratsdaten nur bei Vorliegen des Verdachts einer schweren Straftat zulässig ist,*
- *nur Vorratsdaten solcher Personen gespeichert werden, die Anlass zur Strafverfolgung geben,*
- *die Vorratsdatenspeicherung sich nicht auf geografisch eingegrenzte Gebiete beschränkt,*
- *die Vorratsdaten solcher Personen nicht gespeichert werden dürfen, deren davon betroffene Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen,*
- *grundsätzlich nur Zugang zu den Daten von Personen gewährt wird, die im Verdacht stehen, eine schwere Straftat zu planen, zu begehen oder begangen zu haben oder auf irgendeine Weise in eine solche Straftat verwickelt zu sein oder dass in besonderen Situationen, in denen vitale Interessen der nationalen Sicherheit, der Landesverteidigung oder der öffentlichen Sicherheit durch terroristische Aktivitäten bedroht sind, Zugang zu Daten anderer Personen nur gewährt wird, wenn es objektive Anhaltspunkte dafür gibt, dass diese Daten in einem konkreten Fall einen wirksamen Beitrag zur Bekämpfung solcher Aktivitäten leisten können*“[11].

Der DAV hatte bereits mit Stellungnahme 25/2015 darauf hingewiesen, dass die nationalen Regelungen über die Vorratsdatenspeicherung die Berufsgeheimnisträger nur unzureichend schützen, da auch ihre Daten anlasslos gespeichert werden, dies aber betreffend die Anwältinnen und Anwälte, deren Tätigkeit auf Vertrauen angelegt ist, nicht im Einklang mit § 97 StPO und § 160 StPO steht, die den Schutz von Berufsgeheimnisträgern bereits auf der Erhebungsebene vorsehen.

4. Beschluss des OVG Münster vom 22. Juni 2017

Mit Beschluss vom 22. Juni 2017 erklärte das OVG Münster die Verpflichtung zur Vorratsdatenspeicherung infolge der Rechtsprechung des EuGH in ihrer gegenwärtigen Ausgestaltung nicht mit Art. 15 Abs. 1 der Datenschutzrichtlinie 2002/58/GE vereinbar. Infolge dieser Entscheidung stellte das VG Köln mit Urteil vom 20. April 2018[12] fest, dass der klagende Telekommunikationsdiensteanbieter (= Spacenet) nicht verpflichtet ist, ab dem 1. Juli 2017 die in § 113b Abs. 3 TKG aufgeführten Telekommunikations-

[11] Wissenschaftliche Dienste des Deutschen Bundestages, Ausarbeitung, Zur Vereinbarkeit des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten mit dem EuGH-Urteil vom 21. Dezember 2016 zur Vorratsdatenspeicherung, PE 6-3000-167/16, S. 24.
[12] Az: 9 K 3859/16.

Verkehrsdaten seiner Kunden zu speichern, denen er den Internet-Zugang vermittelt. Unter Berufung auf die Entscheidung des OVG Münster vom 22. Juni 2017 hat die Bundesnetzagentur die seit dem 1. Juli 2017 gemäß § 150 Abs. 13 TKG i. V. m. § 113b TKG bestehende Verpflichtung der Telekommunikationsdienstleister zur Vorratsdatenspeicherung vorerst ausgesetzt[13].

III. Auswirkungen der Rechtsprechung des EuGH auf die Regelungen über die Vorratsdatenspeicherung in Deutschland

Nach Analyse des Urteils des EuGH vom 21. Juni 2017[14] haben die *Wissenschaftliche Dienste des Deutschen Bundestages*[15] darauf hingewiesen, dass die innerstaatlichen Organe, auch Legislativorgane, dafür Sorge tragen sollen, dass „*das nationale Recht so schnell wie möglich mit dem Unionsrecht in Einklang gebracht und den Rechten, die dem Bürger aus dem Unionsrecht erwachsen, die volle Wirksamkeit verschafft wird*". Dies aber ist bislang nicht geschehen, der deutsche Gesetzgeber hat die nationalen Regelungen über die Vorratsdatenspeicherung bislang nicht aufgehoben, sondern diese – im Gegenteil – noch erweitert. Denn der Straftatenkatalog des § 100g Abs. 2 S. 2 StPO wurde mit dem 55. Gesetz zur Änderung des Strafgesetzbuches – Wohnungseinbruchdiebstahl vom 17. Juli 2017[16] erweitert. Offenbar soll die Entscheidung des BVerfG im Hauptsacheverfahren über die Verfassungsbeschwerden von Rechtsanwälten, Ärzten, Journalisten und Mitgliedern des Bundestages bzw. des Berliner Abgeordnetenhauses abgewartet werden. Die Eilanträge der Beschwerdeführer, die durch das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 (im Folgenden: Vorratsdatenspeicherungsgesetz) eingeführte Vorratsdatenspeicherung von Telekommunikations-Verkehrsdaten zu Zwecken der öffentlichen Sicherheit außer Kraft zu setzen, lehnte das Bundesverfassungsgericht ab und führte u. a. aus, dass zwar in dem Verkehrsdatenabruf nach § 100g Abs. 1, Abs. 2 StPO ein schwerwiegender und

[13] Vgl. Editorial FD-StrafR 2017, 392885.
[14] C-231/06, juris Rn. 38-41.
[15] Wissenschaftliche Dienste des Deutschen Bundestages, Ausarbeitung, Auswirkungen auf den Strafprozess bei einer möglicherweise bestehenden Unvereinbarkeit des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten mit dem Urteil des EuGH vom 21. Dezember 2016 zur Vorratsdatenspeicherung, WD 7-3000-191/116, S. 23.
[16] BGBl. 2017 I. 2442.

irreversibler Eingriff in das Grundrecht aus Art. 10 Abs. 1 GG liege, der Gesetzgeber jedoch den Datenabruf von qualifizierten Voraussetzungen abhängig gemacht habe, die das Gewicht der durch den Vollzug der Vorschrift drohenden Nachteile für die Übergangszeit bis zur Entscheidung über die Hauptsache hinnehmbar und im Vergleich mit den Nachteilen für das öffentliche Interesse an einer effektiven Strafverfolgung weniger gewichtig erscheinen lassen[17]. Auch nach der Entscheidung des EuGH vom 21. Dezember 2016[18] lehnte das BVerfG den Antrag auf Erlass einer einstweiligen Anordnung zur Außerkraftsetzung der Regelung über die Vorratsdatenspeicherung ab[19]. Oder um es mit den Worten des OVG Münster zu sagen:

> „*Die Frage, ob und gegebenenfalls in welcher Weise die europäischen Grundrechtecharta oder sonstiges Unionsrecht für die verfassungsrechtliche Beurteilung der durch die Antragstellerin angegriffenen Regelung von Bedeutung sind, ist Teil derjenigen Fragen, deren Klärung das Bundesverfassungsgericht im Eilrechtschutzverfahren nicht für geeignet hält und mit Blick auf die dort gegenwärtigen anhängigen Verfassungsbeschwerden der Hauptsacheentscheidung vorbehalten hat*“[20].

Wohin dies derzeit führt, zeigt nicht zuletzt der Beschluss des Landgerichts Mannheim vom 18. Januar 2018[21] eindrucksvoll. Während sich die Literatur[22] noch sicher war, dass bis zur Hauptsacheentscheidung des BVerfG über die nationalen Regelungen der Vorratsdatenspeicherung eine strafprozessuale Erhebung von anlasslos „auf Vorrat“ gespeicherten Verkehrsdaten nicht zu befürchten sei, muss diese sich nun eines „Besseren“ belehren lassen: Anders als das OVG Münster hat das Landgericht Mannheim „*aufgrund der restriktiven Vorgaben der deutschen Regelung derzeit keine Zweifel an deren Vereinbarkeit mit Unionsrecht und sieht daher keine Veranlassung, ein Vorabentscheidungsersuchen nach Art. 267 AEUV zu stellen*“[23]. Dass bereits die Speicherung der Daten auf das absolut Notwendige zu beschränken ist, blendet das Landgericht völlig aus und zieht sich argumentativ darauf zurück, dass allein das BVerfG oder der EuGH eine verbindliche Entscheidung über die Verfassungs- und Europarechtskonformität des Vorratsdatenspeicherungsgesetzes zu treffen hätten, das BVerfG jedoch mit Beschluss vom 26. März 2017 entschieden habe, dass auch nach

[17] BVerfG B. v. 8.6.2016, 1 BvQ 42/15, juris Rn. 21, 22.
[18] Siehe Fn. 1.
[19] BVerfG B. v. 26.3.2017, 1 BvR 3156/15.
[20] OVG Münster B. v. 22.6.2017, 13 B 238/17, juris Rn. 97.
[21] 4 Qs 39/17, juris.
[22] FD- Strafrecht 2017, 392885, Editorial
[23] LG Mannheim B. v. 18.1.2018, 4 Qs 39/17, juris Rn. 13.

dem Urteil des EuGH vom 21. Dezember 2016 eine Außerkraftsetzung von § 100g StPO und §§ 113a, 113b TKG nicht in Betracht komme und sich das Urteil des EuGH vom 21. Dezember 2016 nicht auf das deutsche Recht beziehe[24]. Mit diesem Beschluss hat das Landgericht Mannheim eine analoge Anwendung des § 100g Abs. 2 StPO i. V. m. § 96 TKG für zulässig erklärt. Den Rückgriff auf § 96 TKG hält es für zulässig, da die Daten i. S. d. § 113b TKG nicht abgerufen werden können, weil die Netzbetreiber die gesetzlichen Speicherpflichten nicht umsetzten.

IV. Prüfungsmaßstab des BVerfG

Ob das BVerfG als Prüfungsmaßstab die Charta der Grundrechte der Europäischen Union anlegen wird, bleibt abzuwarten. Nach seiner Rechtsprechung[25] ist ein Vorabentscheidungsverfahren und eine Prüfung anhand der Charta der Grundrechte der Europäischen Union nur geboten, wenn die angegriffenen nationalen Vorschriften durch das Unionsrecht determiniert sind. Jedenfalls hat es die Beschwerdeführer im Verfahren 1 BvR 141/ 16 betreffend das Vorratsdatenspeicherungsgesetz darauf hingewiesen, dass es neben den mit den Verfassungsbeschwerden aufgeworfenen Fragen bezüglich der materiellen Beurteilung der angegriffenen Vorschriften am Maßstab der Grundrechte des Grundgesetzes voraussichtlich auch auf die Fragen ankommen könne, ob die angegriffenen Vorschriften mit den Anforderungen des EuGH (Urteil vom 21. Dezember 2016; C-203/15 u.a.) vereinbar seien und welche Folgen sich hieraus für die verfassungsrechtliche Beurteilung des BVerfG ergeben. Dies aber lässt den Schluss zu, dass das BVerfG – anders als das Landgericht Mannheim – sehr wohl Zweifel an der Europarechtskonformität der in Rede stehenden nationalen Regelungen hat und sich mit der umstrittenen und nicht einfachen Frage befassen wird, ob und gegebenenfalls wieweit europäische Grundrechte nicht nur die Union selbst, sondern auch ihre Mitgliedstaaten binden[26].

Aber selbst wenn das BVerfG die in Rede stehenden Regelungen (nur) am Maßstab des Art. 10 GG beurteilt, kann nicht von einer Verfassungsmäßigkeit der Vorschriften

[24] Ebenda Rn. 10 ff.
[25] BVerfG NJW 2013, 1499, 1501 („Antiterrordatei").
[26] Siehe hierzu instruktiv Dombert, Der Grundrechtsföderalismus der Vereinigten Staaten von Amerika – Eine Darstellung vor dem Hintergrund der Debatte um die Bindung der Mitgliedstaaten an die Grundrechte der Europäischen Union, Nomos, 2017, S. 23 ff.

ausgegangen werden. Bereits mit Stellungnahme 25/2015 hat der DAV auf die Unverhältnismäßigkeit der Vorratsdatenspeicherung hingewiesen und dargetan, dass das Rechtfertigungsdefizit umso schwerer wiegt, als keine gesicherten empirischen Erkenntnisse darüber vorliegen, ob mit der flächendeckenden Vorratsdatenspeicherung Voraussetzungen geschaffen werden, ohne die eine wirksame Gefahrenabwehr und Strafverfolgung nicht möglich wäre.

V. Fazit

Aus Sicht des DAV verliert Europafreundliche Politik an Glaubwürdigkeit, wenn Verstöße gegen das Unionsrecht hingenommen werden und der Gesetzgeber keine Konsequenzen aus der Rspr. des EuGH zieht. Will der Gesetzgeber dem – aus dem Verfassungsauftrag zur Verwirklichung eines vereinten Europas abgeleiteten – Grundsatz der Europarechtsfreundlichkeit rechtspolitisch Geltung verschaffen, ist er aufgefordert, die Vorratsdatenspeicherung aufzuheben. Tut er dies nicht und verlagert er die Entscheidung nach Karlsruhe, muss er sich nicht wundern, wenn Forderungen der Bundesrepublik Deutschland an andere Mitgliedsstaaten, die Rspr. des EuGH umzusetzen, unerfüllt bleiben.

Stellungnahme zum Entwurf eines Gesetzes zur Stärkung der Bürgerrechte

-

unter besonderer Berücksichtigung
der ermittlungstaktischen und beweisrechtlichen Bedeutung
von Verkehrsdaten in der Ermittlungs- und Verfahrenspraxis
der Strafverfolgungsbehörden und Gerichte[1]

vorgelegt von
Richter am Oberlandesgericht Marc Wenske[2]

Der Entwurf eines Gesetzes zur Stärkung der Bürgerrechte sieht eine Streichung der durch das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 (BGBl. I, S. 2218; im Folgenden: Vorratsdatenspeicherungsgesetz) eingeführten Vorratsspeicherung von Telekommunikations-Verkehrsdaten zu Zwecken der öffentlichen Sicherheit vor.[3] Er stellt damit den vorläufigen Schlusspunkt der rechtspolitischen Diskussion über das in Rede stehende Ermittlungsinstrument dar.

Zur Vorbereitung der rechtspraktischen Bewertung der geltenden Rechtslage sollen die maßgeblichen Regelungen zunächst einleitend zusammenfassend dargestellt werden (**I. u. II.**); sodann soll auf die dem Gesetzesentwurf zugrunde liegenden Bewertungen im Einzelnen näher eingegangen werden, wobei hier der Schwerpunkt auf einer rechtspraktischen Betrachtung des Ermittlungsinstruments gespeicherter Verkehrsdaten liegen wird (**III.**). Abschließend sollen die absehbaren Konsequenzen des Gesetzesvorhabens in den Blick genommen werden (**IV.**).

---

[1] Anhörung des Ausschusses für Recht und Verbraucherschutz vom 13. Juni 2018.
[2] Der Verf. ist Mitglied des mit Revisions- und Beschwerdeverfahren sowie Auslieferungssachen befassten 1. Strafsenats des Hanseatischen Oberlandesgerichts in Hamburg und zugleich Ermittlungsrichter I in Staatsschutzsachen desselben Gerichts; zuvor war er tätig in Großen Strafkammern des Landgerichts Hamburg, am Amtsgericht, dort auch als Ermittlungsrichter, und war abgeordnet als wissenschaftlicher Mitarbeiter an den 5. Strafsenat des Bundesgerichtshofs.
[3] Art. 1, 2, 3 und 6 des Gesetzesentwurfs, BT-Drucks. 19/204.

I. Gesetzessystematischer Hintergrund

Die mit dem Vorratsdatenspeicherungsgesetz eingeführte Speicherpflicht und eingeführte Höchstspeicherfrist für Verkehrsdaten dient nach der Gesetzesbegründung der Vereinheitlichung der Speicherpraxis der Erbringer öffentlich zugänglicher Telekommunikationsdienste. Es soll Unzulänglichkeiten in der Strafverfolgungsvorsorge und der Gefahrenabwehr durch abgestimmte Regelungen in der Strafprozessordnung und im Telekommunikationsgesetz beseitigen.[4]

1. Die erste Tür: Schutzmaßgaben des Telekommunikationsgesetzes

Der durch das Vorratsdatenspeicherungsgesetz neugefasste § 113a Abs. 1 TKG bestimmt mit den Anbietern öffentlich zugänglicher Telekommunikationsdienste für Endnutzer den Verpflichteten der Vorratsdatenspeicherung. Er verpflichtet nunmehr diese – allein – privaten Anbieter öffentlich zugänglicher Telekommunikationsdienste für Endnutzer, bestimmte und näher spezifizierte Verkehrs- und Standortdaten unabhängig von einem besonderen Anlass für einen bestimmten Zeitraum zu speichern und für die Nutzung durch die Sicherheitsbehörden bereitzuhalten. Verkehrsdaten im Sinne des § 113b Abs. 2 und 3 TKG, etwa Rufnummern, Datum und Uhrzeit von Beginn und Ende der Verbindung, Internetprotokoll-Adressen, müssen gemäß § 113b Abs. 1 Nr. 1 TKG für zehn Wochen gespeichert werden; die Speicherpflicht für Standortdaten nach § 113b Abs. 4 TKG, etwa die Bezeichnungen der Funkzellen bei der Nutzung mobiler Telefondienste, beträgt demgegenüber vier Wochen (vgl. § 113b Abs. 1 Nr. 2 TKG). Der Inhalt der Kommunikation, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post dürfen aufgrund dieser Vorschrift nicht gespeichert werden (vgl. § 113b Abs. 5 TKG). Dieses Speicherverbot gilt gleichermaßen für Daten, die den in § 99 Abs. 2 TKG genannten Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen zugrunde liegen (§113b Abs. 6 Satz 1 TKG).

Die Speicherung der Daten hat so zu erfolgen, dass Auskunftsersuchen der berechtigten Stellen unverzüglich beantwortet werden können (vgl. § 113b Abs. 7 TKG). Nach

[4] Vgl. BT-Drucks. 18/5088, S. 21 f.

§ 113b Abs. 8 TKG hat der nach § 113a Abs. 1 TKG Verpflichtete die gespeicherten Daten unverzüglich, spätestens jedoch binnen einer Woche nach Ablauf der Speicherfristen nach § 113b Abs. 1 TKG, irreversibel zu löschen oder die irreversible Löschung sicherzustellen. In § 113c TKG werden abschließend (vgl. § 113c Abs. 2 TKG) die zulässigen Verwendungszwecke der nach § 113b TKG gespeicherten Daten normiert. So dürfen etwa gespeicherte Daten an eine Strafverfolgungsbehörde übermittelt werden, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung, die ihr eine Erhebung der in § 113b TKG genannten Daten zur Verfolgung besonders schwerer Straftaten erlaubt, verlangt. Die Daten sind dabei so zu kennzeichnen, dass erkennbar ist, dass es sich um Daten handelt, die nach § 113b TKG gespeichert waren (vgl. § 113c Abs. 3 Satz 2 TKG).

Weiter wird hier gesetzlich ausdrücklich bestimmt, für welche Zwecke die Daten verwendet werden dürfen und, dass private Telekommunikationsunternehmen von ihrer im Übrigen geltenden Geheimhaltungspflicht insoweit befreit werden. Auch sieht § 113d TKG näher bestimmte Anforderungen an die Gewährleistung der Datensicherheit vor. Der nach § 113a Abs. 1 TKG verpflichtete private Telekommunikationsunternehmer hat gemäß § 113e TKG sicherzustellen, dass für Zwecke der Datenschutzkontrolle jeder Zugriff, insbesondere das Lesen, Kopieren, Ändern, Löschen und Sperren der gespeicherten Daten protokolliert wird und etwa die Protokolldaten – Zeitpunkt des Zugriffs, zugreifende Personen, Zweck und Art des Zugriffs – nach einem Jahr gelöscht werden.

2. Die zweite Tür: Staatlicher Abruf allein auf richterliche Anordnung

Ob die Daten an die staatlichen Stellen weitergegeben werden dürfen, also nach der Erhebung durch die privaten Telekommunikationsanbieter auch den Weg durch eine zweite Tür, zu den Ermittlungs- oder Gefahrenabwehrbehörden finden, ist nicht Regelungsgegenstand des Telekommunikationsgesetzes. Die entsprechenden Verfahrenssicherungen für diese zweite Tür und für eine berechtigte Datenübermittlung an staatliche Stellen bestimmt sich für das Strafverfahren nach § 100g StPO.[5] Während in § 100g Abs. 1 die Erhebung von Verkehrsdaten geregelt wird, die aus geschäftlichen

[5] Vgl. BT-Drucks. 18/5088, S. 36, 40.

Gründen bei den Erbringern öffentlich zugänglicher Telekommunikationsdienste gespeichert werden (§ 96 TKG), legt § 100g Abs. 2 StPO fest, unter welchen Voraussetzungen die gespeicherten retrograden Daten erhoben werden dürfen: Gesetzlich zwingend erforderlich sind hier ein durch bestimmte Tatsachen begründeter Verdacht betreffend eine der in § 100g Abs. 2 Satz 2 StPO enumerativ und abschließend aufgeführten besonders schweren Straftaten,[6] die auch im Einzelfall besonders schwer wiegen. Darüber hinaus muss die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos sein und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache stehen. § 100g Abs. 4 StPO schließt zum Schutz von Berufsgeheimnisträgern im Sinne des § 53 Abs. 1 Satz 1 Nr. 1 bis 5 StPO die Erhebung von Verkehrsdaten nach § 100g Abs. 2 StPO aus.

In formeller Hinsicht wird die Anordnung gesetzlich allein dem Richter überantwortet. Die Überprüfung sämtlicher Anordnungsvoraussetzungen, gerade auch des Tatverdachts und der Tatschwere, unterliegt damit ausschließlich unabhängiger gerichtlicher Kontrolle (Art. 97 Abs. 1 GG; §§ 101a, § 100b Abs. 1 StPO). Schließlich ist nach § 101 a Abs. 6 StPO eine Benachrichtigung der Beteiligten der betroffenen Telekommunikation nach Maßgabe des § 101 Abs. 4 Satz 2 bis 5 und Abs. 5 bis 7 StPO gesetzlich vorgesehen.

II. Rechtsentwicklung nach Inkrafttreten der Neuregelung

Unmittelbar nach Inkrafttreten der vorgenannten Neuregelungen wurden hiergegen Eilanträge beim *Bundesverfassungsgericht (BVerfG)* mit dem Ziel eingereicht, die maßgebenden Bestimmungen des Telekommunikationsgesetzes und der Strafprozessordnung außer Kraft zu setzen; das Bundesverfassungsgerichts hat sämtliche Eilanträge abgewiesen und hierzu in seinen Beschlussgründen namentlich ausgeführt:

> „a) Ein besonders schwerwiegender und irreparabler Nachteil, der es rechtfertigen könnte, den Vollzug der Norm ausnahmsweise im Wege einer einstweiligen Anordnung auszusetzen, liegt in der Datenspeicherung allein nicht.

[6] Vgl. BT-Drucks. 18/5088, S. 31.

Zwar kann die gegenüber den Verpflichteten nach § 113a TKG in § 113b TKG angeordnete umfassende und anlasslose Bevorratung sensibler Daten über praktisch jedermann für staatliche Zwecke, die sich zum Zeitpunkt der Speicherung der Daten nicht im Einzelnen absehen lassen, einen erheblichen Einschüchterungseffekt bewirken, weil das Gefühl entsteht, ständig überwacht zu werden. Dieser Effekt ließe sich für die Zeit zwischen dem Inkrafttreten der Norm und der Entscheidung des Bundesverfassungsgerichts selbst dann nicht rückgängig machen, wenn die Verfassungsbeschwerde in der Hauptsache Erfolg haben sollte.

Der in der Speicherung für Einzelne liegende Nachteil für ihre Freiheit und Privatheit verdichtet und konkretisiert sich jedoch erst durch einen Abruf der Daten zu einer möglicherweise irreparablen Beeinträchtigung. Die Datenbevorratung ermöglicht zwar den Abruf, doch führt erst dieser zu konkreten Belastungen. Das Gewicht eines denkbaren Einschüchterungseffekts hängt dann davon ab, unter welchen Voraussetzungen die bevorrateten Daten abgerufen und verwertet werden können. Je weiter die Befugnisse staatlicher Stellen insoweit reichen, desto eher müssen die Bürgerinnen und Bürger befürchten, dass diese Stellen ihr Kommunikationsverhalten überwachen (vgl. BVerfGE 121, 1, 20). So ist mit der Speicherung allein jedoch noch kein derart schwerwiegender Nachteil verbunden, dass er die Außerkraftsetzung eines Gesetzes erforderte. Dies gilt auch für die Speicherung der Daten von Berufsgeheimnisträgern.

…

b) Eine Aussetzung des Vollzugs ist auch nicht hinsichtlich der §§ 100g, 101a und 101b StPO geboten.

aa) Allerdings liegt in dem Verkehrsdatenabruf nach § 100g Abs. 1 und 2 StPO ein schwerwiegender und nicht mehr rückgängig zu machender Eingriff in das Grundrecht aus Art. 10 Abs. 1 GG. Ein solcher Datenabruf ermöglicht es, weitreichende Erkenntnisse über das Kommunikationsverhalten und die sozialen Kontakte der Betroffenen zu erlangen, ggf. sogar begrenzte Rückschlüsse auf die Gesprächsinhalte zu ziehen. Zudem weist ein Verkehrsdatenabruf eine erhebliche Streubreite auf, da er neben der Zielperson des Auskunftsersuchens notwendigerweise deren Kommunikationspartner erfasst, also vielfach Personen, die in keiner Beziehung zu dem Tatvorwurf stehen und den Eingriff in ihr Grundrecht aus Art. 10 Abs. 1 GG durch ihr Verhalten nicht veranlasst haben (vgl. BVerfGE 107, 299, 318 ff.; 121, 1, 22).

Doch hat der Gesetzgeber mit § 100g Abs. 2 StPO den Abruf von Telekommunikations-Verkehrsdaten im Sinne des § 113b TKG von qualifizierten Voraussetzungen abhängig gemacht, **die das Gewicht der dem Einzelnen und der Allgemeinheit durch den Vollzug der Vorschrift drohenden Nachteile für die Übergangszeit bis zur Entscheidung über die Hauptsache hinnehmbar und im Vergleich mit den Nachteilen für das öffentliche Interesse an einer effektiven Strafverfolgung weniger gewichtig erscheinen lassen.**“[7]

(Hervorhebungen durch *Verf.*)

Mit Urteil vom 21. Dezember 2016 entschied der *Gerichtshof der Europäischen Union (EuGH)* in den verbundenen Verfahren C-203/15 und C-698/15 über die Vereinbarkeit von Regelungen des Königreiches Schweden und des Vereinigten Königreiches

[7] BVerfG, Beschl. v. 8. Juni 2016 – 1 BvR 229/16, EuGRZ 2016, 501; ebenso Beschl. v. 8. Juni 2016 – 1 BvQ 42/15, NVwZ 2016, 1240.

Großbritanniens und Nordirland mit den Maßgaben der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rats vom 12. Juli 2012 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation. Er stellte insoweit klar, dass eine allgemeine und unterschiedslose Vorratsdatenspeicherung unionsrechtlich unzulässig sei.[8]

Auch im Lichte dieser allein das Königreich Schweden und das Vereinigte Königreich Großbritannien und Nordirland betreffenden Entscheidung aus dem Dezember 2016 hat das *BVerfG* keinen Anlass gesehen, nunmehr den bei ihm anhängigen Eilrechtsschutzbegehren gegen die Regelungen im deutschen Recht stattzugeben. Auch die unionsrechtlichen Fragen werden damit dem bislang noch nicht vom *BVerfG* entschiedenen Hauptsacheverfahren über die anhängigen Verfassungsbeschwerden überlassen.[9]

Ungeachtet dessen hob das *OVG Nordrhein-Westfalen* in einem von einem Internetprovider betriebenen verwaltungsgerichtlichen Eilrechtsschutzverfahren im Juni 2017 dessen gesetzliche Pflicht zur Speicherung von Verkehrsdaten bis zur Entscheidung über die Hauptsache wegen einer von ihm erkannten Unvereinbarkeit des deutschen Rechts mit unionsrechtlichen Maßgaben auf.[10] Zur Begründung führte es an, dass sich die Regelungen wegen des mit der Speicherpflicht verbundenen technischen und finanziellen Aufwands als rechtswidriger Eingriff in die unternehmerische Freiheit des dort antragstellenden Internetproviders erweisen würden.

Die Bundesnetzagentur hat diese Eilrechtsentscheidung zum Anlass genommen, keine Anordnungen oder sonstige Maßnahmen zur zwangsweisen Durchsetzung der Speicherverpflichtung gegen sämtliche Erbringer von Telekommunikationsdienstleistungen in den Fällen verletzter gesetzlicher Speicherpflichten zu ergreifen (vgl. § 149 TKG). Sämtliche Erbringer von Telekommunikationsleistungen sehen derzeit mit Blick auf diese Verwaltungspraxis der Bundesnetzagentur und mit Blick auf die Entscheidung des Oberverwaltungsgerichts von einer ihrer gesetzlichen Verpflichtung entsprechenden Speicherung ab. Dies auch, obgleich das *BVerfG* zeitlich nachfolgend eine

[8] Vgl. EuGH, Urt. v. 21. Dezember 2016 – C-203/15 u. C-698/15, NJW 2017, 717.
[9] BVerfG, Beschl. v. 26. März 2017 – 1 BvR 141/16, ZD 2017, 300.
[10] OVG Müster, Beschl. v- 22. Juni 2017 – 13 B 238/17, NVwZ-RR 2018, 43.

(weitere) Verfassungsbeschwerde gegen § 113b Abs. 1 TKG mit folgender Begründung nicht zur Entscheidung angenommen hat:

> „Es handelt sich um eine Berufsausübungsregelung, die – gestützt auf die Erwägung, dass die Daten in Blick auf die Anwendbarkeit der deutschen Regelungen und die Zuständigkeit deutscher Aufsichtsinstanzen im Inland gespeichert werden sollen – ungeachtet der unionsrechtlichen Harmonisierung des Datenschutzes einen legitimen Gemeinwohlzweck verfolgt und im Übrigen verhältnismäßig ist.“[11]

Auch auf eine richterliche Anordnung hin stehen den Strafverfolgungs- und Gefahrenabwehrbehörden mangels Erfüllung der gesetzlichen Speicherpflichten durch die Anbieter öffentlich zugänglicher Telekommunikationsdienste seitdem keine Verkehrsdaten über zurückliegende Telekommunikationsvorgänge als Erkenntnismittel zur Aufklärung von Straftaten oder zur – etwa polizeilichen – Gefahrenabwehr zur Verfügung.

III. Ausgangspunkte des Gesetzesentwurfs

Der Gesetzesentwurf knüpft den Vorschlag, die Neuregelung über die Verkehrsdatenspeicherung aufzuheben (Art. 1, 2, 3 und 6 des Gesetzesentwurfs), an einen doppelten Befund:

Zunächst habe der Gesetzgeber nach Ansicht des Entwurfs bei dem auch ihm obliegenden „Schutz der Bürger vor den Bedrohungen durch Kriminalität und Terrorismus“, die „Grenzen, die das Grundgesetz staatlichem Handeln zieht … mehrfach überschritten“, sodass die „verfassungs- und europarechtswidrige Vorratsdatenspeicherung“ abzuschaffen sei. Überdies sei es – die Vereinbarkeit der Vorratsdatenspeicherung mit dem Grundgesetz unterstellt – „verfassungspolitisch nicht klug“, die äußersten Grenzen des Verfassungsrechts… ohne überzeugende Gründe auszureizen.“[12]

IV. Stellungnahme zu beiden Ausgangspunkten

1. Vom Überschreiten verfassungsrechtlicher Grenzen

An dieser Stelle soll – aus strafrechtspraktischer Sicht – zur Frage der Verfassungswidrigkeit der geltenden Rechtslage nur auf folgende Umstände hingewiesen werden:

[11] BVerfG, Beschl. v. 28. September 2017 – 1 BvR 1560/17, BeckRS 2017, 129759.
[12] BT-Drucks. 19/204 S. 1.

a) Eine Entscheidung des *BVerfG* über die Vereinbarkeit der deutschen Neuregelungen aus dem Jahre 2015 mit dem Grundgesetz, aber auch mit europarechtlichen Maßgaben ist bisher nicht ergangen. Der Ausgang der anhängigen Verfassungsbeschwerdeverfahren ist derzeit nicht absehbar; sämtliche – freilich nur eine äußerst begrenzte verfassungsgerichtliche Prüfpflicht auslösende – Eilanträge blieben erfolglos. Auch kann der fachgerichtlichen Entscheidung eines Oberverwaltungsgerichts kein Fingerzeig auf den Ausgang der Verfassungsbeschwerdeverfahren entnommen werden. Dies gilt schon deshalb, weil sich die verwaltungsgerichtliche Fachentscheidung allein auf eine – vom *BVerfG* aber bereits in seinem Urteil vom 2. März 2010 (1 BvR 256/08) unter dem Aspekt der Berufsausübungsfreiheit (Art. 12 Abs. 1 GG) ohne durchgreifende verfassungsrechtliche Bedenken in den Blick genommene[13] – Beeinträchtigung der auch unionsrechtlich geschützten unternehmerischen Freiheit stützt und damit gerade nicht die erkennbar im Verfassungsbeschwerdeverfahren absehbar besonders bedeutsamen Fragen der Telekommunikationsfreiheit tragend berücksichtigt hat. Im Übrigen sei auf die allein dem Bundesverfassungsgericht als Verfassungsorgan zustehende Kompetenz zur Nichtigerkärung von Gesetzen hingewiesen (vgl. § 95 Abs. 3 BVerfGG).

b) Selbst wenn aber Teile der Neuregelung einer verfassungsgerichtlichen Überprüfung nicht standhalten sollten, so ist mit Blick auf die mit Augenmaß und streng orientiert an den Maßgaben der Entscheidung des *BVerfG* aus dem Jahre 2010 gefassten gesetzlichen Neuregelungen nicht abermals eine vollständige Nichtigerklärung der angegriffenen Vorschriften zu erwarten. Bereits im Jahre 2010 war diese Frage im 1. Senat nicht unumstritten.[14] Der Gesetzgeber würde in diesem Fall deshalb absehbar die Gelegenheit zu partiellen Nachbesserungen haben und wird auch weiterhin nicht pauschal von diesem Ermittlungsinstrument absehen müssen.

c) An der deshalb derzeit offenen verfassungsgerichtlichen Beurteilung ändert auch die zwischenzeitlich ergangene und vorstehend dargelegte Entscheidung des *EuGH* nichts. Zunächst wirkt sie nur inter partes; Regelungen deutschen Rechts waren nicht

[13] NJW 2010, 833, 850.
[14] Vgl. die abweichenden Voten der Richter *Schluckebier* und *Eichberger*, a.a.O., S. 855 f.

Gegenstand der entschiedenen Verfahren. Überdies unterscheiden sich die deutschen Regelungen über die Verkehrsdatenspeicherung von denen, die der Beurteilung durch den *EuGH* unterstellt waren. Hier sei insbesondere auf die verfahrensrechtlichen Absicherungen der „doppelten Tür", auf den uneingeschränkten Richtervorbehalt (vgl. § 101a Abs. 1 Satz 1 StPO), auf die Benachrichtigungspflichten sowie auf die spezifischen gerichtlichen Tenorierungspflichten hingewiesen. Aber auch in materieller Hinsicht unterscheidet sich die deutsche Rechtslage; so liegt nach geltendem Recht eine den schwedischen und britischen Regelungen vergleichbare flächendeckende und undifferenzierte Erhebung von Verkehrsdaten nicht vor. Nach geltendem Recht werden nämlich insbesondere Daten über den E-Mail-Verkehr der Nutzer nicht erhoben; weiterhin ist auf § 113b Abs. 6 TKG hinzuweisen, nach dem Anschlüsse von Personen, Behörden und Organisationen aus dem kirchlichen und sozialen Bereich ausgenommen sind.

2. „Ohne überzeugende Gründe"

Der zweite Begründungsansatz des Gesetzesentwurfs knüpft daran an, dass es an überzeugenden Gründen für das Ermittlungs- und Gefahrenabwehrinstrument der Verkehrsdatenspeicherung fehle. Abgehoben wird damit erkennbar auf die in der langen rechtspolitischen Diskussion regelmäßig vorgetragene Behauptung, dass die Verkehrsdatenspeicherung keinen oder jedenfalls keinen hinreichenden Nutzen habe, der ihren Aufwand gerade auch gemessen am Grundsatz der Verhältnismäßigkeit rechtfertigen könne. Dementsprechend war und ist immer wieder zu lesen, dass retrograd zu erhebenden Verkehrsdaten in der Praxis der Strafverfolgungsorgane keine oder allenfalls geringe praktische Bedeutung zukomme. Auch seien schwerste Straftaten durch dieses Instrument nicht zu verhindern.[15] Hierzu wird als Referenz immer wieder auch ein Gutachten des Max-Planck-Instituts aus dem Jahre 2011 herangezogen.[16]

[15] Vgl. nur etwa https://www.t-online.de/digital/sicherheit/id_74154630/vorratsdatenspeicherung-in-deutschland-das-sollten-sie-wissen.html Beitrag vom 18. Oktober 2015.

[16] Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Max-Planck-Institut für ausländisches und internationales Strafrecht, Freiburg, 2. Aufl. 2011; vgl. zur berechtigten Kritik an Aussagekraft und Methodik des Gutachtens die Stellungnahme des Sachverständige Herrn Richter am Bundesgerichtshof Dr. Nikolaus *Berger* für die Anhörung im Ausschuss für Recht und Verbraucherschutz am Bundesgerichtshof Dr. Nikolaus *Berger* am 21. September 2015; abrufbar unter Bundestag.de.

Aus rechtspraktischer Sicht ist dieser Vermutung indes zu widersprechen. Die Verkehrsdaten sind als Ermittlungswerkzeug aus moderner und effektiver Kriminaltechnik und damit aus einer effektiven Verbrechensaufklärung nicht wegzudenken. Die nachstehende Darstellung soll daher zunächst beschreiben, welche Verkehrsdaten nach geltendem Recht durch die (privaten) Provider gespeichert und durch die Ermittlungsbehörden – allein auf richterliche Anordnung hin – von diesen abgefragt werden können (**a**). Sodann wird anhand von Beispielsfällen aus der Berufspraxis des *Verf.* die ermittlungstaktische Bedeutung der Verkehrsdaten für die Tataufklärung durch die Strafverfolgungsbehörden und für die Beweisführung der Strafgerichte beispielhaft dargestellt werden (**b**). Hierzu sollen die Sachverhalte und Tatvorwürfe mit groben Strichen skizziert und der Einsatz der Verkehrsdaten und seine Folgen für den Verfahrensausgang dargelegt werden. Die Darstellung erhebt freilich nicht den Anspruch einer umfassenden empirischen Untersuchung. Sie soll vielmehr anhand von konkreten Fällen aus der Praxis der Strafjustiz die Bedeutung von Verkehrsdaten für die Aufklärung schwerer Straftaten veranschaulichen.

a) Verkehrsdaten – Welche Informationen sind hiervon umfasst?

Klarstellend sei zunächst nochmals erwähnt, dass durch die Speicherung von Verkehrsdaten keine inhaltliche Aufzeichnung der Telekommunikation erfasst wird. Dies bringt nicht zuletzt § 113b Abs. 5 TKG zum Ausdruck. Eine inhaltliche Überwachung der Telekommunikation wird abschließend in §§ 100a, 100b StPO geregelt und ist nicht Gegenstand der Verkehrsdaten. Die Verkehrsdaten werden danach unterschieden, ob sie die Kennung, den Standort oder den Zeitpunkt der genutzten Geräte betreffen und ob hierbei das angerufene und anrufende Gerät von Relevanz sind.

aa) Kennung

In Hinblick auf die Kennung kann zwischen Festnetz- und Mobilfunkanschlüssen sowie der Nutzung des Internets unterschieden werden. Bei Festnetzanschlüssen wird die Rufnummer gespeichert. Bei Nutzung von Mobilfunkgeräten sind die internationale Kennung oder eine andere Kennung (IMSI – International Mobile Subscriber Identity) und die internationale Gerätekennung erfasst (IMEI – International Mobile Station Equipment Identity). Dies gilt auch für die Übermittlung von Kurznachrichten (SMS –

Short Message Service) und Multimedianachrichten (MMS – Multimedia Messaging Service). Für das Internet werden die Internetprotokoll-Adresse (IP-Adresse) sowie die jeweils zugewiesene Benutzerkennung erfasst.

bb) Standort

Die Standortdaten sind nur bei Mobilfunkgeräten (einschließlich Internet) und öffentlich zugänglichen Internetzugangsdiensten von Relevanz. Dabei sind die Funkzelle und die Funkantenne (Sendemast) erfasst. Eine Funkzelle ist der Bereich, in dem das von einer Sendeeinrichtung eines Mobilfunknetzes gesendete Signal empfangen und fehlerfrei decodiert werden kann (Cell-ID). Über die Abfrage der Funkzelle kann damit eine geographische Zuordnung des genutzten Gerätes erfolgen. Die Funkzellen sind unterschiedlich groß und werden auf Grundlage der von den Netzbetreibern zur Verfügung gestellten Daten durch die Ermittlungsbehörden vermessen. Für eine genauere Zuordnung ist die Auswertung des jeweiligen Funkmasts erforderlich.

cc) Zeitpunkt

Ferner sollen das Datum und die Uhrzeit der jeweiligen Zeitzone sowie Beginn und Ende der Verbindungen erhoben werden.

b) Einblick in die Ermittlungspraxis deutscher Strafverfolgungsbehörden

aa) Verfahrensbeispiele

Nachstehend werden Strafverfahren aus verschiedenen Deliktsbereichen und die jeweilige Bedeutung der Verkehrsdaten als Ermittlungsansatz und/oder als Beweistatsache für die Beweiswürdigung dargestellt. Es handelt sich nicht um systematisch erhobene oder ganz außergewöhnliche Fälle, sondern um alltägliche Strafverfahren, mit denen die Staatsanwaltschaften der Länder und die Landgerichte regelmäßig befasst sind. Zur Vermeidung von Wiederholungen nimmt der *Verf*. hier ergänzend Bezug auf die Stellungnahme des durch den Ausschuss für Recht und Verbraucherschutz im Zuge des Gesetzgebungsverfahrens zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten angehörten Sachverständigen Richter am Bundesgerichtshof Dr. Nikolaus *Berger* vom 21. September 2015.[17] Der Sachverständige

[17] Abrufbar unter Bundestag.de.

hat aus seiner Praxis am Bundesgerichtshof eine beeindruckende Vielzahl an Verfahren zusammengestellt, in denen Verkehrsdaten als Ermittlungsansatz oder aber als Beweismittel eine zentrale Rolle bei der Verbrechensaufklärung gespielt haben und/oder die deshalb ihre Bedeutung in besonderer Weise erhellen. Der *Verf*. war an der damals durchgeführten Erhebung auf Landesebene beteiligt.

Ergänzend hierzu an dieser Stelle nur beispielhaft Folgendes:

(1) Staatsschutzstrafrecht

Verfahrensgegenstand: Der Beschuldigte soll sich ab März 2014 dem sogenannten „Islamischen Staat“ angeschlossen haben. In der Folgezeit soll er durch ihn ausgebildet worden sein und an Kampfhandlungen der Vereinigung – auch etwa bewaffnet mit AK 47 oder Panzerfäusten – teilgenommen haben. Nach seiner Einreise in das Bundesgebiet und während des laufenden Asylverfahrens lebt er in Norddeutschland.

Beweisrechtliche Bedeutung von Verkehrsdaten: Nachdem sich gegen den Beschuldigten Anhaltspunkte im Sinne eines Anfangsverdachts (§ 152 StPO) für die Mitgliedschaft des Beschuldigten in einer ausländischen terroristischen Vereinigung (§ 129b StGB) ergeben hatten, ist – neben weiteren Abklärungen – für die Strafverfolgungsbehörden in diesem aktuell noch laufenden Ermittlungsverfahren von Bedeutung, zu wem der Beschuldigte gerade auch in der zurückliegenden Zeit über den auf ihn registrierten Anschluss Kontakte unterhält. Hieraus können sich Anhaltspunkte für die Aufklärung des Schuldgehalts ergeben, namentlich durch den Abgleich mit weiteren bereits vorliegenden Erkenntnissen zu möglichen Mitgliedern der Vereinigung sowie – etwa mit Blick auf einen naheliegenden Austausch von Bildmaterial untereinander – Anknüpfungspunkte für weitere Erkenntnisse über die Beteiligung an kämpferischen Aktivitäten der Vereinigung.

(2) Bandenkriminalität

Verfahrensgegenstand: Die Angeklagten sind rechtskräftig unter anderem wegen schweren Bandendiebstahls in mehreren Fällen (§ 244 Abs. 1 StGB) sowie wegen vorsätzlichen unerlaubten Ausübens der tatsächlichen Gewalt über eine Kriegswaffe zu mehrjährigen Gesamtfreiheitsstrafen verurteilt worden. Sie hatten sich zusammengeschlossen, um gewerbsmäßig und gemeinschaftlich in Geschäftsräume in Hamburg

und Umgebung einzubrechen. Hierbei gingen sie arbeitsteilig vor (einige Täter nahmen die Einbrüche vor, andere sicherten die Umgebung ab), waren am Tatort maskiert und entfernten sich mit der Beute unter Einsatz eines Sattelschleppers. Hierbei entstand jeweils erheblicher Schaden von bis zu 250.000 Euro.

Beweisrechtliche Bedeutung von Verbindungsdaten: Die Überwachungskameras des geschädigten Betriebes zeichneten zwar das Tatgeschehen auf. Eine Täteridentifikation war anhand dessen aber wegen Maskierung der Täter nicht möglich. Erkennbar war auf dem Videofilm indes, dass die Täter während der Tatbegehung mehrfach und auch länger telefonierten. Vor diesem Hintergrund wurde die Funkzelle des Tatorts ausgemessen und von den Providern die in der tatortrelevanten Funkzelle gespeicherten Verbindungsdaten auf richterliche Anordnung hin mitgeteilt. Anhand dieser Daten konnte ermittelt werden, dass sich am Tatort und in dessen unmittelbarer Umgebung im Zusammenhang mit der Tatbegehung vier Täter aufgehalten hatten, die untereinander in verschiedener Weise miteinander mehrfach in telefonischem Kontakt gestanden hatten. Ferner konnten die IMEI-Nummern festgestellt und anschließend ermittelt werden, mit welchen Rufnummern die Geräte nach Austausch von SIM-Karten im Zeitpunkt der Ermittlungen betrieben wurden. Hierdurch ließen sich die Identitäten der Täter aufklären; die dieserart überführten Angeklagten gestanden in der Hauptverhandlung die Taten überwiegend. Einer Darstellung des Beweisergebnisses der Verkehrsdaten bedurfte es in den schriftlichen Urteilsgründen mit Blick auf diese Geständnisse nicht.

(3) Betäubungsmittelhandel

Verfahrensgegenstand: Die Angeklagten sind rechtskräftig u.a. wegen unerlaubten Handeltreibens mit Betäubungsmitteln in nicht geringer Menge in mehreren Fällen zu mehrjährigen Freiheitsstrafen verurteilt worden (§ 29a BtMG).[18] Sie erwarben gemeinschaftlich insgesamt etwa 150 kg Marihuana in den Niederlanden und verbrachten das Rauschmittel sodann zum Zwecke des gewinnbringenden Verkaufs nach Hamburg und verkauften es dort weiter. Dabei gingen sie arbeitsteilig vor: Drei Täter waren an den Beschaffungsfahrten in den Niederlanden beteiligt, während ein weiterer Täter

[18] Az. 6004 Js 232/10.

jeweils die Abwicklung und Organisation von Hamburg aus übernommen hatte. Zur Abstimmung untereinander griffen sie maßgeblich auf Telekommunikationsmittel zurück, wobei verschiedene SIM-Karten mit niederländischen und deutschen Rufnummern sowie verschiedene Endgeräte eingesetzt wurden.

Beweisrechtliche Bedeutung von Verbindungsdaten: Die Angeklagten haben auch vor Gericht zur Tat keine Angaben gemacht. Im Zuge der Ermittlungen wie auch im gerichtlichen Verfahren kam den Erkenntnissen aus den Verkehrsdaten deshalb zentrale Bedeutung zu. Zunächst ließ sich für die Rufnummer, die auf Grund von Überwachungsmaßnahmen nach § 100a StPO einem konkreten Beschuldigten zugeordnet werden konnte, mit Hilfe von in den Niederlanden im Wege der Rechtshilfe erhobenen Standortdaten nachweisen, dass sich der Nutzer des Telefons zu den fraglichen Zeiten (der Beschaffungsfahrten) jeweils in den Niederlanden aufgehalten hatte. Weiter war anhand der in Deutschland für die den Angeklagten zugeschriebenen Mobilfunkanschlüsse ein Rückschluss auf ihre Abwesenheit vom Bundesgebiet möglich. Denn während der Zeiträume der vorgeworfenen Beschaffungsfahrten ließen sich keine Daten im deutschen Mobilfunknetz feststellen. Dies korrespondierte mit einer Abrede, die im Zuge der Gesprächsüberwachung – nach § 100a StPO – mitgeschnitten worden war. Hiernach war zwischen ihnen vereinbart worden, ihre Mobiltelefone während der Beschaffungsfahrten auszuschalten und in Hamburg zu belassen. Für frühere Zeiträume und dort naheliegend durchgeführte Beschaffungsfahrten konnte auf Verkehrsdaten der von den Angeklagten in Deutschland verwendeten Mobiltelefone nicht mehr zurückgegriffen werden. Der Nachweis der Fahrten erfolgte für zwei Beschuldigte insoweit anhand der Daten über die Anmietung von Kraftfahrzeugen. Einem weiteren Angeklagten, der in den anderen Fällen an der Beschaffung in den Niederlanden beteiligt gewesen war, konnte indes eine Fahrtbeteiligung nicht nachgewiesen werden. Eine Fahrzeuganmietung durch ihn erfolgte in diesem Fall nicht. Deutsche Verkehrsdaten, die eine Nutzung der diesem Beschuldigten durch Telekommunikationsüberwachung zugeordneten Mobilfunknummern und Rufnummern ermöglichen könnten, waren für diesen nicht mehr zu erlangen.

(4) Besonders schwerer Raub

Verfahrensgegenstand: Angeklagt war ein besonders schwerer Raub (§ 249 Abs. 1, § 250 Abs. 2 Nr. 1, § 25 Abs. 2 StGB).[19] Die Angeklagten sollen den Geschädigten aufgefordert haben, sein Mobiltelefon herauszugeben, und – als dieser sich weigerte – diesem sodann mit einer Flasche derart auf den Kopf geschlagen haben, dass der Geschädigte bewusstlos zu Boden stürzte. Anschließend sollen die Angeklagten ihm das Mobiltelefon entwendet und es noch am selben Tage veräußert haben.

Beweisrechtliche Bedeutung von Verbindungsdaten: Die Angeklagten schwiegen im Ermittlungsverfahren. Der hinreichende Tatverdacht wurde gestützt auf die Aussage einer Zeugin, die das Mobiltelefon wenige Stunden später von den Angeklagten zum Kauf angeboten bekommen und es nach Erwerb noch in derselben Nacht verschenkt haben soll. Bei diesem beschenkten Zeugen konnte die Tatbeute schließlich im Rahmen einer Durchsuchung aufgefunden werden. Diese Zeugenaussage wurde bestätigt durch die Verkehrsdaten. Mit Hilfe der Gerätenummer (IMEI-Nummer) des gestohlenen Mobiltelefons konnte ermittelt werden, dass der beschenkte Zeuge das dem Geschädigten entwendete Mobiltelefon mit seiner eigenen SIM-Karte betrieben hatte.

(5) Besonders schwere räuberische Erpressung - „mobile.de“

Verfahrensgegenstand: Dem Angeklagten lag eine schwere räuberische Erpressung zur Last (§§ 253, 255, 250 Abs. 2 Nr. 1 StGB). Er soll ein Scheinangebot über den Verkauf eines Kraftfahrzeugs auf einer Internetplattform zum Preis von 40.000 Euro eingestellt, sich telefonisch mit einem Interessenten über den Verkauf geeinigt und sich mit diesem und dessen Lebensgefährtin verabredet haben. Am abgelegenen Treffpunkt soll der Angeklagte dem Käufer einen Revolver an den Kopf gehalten, Bargeld in Höhe von 40.000 Euro verlangt und für den Fall einer Weigerung mit dem Erschießen des Geschädigten sowie dessen Lebensgefährtin gedroht haben. Der Geschädigte soll sodann das Bargeld übergeben haben.

Beweisrechtliche Bedeutung von Verbindungsdaten: Noch am Tatabend eingeleitete Fahndungsmaßnahmen blieben erfolglos. Eine Identifizierung des Angeklagten

[19] Az. 3411 Js 497/14.

als Täter gelang erst neun Monate später auf Grund eines Hinweises nach Veröffentlichung des Tatgeschehens und eines Phantombildes bei der Sendung „Aktenzeichen XY“. Dieser Hinweis wurde durch die erhobenen Verkehrsdaten bestätigt. Denn anhand der Verkehrsdaten zu der vom Täter gegenüber dem Geschädigten angegebenen Rufnummer konnte ermittelt werden, wo sich der Nutzer vor der Tat aufgehalten hatte. Dies war überwiegend ein Bereich im Osten Hamburgs in der Nähe zur Wohnanschrift des Angeklagten, auf den die Zeugenhinweise abzielten.

(6) Schwerer Raub bei Widerstandsunfähiger

Verfahrensgegenstand: Die Anklage legte den Angeklagten einen gemeinschaftlich begangenen schweren Raub zur Last (§ 249 Abs. 1, § 250 Abs. 1 Nr. 1 b, § 25 Abs. 2, §§ 27, 52 StGB). Sie sollen auf Grundlage eines gemeinsamen Tatplans an der Tür der bettlägerigen älteren Zeugin geklingelt haben. Sodann soll einer der Täter nach Öffnen der Tür durch die Angestellte eines Pflegedienstes dieser eine Hand auf den Mund gedrückt haben, um diese am Schreien zu hindern, sie sodann in das Innere der Wohnung gedrängt und sie nach Bargeld befragt haben. Dann soll die Zeugin gefesselt und mit einem Handtuch geknebelt worden sein. Die Täter sollen mit Bargeld geflüchtet sein und die Geschädigte in gefesseltem Zustand zurückgelassen haben.

Beweisrechtliche Bedeutung von Verbindungsdaten: Die schweigenden Angeklagten – die persönliche Kontakte zum Pflegedienst unterhielten – wurden erheblich belastet durch die Ergebnisse der Verkehrsdatenauswertung ihrer Mobiltelefone. Hiernach sollen zwischen ihnen insbesondere zur Tatzeit und unmittelbar danach mehrere Telefonate geführt worden sein. Überdies zeigte die Geovisualisierung der Verbindungsdaten – eine graphische Aufbereitung der verschiedenen Standorte von Funkzellen, in denen die Mobilfunkanschlüsse eingeloggt waren –, dass sich ein Angeklagter zur Tatzeit in unmittelbarer Nähe des Tatorts aufgehalten hat.

(7) Betrug – „Enkeltrick“

Verfahrensgegenstand: Der Angeklagte ist rechtskräftig wegen banden- und gewerbsmäßig begangener Betrugstaten in der Begehungsweise eines „Enkeltricks“ in mehreren Fällen verurteilt (§ 263 Abs. 1, Abs. 3 Nr. 1 und Abs. 5, §§ 25 Abs. 2, 53 StGB). Insgesamt hat die Bande auf diese Weise knapp 70.000 Euro erbeutet. Der

Angeklagte reiste jeweils aus seiner Heimat Litauen in das Bundesgebiet ein, um hier in Umsetzung des Tatplans die Bargelder in den Wohnungen der Geschädigten abzuholen.

Beweisrechtliche Bedeutung von Verbindungsdaten: In dem zunächst gegen unbekannt geführten Verfahren konnten durch Auswertung der Funkzellendaten deutsche und litauische Rufnummern ermittelt werden, die im Zusammenhang mit den Taten standen. Hinsichtlich dieser Nummern und den dazugehörigen IMEI-Nummern wurde die Herausgabe der Verkehrsdaten angeordnet. Aus diesen Daten ergab sich, dass sich der Nutzer der litauischen Rufnummer im Ausland befand und eine Vielzahl von Gesprächen mit einer deutschen Mobilfunknummer führte, wobei der Standort des Nutzers dieser Rufnummer durch dessen Geodaten innerhalb Deutschlands festgestellt werden konnte. Anhand dessen gelang namentlich der Nachweis, dass sich der Angeklagte zu den jeweiligen Tatzeiten jeweils in Tatortnähe aufgehalten hatte.

(8) Räuberische Erpressung

Verfahrensgegenstand: Der Angeklagte ist rechtskräftig u.a. wegen versuchter räuberischer Erpressung zu einer mehrjährigen Gesamtfreiheitsstrafe verurteilt worden.[20] Zugrunde lagen den Tatvorwürfen per SMS an die Tatopfer übermittelte Drohungen, wie etwa:

> *„Sie haben unsere wahrnung ignorirt.. Ich habe die freundligkeit ihnen mitteilen ich habe Geld bekomen, ihnen Hand und Ohr abschneiden. Sie haben zwei Wochen sich einigen wegen U. mit anwahlt. kein wort an polizei oder klug, sonst sofort kugel in kopf. Deine letzte chance , danach du nie wieder gesund dein geld ausgeben. Allah dich bestrafen, du ungläubiger.“*

Beweisrechtliche Bedeutung von Verbindungsdaten: Der Angeklagte hat zunächst geschwiegen und sich später dahin eingelassen, dass jemand anderes diese Nachrichten versandt haben muss. Die Strafkammer sieht den Angeklagten – sachlichrechtlich durch den Bundesgerichtshof unbeanstandet – auf Grund folgender, maßgeblich auf die Verkehrsdaten gestützter beweiswürdigender Erwägungen als überführt an:

[20] Az. 6003 Js 21/13.

„(...) Der Angeklagte wird insbesondere belastet durch die ... Verbindungsdaten zu der Rufnummer 49176XXX, die mit dem Zeugen K. eingehend in der Hauptverhandlung erörtert wurden. Von dieser Rufnummer aus sind um 19:53 und um 20:04 Uhr die SMS an den Zeugen Ko. und den Zeugen Sch. versandt worden. Aus den Verbindungsdaten zu der genannten Rufnummer ergibt sich, dass die SMS von einem Endgerät mit der IMEI-Nummer 35151XXX versandt wurde. Diese IMEI-Nummer ist einem Mobiltelefon Nokia E72 zugeordnet. Das Gerät wurde ausweislich des Durchsuchungsberichts der Beamtin Schoe. vom 7. Mai 2013 nebst Sicherstellungsverzeichnis und Lichtbild des Mobiltelefons sowie der Angaben des Zeugen K. bei der Durchsuchung des Wohnhauses des Angeklagten in der H.- Straße 15 in G..., am 7. Mai 2013 ... sichergestellt. ... Das Mobiltelefon Nokia E 72 mit der IMEI-Nummer 35151XXX wurde auch vor und nach der Tat von dem Angeklagten genutzt. Das bestreitet der Angeklagte nicht. Die Zuordnung des Mobiltelefons zum Angeklagten wird bestätigt erstens durch den ausgelesenen SMS-Speicher des Geräts, dessen Auswertung nach Angaben des Zeugen K. ergeben hat, dass das Mobiltelefon vom Angeklagten genutzt wurde, insbesondere waren keine ausgehenden SMS gespeichert, die nicht von ihm herrührten...

Die SIM-Karte mit der Rufnummer 4917XXX und das Endgerät mit der IMEI-Nummer 35151XXX waren ... zum Zeitpunkt der Versendung der SMS an die Zeugen Ko. und Sch. nach dem mit dem Zeugen K. erörterten Ergebnis der Verkehrsdatenauswertung eingeloggt bei einer Funkzelle LAC 10109/ Cell-ID 26360 mit den Koordinaten N 53.5939, E 10.3903 des Providers O2, einem Funkturm im Bereich der Trittauer Heide östlich der Bundesstraße 404 und nördlich der Ortschaft K. Auch die russisch-sprachige Droh-SMS an den Zeugen Kh. wurde von dieser Funkzelle aus unter der Rufnummer 49176XXX versandt, eine IMEI-Nummer des für diese SMS verwendeten Endgerätes war insoweit zum Zeitpunkt der Verkehrsdatenabfrage nicht mehr gespeichert, da die IMEI vom Anbieter nach den vom Zeugen K. berichteten Ermittlungen (Auskunft der Firma Telefonica) bereits nach sieben Tagen gelöscht wurde. Diese Funkzelle deckt nach der Funkzellenausmessung des Landeskriminalamtes ... auch den Bereich H.Straße 15 in G.... im Übrigen weite Teile von G. und K...ab

Zur Tatzeit ... waren nach der mit dem Zeugen K. erörterten Auswertung der Verkehrsdaten und der Funkzellenabmessung in der H.-Straße in G. durch das Landeskriminalamt ... auch die anderen vom Angeklagten regelmäßig genutzten Mobilfunkgeräte in Funkzellen eingeloggt, die ebenfalls den Wohnort des Angeklagten abdecken. Hochwahrscheinlich befand sich der Angeklagte demnach zuhause, als die SMS versandt wurden, jedenfalls aber an einem Ort in der Nähe, von dem die SMS versandt worden sein könnten. Die grundsätzliche Nutzung der im Folgenden genannten Geräte und SIM-Karten und deren Zuordnung zu seiner Person hat der Angeklagte in der Hauptverhandlung bestätigt... Das iPad mit der IMEI-Nummer 01292XXX ... war im Laufe des Tattages bis 16:32 Uhr und dann wieder um 19:39 Uhr eingeloggt in der Funkzelle LAC Cell-ID 1022,25, Koordinaten N533706, E 102344, einem Funkturm in Trittau, der nach der Messung des LKA ... auch die Wohnanschrift des Angeklagten abdeckt. Das iPhone mit der IMEI-Nummer 0130XXX mit der zugehörigen SIM-Twin-Karte mit derselben Rufnummer 0172XXX war ab 19:43 Uhr teils in den genannten Funkturm in Trittau eingeloggt, teils in die Funkzelle des Providers Vodafone mit der Zellkennung LAC/Zell-ID 409/15001, einem Funkmast in Witzhave mit den

Koordinaten N53.565833, E10.339722, der nach der Funkzellenausmessung ... gleichfalls die Wohnanschrift des Angeklagten abdeckt. ... Ein weiteres iPhone mit der IMEI-Nummer 01265XXX und der SIM-Karte mit der Rufnummer 0172XXX war ab 19:03:22 Uhr eingeloggt in die Funkzelle in Witzhave."

(9) Besonders schwerer Raub – Freispruch

Verfahrensgegenstand: Der Angeklagte ist rechtskräftig vom Vorwurf des besonders schweren Raubes freigesprochen worden (§ 249 Abs. 1, § 250 Abs. 2 StGB).[21]

Beweisrechtliche Bedeutung von Verbindungsdaten: Der Angeklagte hat im Ermittlungsverfahren und vor der Strafkammer geschwiegen. Besondere Bedeutung kam in diesem „Indizienprozess" namentlich den erhobenen Verkehrsdaten betreffend den Mobilanschluss zu, von dem aus eine Pizzabestellung aufgegeben und mittels dessen der Lieferant in einen Hinterhalt gelockt worden war. Die Telefonnummer war als sog. Pre-Paid-Karte ausgegeben worden; die hierbei vom Käufer angegebenen Personalien erwiesen sich als fiktiv. Gleichwohl sprach zunächst alles für eine Nutzung des Anschlusses allein durch den Angeklagten, denn sämtliche im Wege der Verkehrsdatenerhebung gesicherte Verbindungen dieses Anschlusses in der Zeit vor der Tatbegehung wiesen Bezüge zum familiären Umfeld, den Eltern und Geschwistern, oder aber zum Freundeskreis des Angeklagten auf. Nur die Gesprächspartner vereinzelter Verbindungen ließen sich nicht mehr rekonstruieren. Der Schluss von diesen Verkehrsdaten auf die Täterschaft des Angeklagten konnte indes nur dann tragfähig sein, wenn mit der notwendigen Gewissheit auszuschließen war, dass jemand anderes Zugriff auf den Anschluss hatte. Bis zum letzten Hauptverhandlungstag schien sich dies durch das Ergebnis der Beweisaufnahme zu bestätigen. Einem im Rahmen des Schlussvortrags des Verteidigers gestellten Beweisantrag betreffend den Standort des Tathandys drei Tage vor der Tat kam die Strafkammer nach. Die Auswertung des Standortes zu diesem Zeitpunkt ergab, dass der Anschluss eingeloggt war in einer Funkzelle im nördlichen Schleswig-Holstein, nicht aber – was angesichts zahlreicher übereinstimmender und glaubhafter Zeugenaussagen zum Aufenthalt des Angeklagten an diesem Tage zu erwarten gewesen wäre – in Hamburg-Harburg. In den Urteilsgründen hat die Strafkammer Folgendes ausgeführt:

[21] Az. 4181 Js 1/12.

„Trotz dieser teilweise gewichtigen Beweiszeichen vermochte die Strafkammer letzte Zweifel an der Täterschaft des Angeklagten nicht zu überwinden. Diese betrafen die Frage, ob der Angeklagte die Mobilfunknummer zur Tatzeit auch selbst genutzt hat.

Zwar lag es mit Blick auf den längeren vorangegangenen Zeitraum, in dem der Angeklagte den Anschluss ersichtlich für sich genutzt hat, nicht etwa nahe, dass er den Anschluss in der Tatnacht Dritten zur Verfügung gestellt hat oder ihn gänzlich aufgegeben haben sollte. Auch deuteten die Verbindungs- und Standortdaten vom Tattage nicht auf einen anderen Nutzer hin. Das bestimmende Gewicht des Beweiszeichens „Nutzung des Tat-Mobiltelefons" wurde aber für die Strafkammer dadurch in Frage gestellt, dass zumindest für den 25. Dezember 2011 und damit drei Tage vor der Tatbegehung ein Dritter den Mobilfunkanschluss verwendet haben muss. Mehrere Zeugen, darunter die S., hatten glaubhaft angegeben, dass der Angeklagte an jenem Abend jedenfalls ab 21 Uhr bei den Eheleuten S. in Hamburg Musik gemacht hätte. Zur selben Zeit war der Mobilfunkanschluss allerdings eingeloggt in einer Funkzelle in Tarp/Schleswig-Holstein. Damit war durch die Strafkammer in der gebotenen Gesamtschau zu berücksichtigen, dass ein Dritter zumindest drei Tage vor der Tat Zugang zu diesem Anschluss hatte.

Dies schwächte das Beweiszeichen in ganz empfindlicher Weise. Denn es konnte nunmehr nicht sicher ausgeschlossen werden, dass ein Dritter möglicherweise auch am Tatabend Zugang zu dem Mobilfunkanschluss hatte. Diese Schwäche des Beweiszeichens war ferner zu Lesen vor dem Hintergrund, dass der Anschluss am Abend unmittelbar vor der Tat zumindest auch in Eidelstedt eingeloggt war. Dort wohnte die Freundin des H., die Zeugin P. Überdies war zu bedenken, dass gerade der tatverdächtige H. engen Kontakt zur Familie des Angeklagten hatte und daher zahlreiche Verbindungen des Tathandys auch auf Telefonate durch ihn zurückzuführen sein könnten.

Die Strafkammer vermochte deshalb auch nach umfassender Beweisaufnahme und Gesamtschau der vorliegenden Beweiszeichen letzte bestimmende Zweifel an der Täterschaft des Angeklagten nicht zu überwinden."

b) Zusammenfassende Überlegungen

Die vorstehend dargestellten Verfahrensskizzen zeigen auf, dass die Verkehrsdaten teilweise zum unmittelbaren Tatnachweis dienten. In der überwiegenden Anzahl der Fälle waren sie aber – wie aus Sicht des *Verf.* rechtspraktisch in der überwiegenden Anzahl der Verfahren – ein Hebel für weitere wesentliche Ermittlungsschritte. Sie lieferten auch Hinweise auf weitere Personen, die im unmittelbaren zeitlichen und örtlichen Zusammenhang mit der Tat im Kontakt zum Verdächtigen standen und können dieserart Täterstrukturen aufzuklären helfen. Ferner vermögen sie Schlüsse auf die Anwesenheit von Verdächtigen an bestimmten Orten zu bestimmten Zeiten zu tragen und deren Reisewege – etwa bei unerlaubter Drogeneinfuhr oder Schleuserhandlungen – oder gar Rückschlüsse durch die jeweils von einer Telefonnummer geführten

Gespräche auf den Nutzer eines Anschlusses nachvollziehbar zu belegen; dies alles, ohne dass hierbei auf Gesprächsinhalte zugegriffen wird. Die Verfahrensskizzen belegen ferner, dass den hierdurch gewonnenen Erkenntnissen nicht ausschließlich belastende Wirkung zukommen muss. Gerade bei dem Rückschluss auf den Nutzer eines Tattelefons ist einem Angeklagten möglich durch Verkehrsdaten entlastender Umstände – etwa gar in Form einer Alibibehauptung – vorzubringen.

c) Verfahrensrelevanz aus der Sicht anderer Dienststellen

Über die vorstehend beschriebenen Verfahren aus dem Alltag der Ermittlungsbehörden hinaus gibt es zahlreiche Kriminalitätsbereiche, in denen Verkehrsdaten wegen spezifischer Tatbegehungsweisen eine besondere Bedeutung zukommt („Enkeltrick"; „Autobahnschütze", dessen Standorte jeweils anhand Verbindungsdaten aufgeklärt werden konnten).

Betreffend die besondere ermittlungstaktische Bedeutung von IP-Adressen hat sich erst jüngst der Präsident des Bundeskriminalamtes geäußert: Hiernach hätten im Jahre 2017 trotz 8.400 Hinweisen auf Kinderpornografie die Ermittlungen eingestellt werden müssen, weil eine retrograde Abfrage von IP-Adressen derzeit mangels tatsächlicher Speicherungen durch die Internetdienstleister nicht möglich sei.[22] Die Verkehrsdaten sind nach Einschätzung weiterer Fachdienststellen geeignet, eine Aufklärung etwa auch in der Pyramide der Täter nach oben hin zu ermöglichen. Insbesondere sei eine erleichterte Aufklärung der Hintergründe und Ursprünge („Wer hat die Datei wann zuerst hochgeladen?") sowie – jedenfalls in Einzelfällen – die Ermittlung des Aufenthaltsortes eines abgebildeten Kindes möglich. Ferner wird mit Recht darauf hingewiesen, dass Verkehrsdaten gerade auch die Aufklärung von Tatserien erleichtern kann. So können etwa Kreuzvergleiche zwischen verschiedenen Funkzellen und unterschiedlichen Tatorten ergeben, dass jeweils dieselbe Nummer dort eingeloggt war. Gerade bei Serientaten dient deren Aufklärung nicht nur dem Strafverfolgungsinteresse, sondern sie beugt mit der Ermittlung und Verurteilung des Serientäters auch von ihm drohenden Wiederholungstaten vor.

[22] Pressemitteilung des BKA vom 6. Juni 2018.

Schließlich weist das BKA auch mit Recht darauf hin, dass – jenseits gefahrenabwehrrechtlicher Aspekte – die Strafverfolgung gerade auch terroristischer Straftaten, etwa solche von Mitgliedern des sog. „Islamischen Staats“, ohne Verkehrsdatenspeicherung deutlich erschwert oder gar unmöglich sei. Mit Hilfe dieser Daten können die Anrufziele der sich etwa in Syrien aufhaltenden Verdächtigen in Deutschland erhellt und hierdurch Erkenntnisse über die Strukturen und Beteiligtenkreise auch im Bundesgebiet gewonnen und namentlich die Urheber im Internet hochgeladener, verherrlichender Videos ermittelt werden.

V. Abschließende Bewertung

1. Die Verkehrsdatenspeicherung ist heute als Instrument zeitgemäßer strafrechtlicher Ermittlungen nicht wegzudenken und steht in ihrer kriminalistischen Bedeutung den Errungenschaften der Daktyloskopie gleich. Dies belegen neben Einblicken in die Strafrechtspraxis eindrucksvoll schon die seit langem festzustellenden exorbitanten Steigerungsraten hinsichtlich der Zahl der Telefonanschlüsse, vor allem aber auch der im Netz ausgetauschten Sprach- und Datenvolumina.[23] Das Kommunikationsverhalten der Menschen hat sich in den letzten Jahrzehnten grundlegend verändert;[24] damit geht erkennbar einher auch die Verwendung dieser Mittel für die Begehung schwerer und schwerster Straftaten sowie korrespondierend hiermit die Annahme eines erfolgversprechenden ermittlungstaktischen Anknüpfungspunkts für die Tataufklärung.

2. Die derzeit geltende Rechtslage stellt unter Beachtung bisheriger verfassungsgerichtlicher Maßgaben einen mit Augenmaß gestalteten Ausgleich zwischen der rechtsstaatlichen Pflicht auf eine zu gewährleistende effektive Strafverfolgung einerseits und einen streng begrenzten und strikten formellen Anforderungen unterworfenen Eingriff in die Freiheitsrechte der Bürger andererseits dar.

3. Die Verkehrsdaten werden nicht bei staatlichen Behörden gespeichert, sondern unter strengen Sicherheitsbedingungen bei privaten Telekommunikationsprovidern für die gesetzliche Höchstspeicherdauer vorgehalten. Entgegen einer weit verbreiteten

[23] Vgl. nur die Übersicht im Tätigkeitsbericht der Bundesnetzagentur aus dem Jahre 2016, S. 28.
[24] Vgl. bereits BT-Drucks. 16/5846, S. 38, 50 ff., 59.

Sorge ist allein mit der Speicherpflicht für die privaten Anbieter von Telekommunikationsdienstleistungen keine flächendeckende staatliche Überwachung aller Bürger verbunden.

4. Die kurzfristig gespeicherten Verkehrsdaten dürfen von den Strafverfolgungsbehörden nur zur Aufklärung schwerwiegender Straftaten und nur mit richterlicher Genehmigung abgerufen und verwendet werden. Die Hürden dafür sind ebenso hoch wie bei dem – freilich ungleich intensiveren – Eingriff durch eine Wohnraumüberwachung und damit sogar strenger als bei der – ebenfalls eingriffsintensiveren – Überwachung von Telefongesprächen.

5. Die derzeit ergebnisoffene verfassungsgerichtliche Bewertung sollte vor dem Hintergrund der ausdifferenzierten deutschen Regelungen abgewartet werden. Auch ist gerade mit Blick auf die Bedeutung des Ermittlungsinstruments sorgsam zu prüfen, ob und in welchem Umfang die Maßgaben der Rechtsprechung des *EuGH* Anlass zur einer – etwa teilweisen – Korrektur des geltenden Rechts geben. Eine dem vorgreifende – gar übereilte – vollständige Abschaffung des Ermittlungsinstruments wird der Verantwortung für eine effektive und verantwortungsvolle Strafrechtspflege nicht gerecht. Sie hat auch der *EuGH* nicht pauschal gefordert, sondern erkennbar weiterhin gesetzgeberischen Handlungsspielraum gesehen.

6. Eine Alternative zur Speicherung von Verkehrsdaten über einen begrenzten Zeitraum durch private Anbieter ist derzeit nicht ersichtlich. Bei einem Verzicht hierauf – auch unter Einführung eines vom Gesetzesentwurf indes nicht vorgesehenen sog. Quick-Freeze – hinge die erfolgreiche und öffentlich wahrnehmbare Verfolgung schwerster Straftaten von Zufälligkeiten, wie etwa der Sicherung und Auswertung von Tatortspuren, sowie von dem Umstand ab, welche Priorität die Ermittlungsbehörden dem jeweiligen Verfahren zuschreiben. Auch ist es etwa unvorhersehbar,

- wann eine Tat den Ermittlungsbehörden bekannt wird;
- wann eine Tat angezeigt wird;
- ob bei der Tatbegehung auch die Verwendung von Telekommunikationsdiensten bedeutsam war;
- welcher Telefonanschluss (Nummer, IMSI- oder IMEI-Nummer) hier von Bedeutung war.

Wird nach einer Vermisstenmeldung ein Tötungsdelikt zum Nachteil der vermisst gemeldeten Person erst Wochen später bekannt, so wäre deshalb bei fehlender Speicherpflicht von Verkehrsdaten dieser wichtige Ermittlungsansatz – namentlich die Feststellung anwesender Personen in der betreffenden Funkzelle – bei einem Kapitalverbrechen verloren.

7. Der Erforderlichkeit einer Verkehrsdatenspeicherung kann auch nicht entgegengehalten werden, dass sie zur Abwehr terroristischer Gewalttaten ungeeignet sei und dies durch bereits erfolgte Terroranschläge auch in Deutschland belegt werde. Freilich: Die strafprozessuale Abrufbefugnis von Verkehrsdaten kann einen Anschlag zwar nicht verhindern; dies schaffen andere repressive und eben nicht gefahrenabwehrrechtliche Ermittlungsinstrumente, wie etwa Wohnraumdurchsuchungen, jedoch ebenfalls nicht. Ermöglicht werden aber eine Aufhellung des Täterumfelds und der Täterbewegungen, ihrer Kontaktpersonen und Unterstützer sowie in diesem Umfang auch die Verhinderung von Wiederholungstaten. Indem Unterstützer ermittelt und strafrechtlich verfolgt werden, wird nicht nur generalpräventiv auch terroristischen Straftaten vorgebeugt, sondern effektiv gerade auch islamistischer Terrorismus durch das Strafrecht bekämpft.

Prof. Dr. Ferdinand Wollenschläger

Schriftliche Stellungnahme

Öffentliche Anhörung

des Ausschusses für Recht und Verbraucherschutz

des Deutschen Bundestages

zum

Gesetzentwurf

der Abgeordneten Christian Lindner u.a. und der Fraktion der FDP

Entwurf eines Gesetzes zur Stärkung der Bürgerrechte

(Bürgerrechtestärkungs-Gesetz – BüStärG)

BT-Drs. 19/204

am 13. Juni 2018

Inhaltsübersicht

I. Zusammenfassende Gesamtbewertung

Die im zu begutachtenden Gesetzentwurf vorgesehene (vollständige) Aufhebung der TK-Verkehrsdatenspeicherung ist – in Einklang mit der Rechtsprechung sowohl des Bundesverfassungsgerichts (BVerfG) als auch des Europäischen Gerichtshofs (EuGH) – weder verfassungs- noch europarechtlich geboten. Darüber hinaus ist es trotz der strengen EuGH-Rechtsprechung unions(grund)rechtlich vertretbar, an der aktuellen Regelung im Telekommunikationsgesetz mit seinem Konzept einer restriktiven allgemeinen TK-Verkehrsdatenspeicherung – unter Inkaufnahme eines Prozessrisikos – festzuhalten.

Eine Speicherpflicht für Verkehrsdaten stellt, wie bereits in meiner Stellungnahme zum ursprünglichen Gesetzentwurf (siehe Anlage) ausgeführt, 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 BVerfG die grundrechtlich und rechtsstaatlich fundierte Pflicht, eine effektive Strafverfolgung sicherzustellen und Individualrechtsgüter vor Beeinträchtigungen durch Dritte zu schützen; auch die EU-Grundrechte-Charta kennt ein Recht auf Sicherheit (Art. 6 GRC).

Das **BVerfG** hat vor diesem Hintergrund 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 gesetzliche Regelung **wahrt** nicht nur **die verfassungsrechtlichen Grundsatzanforderungen** (näher Anlage, II.); vielmehr schöpft sie den vom Grundgesetz belassenen Gestaltungsspielraum des Gesetzgebers nicht aus (namentlich Höchstspeicherfrist; erfasste Verkehrsdaten; Verwendungszwecke). Daher ist der **Forderung** des hier zu begutachtenden Gesetzentwurfs, die **TK-Verkehrsdatenspeicherung wegen ihrer Verfassungswidrigkeit abzuschaffen**, **nicht zu folgen**.

Ebenso wenig zu folgen ist der **Forderung des** vorliegenden **Gesetzentwurfs**, die **TK-Verkehrsdatenspeicherung wegen ihrer Europarechtswidrigkeit aufzuheben**. Denn – unabhängig davon, welche Grenzen man der Rechtsprechung des EuGH entnimmt – hat dieser in seinem Tele2-Urteil vom 21.12.2016 anerkannt, dass eine auf das absolut Notwendige beschränkte TK-Verkehrsdatenspeicherung zulässig ist. **Ob** überdies **europarechtlich** eine **Modifikation** der im TKG normierten Pflicht zur Speicherung von TK-Verkehrsdaten **geboten** ist, hängt namentlich von der vielschichtigen Beantwortung der Frage ab, ob das Unionsrecht eine hinsichtlich des von ihr erfassten Personenkreises allgemeine TK-Verkehrsdatenspeicherung verbietet und nur eine Speicherung von Daten solcher Personenkreise zulässt, die in einem zumindest mittelbaren – etwa geographischen – Bezug zu Gefahren respektive Straftaten stehen.

Entscheidend hierfür ist auch aus unionsrechtlicher Warte eine Abwägung der widerstreitenden Grundrechte auf Freiheit (Art. 7, 8 und 11 GRC) und Sicherheit (Art. 6 GRC). Wie schon die Wertungen des Urteils des BVerfG vom 2.3.2010 sowie der ergangenen Eil-entscheidungen zum aktuellen TKG illustrieren, lässt sich, abstrakt betrachtet, eine **allgemeine TK-Verkehrsdatenspeicherung** als auch **unions(grund)rechtskonform** ansehen.

Auch die **aktuelle EuGH-Rechtsprechung zwingt zu keiner Modifikation des TKG**. **Erstens** lässt sich aus der Unvereinbarkeit bestimmter Regelungen (anderer Normgeber) der TK-Verkehrsdatenspeicherung nach den Urteilen des EuGH vom 8.4.2014 (Rs. Digital Rights) und vom 21.12.2016 (Rs. Tele2 u.a.) nicht auf die Unions(grund)rechtswidrigkeit der im TKG vorgesehenen allgemeinen TK-Verkehrsdatenspeicherung schließen. Zwar hat der EuGH die Allgemeinheit des erfassten Personenkreises besonders problematisiert; allerdings erweist sich die deutsche Regelung im Übrigen als deutlich grundrechtsschonender als die streitgegenständlichen Regelungen, was bei der für das TKG anzustellenden Gesamtabwägung zu berücksichtigen ist (TKG: nach Datenart differenzierte Speicherdauer; keine Speicherung von Daten von Diensten der elektronischen Post und von besonderer Vertraulichkeit unterliegender Verbindungen; kurze Speicherfrist von lediglich vier bzw. zehn Wochen und nicht von sechs Monaten). **Zweitens** stellen die allgemeinen Ausführungen des EuGH zur Zulässigkeit nationaler Regelungen der TK-Verkehrsdatenspeicherung im Tele2-Urteil (Rn. 108 ff.), aus denen sich die Unions(grund)rechtswidrigkeit der allgemeinen TK-Verkehrsdatenspeicherung ableiten lässt, lediglich ein Obiter Dictum dar, das keine Pflicht des deutschen Gesetzgebers zur Modifikation des TKG begründet; zudem verbleibt eine Restunsicherheit hinsichtlich des abschließenden Charakters dieser Urteilspassage.

Unabhängig davon sollte die restriktive Rechtsprechung des das Unionsrecht letztverbindlich auslegenden EuGH Anlass zur erneuten **Reflexion** der TKG-Regelungen geben. Insoweit ist es vor dem skizzierten Hintergrund **unions(grund)rechtlich vertretbar**, **am aktuellen TKG mit seinem Konzept einer restriktiven allgemeinen TK-Verkehrsdatenspeicherung festzuhalten** und eine erneute Entscheidung des EuGH abzuwarten, zumal der EuGH in seinem Gutachten zur Fluggastdatenspeicherung vom 26.7.2017 kein generelles unions(grund)rechtliches Verbot einer allgemeinen Vorratsdatenspeicherung angenommen hat, worin eine Lockerung gegenüber der Tele2-Entscheidung zu sehen ist. Freilich verbleibt das nicht zu vernachlässigende **Prozessrisiko**, dass der EuGH in einem späteren Verfahren das Obiter Dictum als abschließend bestätigt und die Unionsrechtswidrigkeit der deutschen Regelung feststellt.

II. Europarechtliches Verbot einer allgemeinen TK-Verkehrsdatenspeicherung?

Europarechtliche Handlungspflichten für den deutschen Gesetzgeber bestehen, wenn das Unionsrecht in seiner für den deutschen Gesetzgeber verbindlichen Auslegung durch den EuGH eine allgemeine TK-Verkehrsdatenspeicherung verbietet und nur eine Speicherung von Daten solcher Personenkreise zulässt, die in einem zumindest mittelbaren – etwa geographischen – Bezug zu Gefahren respektive Straftaten stehen.

Einleitend sei festgehalten, dass sich die europarechtliche Bewertung des Gesetzentwurfs als komplex erweist, da verschiedene Aspekte auseinandergehalten werden müssen, nämlich die Anwendbarkeit des Unionsrechts einschließlich der Unionsgrundrechte auf nationale Regelungen der TK-Verkehrsdatenspeicherung, die vom jeweiligen Grundrechtsinterpreten für richtig erachtete Auslegung des Unionsrechts insoweit, der Inhalt der einschlägigen Entscheidungen des EuGH sowie deren Bindungswirkung für den deutschen Gesetzgeber.

Dieser Abschnitt legt dar, dass nach dem Tele2-Urteil des EuGH nationale Regelungen der TK-Verkehrsdatenspeicherung dem Unionsrecht und damit auch den Unionsgrundrechten unterliegen – eine Entscheidung, die mit guten Gründen bezweifelt werden kann, wobei der Anwendungsbereich des Unionsrechts mit Ablauf der Umsetzungsfrist der Datenschutz-Richtlinie (EU) 2016/680 am 6.5.2018 eine Erweiterung erfahren hat (1.). Wie bereits die Wertungen der Rechtsprechung des BVerfG zeigen, lässt sich eine allgemeine TK-Verkehrsdatenspeicherung, abstrakt betrachtet, als unions(grund)rechtskonform ansehen (2.). Hinsichtlich der Positionierung des EuGH in dieser Frage ist zunächst festzuhalten, dass die Beantwortung der Vorabentscheidungsersuchen in den Urteilen des EuGH vom 8.4.2014 in der Rs. Digital Rights (3.) und vom 21.12.2016 in der Rs. Tele2 u.a. (4.a) keine Pflicht des deutschen Gesetzgebers zur Aufhebung der TK-Verkehrsdatenspeicherung zu begründen vermag, da das deutsche Recht weniger stark in Grundrechte eingreift als die streitgegenständlichen Regelungen und die Aussagen des Urteils somit nicht unbesehen auf die deutsche Rechtslage übertragen werden können. Auch die allgemeinen Ausführungen des EuGH zur Zulässigkeit nationaler Regelungen der TK-Verkehrsdatenspeicherung im Tele2-Urteil (Rn. 108 ff.), die als Beleg für die Unions(grund)rechtswidrigkeit der allgemeinen TK-Verkehrsdatenspeicherung im TKG herangezogen werden, stellen lediglich ein Obiter Dictum dar, das keine Pflicht des deutschen Gesetzgebers zur Modifikation des TKG begründet; zudem verbleibt eine Restunsicherheit hinsichtlich des abschließenden Charakters dieser Passage (4.b). In seinem Gutachten vom 26.7.2017 zum Fluggastdatenabkommen mit Kanada hat der EuGH überdies einem generellen unionsrechtlichen Verbot der Vorratsdatenspeicherung eine Absage erteilt (5.). Unabhängig davon, wie man den Inhalt des

Tele2-Urteils und dessen rechtlichen Konsequenzen für den deutschen Gesetzgeber bewertet, ist hinsichtlich des hier zu begutachtenden Gesetzentwurfs schließlich festzuhalten, dass dieser mit seiner vollständigen Aufhebung der Regelungen der TK-Verkehrsdatenspeicherung über das unionsrechtlich Gebotene hinausgeht (6.).

1. Anwendbarkeit der Unionsgrundrechte und des Unionsrechts

Gemäß Art. 51 Abs. 1 S. 1 GRCh bindet die Grundrechtecharta die Mitgliedstaaten der Europäischen Union ausschließlich bei der Durchführung des Rechts der Union.[1] Während nationale Regelungen, die eine EU-Richtlinie wie die frühere Vorratsdatenspeicherungs-Richtlinie 2006/24/EG umsetzen, ohne Weiteres derartige, einer EU-Grundrechtsbindung unterliegende Durchführungsvorschriften darstellen, stellt sich die Frage, ob hiervon auch nach Ungültigerklärung der Richtlinie 2006/24/EG durch den EuGH[2] und damit in Ermangelung einer unionsrechtlichen Regelung der TK-Verkehrsdatenspeicherung noch die Rede sein kann. Der EuGH hat dies in seinem Urteil vom 21.12.2016 in der Rs. Tele2 u.a. angenommen. Denn für die Bejahung einer Durchführung von Unionsrecht genüge der durch die E-Privacy-Richtlinie 2002/58/EG gezogenen Rahmen für nationale Speicherpflichten von TK-Verkehrsdaten (Rn. 64 ff.), obgleich diese Richtlinie gemäß ihres Art. 1 Abs. 3 „auf keinen Fall für Tätigkeiten betreffend die öffentliche Sicherheit … und die Tätigkeiten des Staates im strafrechtlichen Bereich“ gilt.

Ob diese Annahme des Tele2-Urteils zutrifft, lässt sich, wie bereits in meiner Stellungnahme zum ursprünglichen Gesetzentwurf (siehe Anlage, III.1.) und andernorts[3] ausgeführt, mit guten Gründen bezweifeln. Es erscheint vielmehr vorzugswürdig, Art. 15 Abs. 1 E-Privacy-Richtlinie 2002/58/EG als klarstellende, keine Grundrechtsbindung der Mitgliedstaaten nach sich ziehende Öffnungsklausel zu verstehen.[4]

Ob im Zuge der aktuellen Reform der E-Privacy-Richtlinie[5] für die Unions(grund)rechtsbindung relevante Änderungen an diesem Rechtsrahmen erfolgen, bleibt abzuwarten. Ebenfalls

---

[1] Zur Bindung der Mitgliedstaaten an die EU-Grundrechte *F. Wollenschläger*, Grundrechtsschutz und Unionsbürgerschaft, in: Hatje/Müller-Graff (Hrsg.), Enzyklopädie Europarecht I, 2014, § 8 Rn. 16 ff.

[2] EuGH, verb. Rs. C-293/12 und C-594/12, ECLI:EU:C:2014:238, Rn. 71 – Digital Rights.

[3] *F. Wollenschläger/L. Krönke*, NJW 2016, S. 906. Siehe auch *X. Brechot*, Revue de l'Union Européenne 2017, S. 178 (182 f.); *W. Ziebarth*, ZUM 2017, S. 398 (403 f.).

[4] Näher *F. Wollenschläger/L. Krönke*, NJW 2016, S. 906 (908). Siehe auch *X. Brechot*, Revue de l'Union Européenne 2017, S. 178 (182 f.).

[5] Siehe den Vorschlag der Europäischen Kommission für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und

abzuwarten bleibt, ob und wie sich das BVerfG im anhängigen Verfassungsbeschwerdeverfahren hinsichtlich der TK-Verkehrsdatenspeicherung zur Frage der Bindung an die Unionsgrundrechte positioniert.[6] In seinem Urteil zur Anti-Terror-Datei vom 24.4.2013 ist es einer zu weitgehenden Bindung der Mitgliedstaaten an die EU-Grundrechte mit deutlichen Worten entgegengetreten;[7] Stimmen im Schrifttum weisen dementsprechend auf die Möglichkeit einer Ultra-vires-Kontrolle hin[8].

In den Eilentscheidungen zur aktuellen TK-Verkehrsdatenspeicherung hat das BVerfG die Bedeutung der Unionsgrundrechte offen gelassen:

> Ob und gegebenenfalls in welcher Weise die Europäische Grundrechtecharta oder sonstiges Unionsrecht für die Beurteilung der angegriffenen Vorschriften Bedeutung entfaltet, ist im Hauptsacheverfahren zu entscheiden. Dass Unionsrecht dazu verpflichten könnte, die angegriffenen Vorschriften schon im Eilverfahren im Wege der einstweiligen Anordnung außer Kraft zu setzen, ist weder substanziiert vorgetragen noch ersichtlich.[9]

Schließlich gilt es festzuhalten, dass, auch wenn man dem Tele2-Urteil hinsichtlich der Anwendbarkeit des Unionsrechts nicht folgt, seit Ablauf der Umsetzungsfrist der Richtlinie (EU) 2016/680 (zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr), d.h. seit dem 6.5.2018, jedenfalls der Zugriff auf die Daten durch entsprechende Behörden (siehe Art. 3 Nr. 7 Richtlinie 2016/680/EU) zu den genannten Zwecken (Art. 2 Richtlinie 2016/680/EU) in den Anwendungsbereich des Unionsrechts i.S.d. Art. 51 Abs. 1 GRC fällt. Das Verhältnis dieser Richtlinie zur E-Privacy-Richtlinie ist freilich ungeklärt und anders als in der Datenschutz-Grundverordnung (EU) 2016/679 nicht ausdrücklich geregelt [siehe Art. 95 Verordnung (EU) 2016/679]. Im Tele2-Urteil hat der EuGH auch den Zugriff auf die Daten der E-Privacy-Richtlinie unterstellt (Rn. 76 f.), so dass nunmehr jedenfalls insoweit ein überschneidender Anwendungsbereich besteht und sich die Frage der (Neu-)Abgrenzung stellt.

2. Unions(grund)rechtskonformität der TK-Verkehrsdatenspeicherung

Die TK-Verkehrsdatenspeicherung stellt einen Eingriff in Art. 7 (Achtung des Privatlebens), Art. 8 (Schutz personenbezogener Daten) und Art. 11 (Recht auf freie Meinungsäußerung) GRC

---

zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), COM (2017) 10. Zum Gesetzgebungsverfahren: https://eur-lex.europa.eu/procedure/DE/2017_3?qid=1526909146823&rid=1.

[6] Vgl. auch *R. Derksen*, NVwZ 2017, S. 1005 (1005).

[7] BVerfGE 133, 277 (315 f.). Siehe dazu *F. Wollenschläger*, in: H. Dreier (Hrsg.), GG, Bd. 2, 3. Aufl. 2015, Art. 23 Rn. 103.

[8] *X. Brechot*, Revue de l'Union Européenne 2017, S. 178 (186).

[9] BVerfG, NVwZ 2016, S. 1240 (1242). Ebenso Beschl. v. 8.6.2016, 1 BvR 229/16, juris, Rn. 27.

dar,[10] der freilich einer Rechtfertigung gemäß Art. 52 Abs. 1 GRC[11] zugänglich ist. Nach der zuletzt genannten Bestimmung muss „jede Einschränkung der Ausübung der in der Charta anerkannten Rechte und Freiheiten gesetzlich vorgesehen sein und [den] Wesensgehalt dieser Rechte und Freiheiten achten … Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen der Ausübung dieser Rechte und Freiheiten nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen".[12]

Die unionsgrundrechtliche Zulässigkeit der TK-Verkehrsdatenspeicherung hängt hinsichtlich ihres „Ob" und „Wie" demnach von einer Abwägung der widerstreitenden Belange von Freiheit und Sicherheit ab (näher dazu meine Stellungnahme zum ursprünglichen Gesetzentwurf, Anlage, III.2.). Wie bereits die Wertung des (freilich die Auslegung nationaler Grundrechte betreffenden) Urteils des BVerfG vom 2.3.2010 illustriert, lässt sich eine allgemeine TK-Verkehrsdatenspeicherung als unions(grund)rechtskonform ansehen. Auch in seinen (wiederum nur die nationalen Grundrechte betreffenden) Eilentscheidungen zur TK-Verkehrsdatenspeicherung hat das BVerfG weniger die allgemeine Speicherpflicht als den behördlichen Zugriff auf die Daten akzentuiert. Denn erst dieser begründe konkrete Belastungen; im Wortlaut:

> Zwar kann die gegenüber den Verpflichteten nach § 113 a TKG in § 113 b TKG angeordnete umfassende und anlasslose Bevorratung sensibler Daten über praktisch jedermann für staatliche Zwecke, die sich zum Zeitpunkt der Speicherung der Daten nicht im Einzelnen absehen lassen, einen erheblichen Einschüchterungseffekt bewirken, weil das Gefühl entsteht, ständig überwacht zu werden. Dieser Effekt ließe sich für die Zeit zwischen dem Inkrafttreten der Norm und der Entscheidung des BVerfG selbst dann nicht rückgängig machen, wenn die Verfassungsbeschwerde in der Hauptsache Erfolg haben sollte.
>
> Der in der Speicherung für Einzelne liegende Nachteil für ihre Freiheit und Privatheit verdichtet und konkretisiert sich jedoch erst durch einen Abruf der Daten zu einer möglicherweise irreparablen Beeinträchtigung. Die Datenbevorratung ermöglicht zwar den Abruf, doch führt erst dieser zu konkreten Belastungen. Das Gewicht eines denkbaren Einschüchterungseffekts hängt dann davon ab, unter welchen Voraussetzungen die bevorrateten Daten abgerufen und verwertet werden können. Je weiter die Befugnisse staatlicher Stellen insoweit reichen, desto eher müssen die Bürgerinnen und Bürger befürchten, dass diese Stellen ihr Kommunikationsverhalten überwachen (vgl. BVerfGE 121, 1 [20] = NVwZ 2008, 543). So ist mit der Speicherung allein jedoch noch kein derart schwerwiegender Nachteil verbunden, dass er die Außerkraftsetzung eines Gesetzes erforderte. Dies gilt auch für die Speicherung der Daten von Berufsgeheimnisträgern.[13]

---

[10] EuGH, verb. Rs. C-203/15 und C-698/15, ECLI:EU:C:2016:970, Rn. 93 – Tele 2.

[11] Im Kontext von Art. 8 GRC sind überdies dessen Absätze 2 und 3 zu beachten; diese lauten: „(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht."

[12] EuGH, verb. Rs. C-203/15 und C-698/15, ECLI:EU:C:2016:970, Rn. 94 – Tele 2.

[13] BVerfG, NVwZ 2016, S. 1240 (1241). Ebenso Beschl. v. 8.6.2016, 1 BvR 229/16, juris, Rn. 18 f.

3. Das Urteil des EuGH vom 8.4.2014 in der Rs. Digital Rights

Bereits das erste Urteil des EuGH zur Verkehrsdatenspeicherung wird mitunter dahin interpretiert, dass der Gerichtshof einer allgemeinen Verkehrsdatenspeicherung einen unionsgrundrechtlichen Riegel vorgeschoben habe.[14] Diese Interpretation geht, wie bereits in meiner Stellungnahme zum ursprünglichen Gesetzentwurf ausgeführt (siehe Anlage, III.2.), 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 allgemeine Speicherung von TK-Verbindungsdaten – für sich genommen die Unionsgrundrechtswidrigkeit der TK-Verkehrsdatenspeicherung begründen würden. Eine Extrapolation des Urteils auf die hier zu beurteilenden Regelungen bewegt sich folglich im Bereich des Spekulativen. Anders als das BVerfG formulierte der Gerichtshof keine konkreten Voraussetzungen, unter denen eine vorsorgliche Speicherung von Verkehrsdaten zulässig ist.[15]

4. Das Urteil des EuGH vom 21.12.2016 in der Rs. Tele2 u.a.

In seinem Urteil vom 21.12.2016 in der Rs. Tele2 hat der EuGH zum einen bestimmte nationale Regelungen der TK-Verkehrsdatenspeicherung für unionsrechtswidrig erklärt (a) und sich zum anderen allgemein zur Vereinbarkeit von Regelungen der TK-Verkehrsdatenspeicherung mit dem Unionsrecht geäußert (b). Ausgeklammert bleiben im Folgenden die Ausführungen des EuGH zu Anforderungen an den Zugang zu den gespeicherten Daten (Frage 2, Rn. 113 ff.), da sie kein grundsätzliches Verbot der allgemeinen TK-Verkehrsdatenspeicherung begründen.[16]

---

[14] 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.); *A. Roßnagel*, NJW 2017, S. 696 (697 f.); *I. Spiecker gen. Döhmann*, JZ 2014, S. 1109 (1112); *H. A. Wolff*, DÖV 2014, S. 608 (610); *W. Ziebarth*, ZUM 2017, S. 398 (400 ff.). **A.A.** *W. Durner*, DVBl. 2014, S. 712 (714); *N. Härting*, BB 2014, S. 1105 (1105); *S. Simitis*, NJW 2014, S. 2158 (2160).

[15] 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.

[16] Vgl. aber auch VG Köln, Urt. v. 20.4.2018, Az. 9 K 7417/17, Umdruck, Rn. 96 ff.

Ob nach dem Tele2-Urteil eine allgemeine TK-Verkehrsdatenspeicherung per se unionsgrundrechtswidrig ist, wird in der Literatur unterschiedlich beurteilt.[17] Das OVG Münster hat in seinem Beschluss im vorläufigen Rechtsschutz vom 22.6.2017 eine Speicherpflicht von Telekommunikationsunternehmen wegen der aus dem Tele2-Urteil des EuGH folgenden Unionsrechtswidrigkeit einer allgemeinen TK-Verkehrsdatenspeicherung verneint;[18] aufgrund dieser oberverwaltungsgerichtlichen Entscheidung sieht die Bundesnetzagentur mittlerweile von „Anordnungen und sonstigen Maßnahmen zur Durchsetzung der in § 113b TKG geregelten Speicherverpflichtungen gegenüber allen verpflichteten Unternehmen" ab[19]. Das VG Köln hat mit Urteil vom 20.4.2018 eine aus dem Tele2-Urteil des EuGH folgende Unionsrechtswidrigkeit einer allgemeinen TK-Verkehrsdatenspeicherung in der (nicht rechtskräftigen) Hauptsache bestätigt.[20] Das LG Mannheim geht in einem Beschluss vom 18.1.2018 demgegenüber von einer nach wie vor bestehenden Anwendbarkeit der deutschen Regelungen zur TK-Verkehrsdatenspeicherung aus.[21]

---

[17] **Bejahend**: *X. Brechot*, Revue de l'Union Européenne 2017, S. 178 (183 f.); *D.-K. Kipker/J. Schefferski/M. Stelter*, ZD 2017, S. 131 (131 f.): „dürften" (132); *H. P. Lehr*, ÖJZ 2017, S. 281 (281 f.); *N. Marsch*, VerfBlog, 2016/12/23; *A. Oehmichen/C. Mickler*, NZWiSt 2017, S. 298 (302 f., 306 f.); *S. Peyrou*, Journal de droit européen 2017, S. 107 (107 ff.); *R. Priebe*, EuZW 2017, S. 136 (138 f.); *A. Roßnagel*, NJW 2017, 696 (697 f.); *S. Rößner*, K & R 2017, S. 560 (561 f.); *X. Tracol*, Computer Law & Security Review 2017, S. 541 (545 ff.); *W. Ziebarth*, ZUM 2017, S. 398 (404). **A.A.** *W. Bär*, NZWiSt 2017, S. 81 (86); *A. Sandhu*, EuR 2017, S. 453 (467 f., 469); ferner im Ergebnis (über eine Reduktion der Anforderungen bzw. veränderte Bedrohungslagen) *W. Frenz*, DVBl. 2017, S. 183 (185 f.). **Ambivalent** *R. Derksen*, NVwZ 2017, S. 1005 (1006, 1009), der „praktisch kaum noch ein Spielraum" sieht (1006), indes „[z]wingende Schlussfolgerungen zur Europarechtskonformität für andere nationale Regelungen zur Vorratsdatenspeicherung als die vom EuGH untersuchten" verneint (1009); *W. R. Mbioh*, EDPL 2017, S. 273 (277) – „for instance"; *L. Woods*, Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber), abrufbar unter: http://eulawanalysis.blogspot.de/2016/12/data-retention-and-national-law-ecj.html (13.4.2017).

[18] OVG Münster, NVwZ-RR 2018, S. 43 (45 ff. – Zitat S. 45): „Nach einer Klärung grundsätzlicher Rechtsfragen zur Reichweite und zu den materiell-rechtlichen Anforderungen des im vorliegenden Zusammenhang maßgeblichen Unionsrechts durch das Urteil des EuGH vom 21.12.2016 steht fest, dass die durch § 113 a I iVm § 113 b TKG für die Erbringer öffentlich zugänglicher Telekommunikationsdienste für Endnutzer geregelte Pflicht zur Speicherung von Telekommunikationsverkehrsdaten mit Art. 15 I der RL 2002/58/EG … im Lichte der Grundrechte aus Art. 7, 8 und 11 sowie Art. 52 I GRCh unvereinbar ist. Dies folgt jedenfalls daraus, dass die Speicherpflicht keinen Zusammenhang zwischen den auf Vorrat zu speichernden Daten und dem durch das Gesetz verfolgten Zweck der Bekämpfung schwerer Straftaten bzw. der Abwehr schwerwiegender Gefahren für die öffentliche Sicherheit verlangt, sondern unterschiedslos ohne jede personelle, zeitliche oder geografische Begrenzung nahezu sämtliche Nutzer der von § 113 b TKG erfassten Telekommunikationsmittel erfasst."

[19] Mitteilung der Bundesnetzagentur zur Speicherverpflichtung nach § 113b TKG, www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS.html (25.5.2018).

[20] VG Köln, Urt. v. 20.4.2018, Az. 9 K 7417/17, Umdruck, Rn. 86 ff.

[21] LG Mannheim, ZD 2018, S. 223 (224): „Nach Auffassung der Kammer ist auch sonst nicht ersichtlich, dass Verfassungs- oder Unionsrecht derzeit dazu verpflichten könnte, § 100g StPO und §§ 113a, 113b TKG nicht anzuwenden."

a) Verbot bestimmter nationaler Regelungen der TK-Verkehrsdatenspeicherung

Der EuGH hat in seinem Tele2-Urteil zunächst nationale Regelungen der TK-Verkehrsdatenspeicherung wie die in einem der Ausgangsverfahren (Rs. C-203/15) streitigen wegen ihrer hohen Eingriffsintensität (vgl. Rn. 98 ff.) für unionsrechtswidrig erklärt: „Eine nationale Regelung wie die im Ausgangsverfahren in Rede stehende überschreitet somit die Grenzen des absolut Notwendigen und kann nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden, wie es Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta verlangt“ (Rn. 107). Gekennzeichnet war diese Regelung freilich dadurch, „dass sie eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsieht und die Betreiber elektronischer Kommunikationsdienste verpflichtet, diese Daten systematisch und kontinuierlich auf Vorrat zu speichern, und zwar ausnahmslos. Wie aus der Vorlageentscheidung hervorgeht, entsprechen die von dieser Regelung erfassten Datenkategorien im Wesentlichen denen, deren Vorratsspeicherung nach der Richtlinie 2006/24 vorgesehen war“ (Rn. 97).

Demgegenüber ist mit Blick auf die deutschen Regelungen des TKG zur TK-Verkehrsdatenspeicherung festzuhalten, dass sie deutlich grundrechtsschonender ausgestaltet ist. Zwar greift auch diese allgemein, was der EuGH besonders problematisiert hat (vgl. Rn. 105 f.):

> Zum anderen sieht eine nationale Regelung wie die im Ausgangsverfahren, die sich allgemein auf alle Teilnehmer und registrierten Nutzer erstreckt und alle elektronischen Kommunikationsmittel sowie sämtliche Verkehrsdaten erfasst, keine Differenzierung, Einschränkung oder Ausnahme in Abhängigkeit von dem verfolgten Ziel vor. Sie betrifft pauschal sämtliche Personen, die elektronische Kommunikationsdienste nutzen, ohne dass sich diese Personen 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 …
>
> Eine solche Regelung verlangt 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 Zeitraums und/oder eines geografischen Gebiets und/oder eines Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Bekämpfung von Straftaten beitragen könnten (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 59).

Allerdings normiert das TKG keine „unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel“, die ausnahmslos gilt, womit sie sich auch nicht als Regelfall i.S.d. Rn. 104 des Tele2-Urteils[22] erweist. Vielmehr enthält § 113b Abs. 1 TKG zunächst eine nach

[22] Diese lautet: „Eine solche Regelung hat zum einen in Anbetracht ihrer in Rn. 97 des vorliegenden Urteils beschriebenen charakteristischen Merkmale zur Folge, dass die Vorratsspeicherung der Verkehrs- und Standortdaten die Regel ist,

der Datenart differenzierte Regelung der Speicherdauer: Standortdaten sind nur für vier Wochen zu speichern, die übrigen von der Speicherpflicht erfassten Daten für zehn Wochen. Darüber hinaus untersagt § 113b Abs. 5 TKG eine Speicherung von Daten von Diensten der elektronischen Post. Hinzu kommt, dass § 113 Abs. 6 TKG besonderer Vertraulichkeit unterliegende Verbindungen von der Speicherpflicht ausnimmt, nämlich „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 besonderen Verschwiegenheitsverpflichtungen unterliegen“ (§ 99 Abs. 2 Satz 1 TKG) – ob diese Regelung sowie die Erhebungs- und Verwertungsverbote zugunsten von Berufsgeheimnisträgern (§ 100g Abs. 4 StPO) im Übrigen unionsgrundrechtlich genügen, ist offen, aber wiederum von einer Gesamtabwägung abhängig[23]. Schließlich ist eine Speicherfrist von lediglich vier bzw. zehn Wochen vorgesehen (§ 113b Abs. 1 TKG), im Gegensatz zur sechsmonatigen Speicherfrist der Regelung des Ausgangsverfahrens (vgl. Rn. 19).

Vor diesem Hintergrund lässt sich aus der vom EuGH bejahten Unionsrechtswidrigkeit nationaler Regelungen der TK-Verkehrsdatenspeicherung wie solchen des Ausgangsverfahrens (Rs. C-203/15) nicht zwingend auf die Unionsrechtswidrigkeit der deutschen Regelung schließen. Entscheidend ist nämlich eine Gesamtabwägung, in die die Allgemeinheit als zwar grundrechtsintensiver, aber doch nur ein Aspekt des Eingriffs einzustellen ist.[24]

b) Allgemeine Ausführungen zur Zulässigkeit der TK-Verkehrsdatenspeicherung

Über die eigentliche Vorlagefrage und ihre Beantwortung hinaus, die sich auf die Vereinbarkeit von nationalen Regelungen der TK-Verkehrsdatenspeicherung wie solchen des Ausgangsverfahrens mit Unionsrecht bezieht (vgl. Rn. 62, 112), enthält das Urteil allgemeine Ausführungen zur Vereinbarkeit von Regelungen der TK-Verkehrsdatenspeicherung mit dem Unionsrecht.

---

obwohl nach dem mit der Richtlinie 2002/58 geschaffenen System die Vorratsspeicherung von Daten die Ausnahme zu sein hat.“

[23] Verneinend, eine Ausnahme von der Speicherpflicht schon zugunsten von Berufsgeheimnisträgern fordernd *R. Derksen*, NVwZ 2017, S. 1005 (1006 f.); *A. Roßnagel*, NJW 2017, S. 696 (698); *A. Sandhu*, EuR 2017, S. 453 (468). Im Urteil des EuGH (Rn. 105) heißt es: „Zudem sieht sie keine Ausnahme vor, so dass sie auch für Personen gilt, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 57 und 58).“

[24] Gleichwohl von der Unionsrechtswidrigkeit ausgehend VG Köln, Urt. v. 20.4.2018, Az. 9 K 7417/17, Umdruck, Rn. 101 ff.

Der EuGH bekräftigt zunächst die grundsätzliche Zulässigkeit der TK-Verkehrsdatenspeicherung und unterwirft sie einem strengen Verhältnismäßigkeitsvorbehalt (Rn. 108):

Hingegen untersagt Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta einem Mitgliedstaat nicht, eine Regelung zu erlassen, die zur Bekämpfung schwerer Straftaten vorbeugend die gezielte Vorratsspeicherung von Verkehrs- und Standortdaten ermöglicht, sofern die Vorratsdatenspeicherung hinsichtlich Kategorien der zu speichernden Daten, der erfassten elektronischen Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt ist.

Im Folgenden leitet er hieraus bestimmte Anforderungen ab (Rn. 109 ff.):

109. Um den in der vorstehenden Randnummer des vorliegenden Urteils genannten Erfordernissen zu genügen, muss die betreffende nationale Regelung erstens klare und präzise Regeln über die Tragweite und die Anwendung einer solchen Maßnahme der Vorratsdatenspeicherung vorsehen und Mindesterfordernisse aufstellen, so dass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken ermöglichen. Sie muss insbesondere angeben, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme der Vorratsdatenspeicherung vorbeugend getroffen werden darf, um so zu gewährleisten, dass eine derartige Maßnahme auf das absolut Notwendige beschränkt wird (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 54 und die dort angeführte Rechtsprechung).

110. Zweitens können sich die materiellen Voraussetzungen, die eine nationale Regelung, die im Rahmen der Bekämpfung von Straftaten vorbeugend die Vorratsspeicherung von Verkehrs- und Standortdaten ermöglicht, erfüllen muss, um zu gewährleisten, dass sie auf das absolut Notwendige beschränkt wird, zwar je nach den zur Verhütung, Ermittlung, Feststellung und Verfolgung schwerer Straftaten getroffenen Maßnahmen unterscheiden, doch muss die Vorratsspeicherung der Daten stets objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen. Diese Voraussetzungen müssen insbesondere in der Praxis geeignet sein, den Umfang der Maßnahme und infolgedessen die betroffenen Personenkreise wirksam zu begrenzen.

111. Bei der Begrenzung einer solchen Maßnahme im Hinblick auf die potenziell betroffenen Personenkreise und Situationen muss sich die nationale Regelung auf objektive Anknüpfungspunkte stützen, die es ermöglichen, Personenkreise zu erfassen, deren Daten geeignet sind, einen zumindest mittelbaren Zusammenhang mit schweren Straftaten sichtbar zu machen, auf irgendeine Weise zur Bekämpfung schwerer Kriminalität beizutragen oder eine schwerwiegende Gefahr für die öffentliche Sicherheit zu verhindern. Eine solche Begrenzung lässt sich durch ein geografisches Kriterium gewährleisten, wenn die zuständigen nationalen Behörden aufgrund objektiver Anhaltspunkte annehmen, dass in einem oder mehreren geografischen Gebieten ein erhöhtes Risiko besteht, dass solche Taten vorbereitet oder begangen werden.

Richtig ist, dass die vorstehend zitierte Rn. 111 die Unzulässigkeit einer allgemeinen, mithin alle Personen unabhängig von einem zumindest mittelbaren – etwa geographischen – Bezug zu Gefahren respektive Straftaten erfassenden, TK-Verkehrsdatenspeicherung nahelegt. Demgegenüber ist jedoch zweierlei zu berücksichtigen: zum einen handelt es sich bei der zitierten Urteilspassage um ein den deutschen Gesetzgeber nicht unmittelbar zur Modifikation des TKG verpflichtendes Obiter Dictum (aa); zum anderen verbleibt eine Restunsicherheit hinsichtlich des abschließenden Charakters dieser Urteilspassage (bb). Ein Prozessrisiko besteht freilich (cc).

aa) Obiter Dictum: (keine) unmittelbare Bindung des deutschen Gesetzgebers

Ob das Tele2-Urteil des Gerichtshofs den deutschen Gesetzgeber verpflichtet, die Regelungen zur TK-Verkehrsdatenspeicherung zu modifizieren, beurteilen Rechtsprechung und Schrifttum kontrovers, ohne die rechtsdogmatische Fundierung des Ergebnisses indes regelmäßig näher zu erörtern.[25]

Hinsichtlich der Bindungswirkung von Entscheidungen des EuGH im Vorabentscheidungsverfahren ist zwischen der das Ausgangsverfahren betreffenden Rechtskraft inter partes und einer darüber hinausgehenden Bindungswirkung erga omnes zu unterscheiden.[26] Letztere steht in der vorliegenden Konstellation inmitten. Beide Fragen sind unionsrechtlich nicht ausdrücklich geregelt. In seinem Urteil in der Rs. Jonkman vom 21.6.2007 hat der EuGH die Frage, „ob ein Mitgliedstaat verpflichtet ist, seine Rechtsvorschriften anzupassen, wenn der Gerichtshof auf ein Vorabentscheidungsersuchen ein Urteil erlassen hat, aus dem sich die Unvereinbarkeit dieser Rechtsvorschriften mit dem Gemeinschaftsrecht ergibt", bejaht und ausgeführt:

> Insofern ist darauf hinzuweisen, dass die Mitgliedstaaten nach dem in Artikel 10 EG [= Art. 4 Abs. 3 EUV] vorgesehenen Grundsatz der loyalen Zusammenarbeit verpflichtet sind, die rechtswidrigen Folgen eines Verstoßes gegen das Gemeinschaftsrecht zu beheben (Urteil vom 7. Januar 2004, Wells, C-201/02, Slg. 2004, I-723, Randnr. 64 und die dort angeführte Rechtsprechung).
>
> Daher sind die Behörden des betreffenden Mitgliedstaats verpflichtet, aufgrund eines auf ein Vorabentscheidungsersuchen ergangenen Urteils, aus dem sich die Unvereinbarkeit nationaler Rechtsvorschriften mit dem Gemeinschaftsrecht ergibt, die allgemeinen oder besonderen Maßnahmen zu ergreifen, die geeignet sind, die Beachtung des Gemeinschaftsrechts in ihrem Hoheitsgebiet zu sichern (vgl. in diesem Sinne Urteile Wells, Randnrn. 64 und 65, sowie vom 25. März 2004, Azienda Agricola Giorgio, Giovanni et Luciano Visentin u. a., C-495/00, Slg. 2004, I-2993, Randnr. 39). Den Behörden verbleibt die Wahl der zu ergreifenden Maßnahmen, doch müssen sie insbesondere dafür sorgen, dass das nationale Recht so schnell wie möglich mit dem Gemeinschaftsrecht in Einklang gebracht und den Rechten, die dem Bürger aus dem Gemeinschaftsrecht erwachsen, die volle Wirksamkeit verschafft wird.[27]

---

[25] Gegen eine Bindung Deutscher Bundestag, Wissenschaftliche Dienste, Ausarbeitung WD 7 – 3000 – 191/16, S. 23; *R. Derksen*, NVwZ 2017, S. 1005 (1009); ferner *A. Sandhu*, EuR 2017, S. 453 (464, 467 f.). Anders OVG Münster, NVwZ-RR 2018, S. 43 (48): „Statt dessen hat er [der EuGH] – über die konkret aufgeworfenen Vorlagefragen hinaus – allgemein und verbindlich dargelegt, welche materiell-rechtlichen Anforderungen sich aus Art. 15 I der RL 2002/58/EG für die Zulässigkeit einer nationalen Regelungen zur Vorratsspeicherung von Verkehrs- und Standortdaten ergeben"; *X. Tracol*, Computer Law & Security Review 2017, S. 541 (549): Erga-omnes-Wirkung – siehe aber auch S. 550 f. Für eine Handlungspflicht ferner *A. Oehmichen/C. Mickler*, NZWiSt 2017, S. 298 (307); *S. Rößner*, K & R 2017, S. 560 (562 f.). Unklar („zumindest faktisch[e] Bindung") VG Köln, Urt. v. 20.4.2018, Az. 9 K 7417/17, Umdruck, Rn. 84 f., zumal inter partes (Rn. 76).

[26] Siehe nur *C. F. Germelmann*, Die Rechtskraft von Gerichtsentscheidungen in der Europäischen Union, 2009, S. 404 ff., 439 f.; *M. Pechstein*, EU-Prozessrecht, 4. Aufl. 2011, Rn. 862 ff.

[27] EuGH, verb. Rs. C-231–233/06, Slg. I-2007, 5149, Rn. 37 f. – Jonkman; Siehe auch *U. Ehricke*, in: Streinz (Hrsg.), EUV/AEUV, 2. Auflage 2012, Art. 267 AEUV Rn. 69 ff., 73; *U. Karpenstein*, in: E. Grabitz/M. Hilf/M. Nettesheim (Hrsg.), Art. 267 AEUV Rn. 106 (Stand: 50. EL Mai 2013).

Vorliegend ist freilich zu berücksichtigen, dass aus dem Tenor des Tele2-Urteils einschließlich der ihn tragenden Entscheidungsgründe[28] keine Unvereinbarkeit der deutschen Regelung mit dem Unionsrecht folgt. Denn die Vorlagefrage bezieht sich auf Regelungen, „die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsieht." Die fragliche deutsche Regelung bleibt jedoch hinter dem zurück (siehe II.4.a). Bei den allgemeinen Ausführungen zur Unionsrechtskonformität von Regelungen der TK-Verkehrsdatenspeicherung (Rn. 108 ff.) handelt es sich demgegenüber um ein Obiter Dictum.[29] Denn diese Urteilspassage bezieht sich nicht auf die streitgegenständliche Regelung des Ausgangsverfahrens, sondern abstrakt auf Regelungen zur TK-Verkehrsdatenspeicherung. Dies verdeutlicht namentlich der Umstand, dass die Unionsrechtswidrigkeit von Regelungen der TK-Verkehrsdatenspeicherung wie solchen des Ausgangsverfahrens bereits zuvor festgestellt wird (Rn. 107). Damit gehen die Ausführungen über die Beantwortung der Vorlagefrage hinaus.

Trotz der einleitend skizzierten Unterscheidung von Rechtskraft inter partes und Bindungswirkung erga omnes kann die Bindungswirkung auch eines Vorabentscheidungsverfahrens nicht über die sachliche Reichweite der Rechtskraft hinaus erstreckt werden.[30] Rechtsprechung des EuGH hierzu ist nicht ersichtlichlich; für die – im deutschen Kontext ausdrücklich angeordnete Bindung u.a. des Gesetzgebers an Entscheidungen des BVerfG (§ 31 Abs. 1 BVerfGG)[31] – ist anerkannt, dass sich diese nicht auf Obiter Dicta, sondern nur auf die die Entscheidung tragenden Gründe erstreckt.[32]

Im Übrigen sei darauf hingewiesen, dass auch bei Annahme einer Bindung die Loyalitätspflicht kein absolutes Normwiederholungsverbot begründet, der Gesetzgeber vielmehr die Möglich-

---

[28] Zum Streit um eine Bindung auch an die tragenden Entscheidungsgründe (und ablehnend) *C. F. Germelmann*, Die Rechtskraft von Gerichtsentscheidungen in der Europäischen Union, 2009, S. 424 ff.; *B. Wegener*, in: C. Calliess/M. Ruffert (Hrsg.), EUV/AEUV, 5. Aufl. 2016, Art. 267 AEUV Rn. 48.

[29] Vgl. allgemein zu Obiter Dicta *C. F. Germelmann*, Die Rechtskraft von Gerichtsentscheidungen in der Europäischen Union, 2009, S. 430 f.

[30] Vgl. auch *B. Wegener*, in: C. Calliess/M. Ruffert (Hrsg.), EUV/AEUV, 5. Aufl. 2016, Art. 267 AEUV Rn. 48: Bindung der Urteile „nach Maßgabe ihres im Lichte der Entscheidungsgründe zu interpretierenden Tenors". Ebenso *M. Pechstein*, EU-Prozessrecht, 4. Aufl. 2011, Rn. 859 (siehe aber auch Rn. 869).

[31] Dieser lautet: „Die Entscheidungen des Bundesverfassungsgerichts binden die Verfassungsorgane des Bundes und der Länder sowie alle Gerichte und Behörden."

[32] Siehe nur m.w.N. *A. von Ungern-Sternberg*, BeckOK BVerfGG, 4. Edition (Stand: 01.12.2017), § 31 Rn. 30.

keit haben muss, jedenfalls bei Änderungen der für die rechtliche respektive tatsächliche Einschätzung maßgeblichen Umstände auf eine Korrektur der Rechtsprechung hinzuwirken.[33] Insoweit ist die Entscheidung des EuGH im Fluggastdaten-Gutachten zu berücksichtigen, aufgrund dessen kein generelles unionsgrundrechtliches Verbot der anlasslosen Vorratsdatenspeicherung besteht (siehe II.5.). Mit Ablauf der Umsetzungsfrist der Richtlinie (EU) 2016/680 zum 6.5.2018 ist überdies ein neuer, für die Beurteilung der TK-Verkehrsdatenspeicherung maßgeblicher Rechtsakt hinzugetreten, dessen Verhältnis zur streitgegenständlichen E-Privacy-Richtlinie zu klären ist.

Das BVerfG hat das Tele2-Urteil – anders als das VG Köln und das OVG Münster (siehe oben, II.4.) – nicht zum Anlass genommen, die TK-Verkehrsdatenspeicherung im Wege einer einstweiligen Anordnung auszusetzen:

> Auch nach der Entscheidung des Gerichtshofs der Europäischen Union (vgl. EuGH, Urteil der Großen Kammer vom 21. Dezember 2016 – Rs. C-203/15 und C-698/15 –, Tele2 Sverige u.a., NJW 2017, S. 717 ff.) stellen sich hinsichtlich der verfassungsrechtlichen Bewertung der hier angegriffenen Regelung sowie der Folgen, die sich aus jener Entscheidung hierfür ergeben, Fragen, die nicht zur Klärung im Eilrechtsschutzverfahren geeignet sind. Insoweit ist über den Antrag auf Erlass einer einstweiligen Anordnung unverändert auf der Grundlage einer Folgenabwägung zu entscheiden, wie in den Beschlüssen der 3. Kammer des Ersten Senats des Bundesverfassungsgerichts vom 8. Juni 2016 (vgl. 1 BvQ 42/15 und 1 BvR 229/16, www.bverfg.de, Rn. 12 ff.) geschehen. Dieser Entscheidung stehen auch nicht die Anforderungen des Unionsrechts an nationale Bestimmungen für den Erlass vorläufiger Maßnahmen zur Aussetzung der Anwendung nationaler Bestimmungen bei Unionsrechtswidrigkeit entgegen (vgl. EuGH, Urteil der Großen Kammer vom 13. März 2007 – Rs. C-432/05 –, Unibet [London] Ltd. u.a. gegen Justitiekanslern, NJW 2007, S. 3555 <3559 Rn. 83>).[34]

bb) Abschließender Charakter?

Abgesehen von der Qualität der Entscheidungspassage als Obiter Dictum ist noch auf Folgendes hinzuweisen: Zweifelsohne lassen sich die Rn. 108 ff. des Tele2-Urteils so verstehen, dass nur eine den dort genannten Voraussetzungen entsprechende Regelung als unions(grund)rechtskonform anzusehen und nach Rn. 111 eine allgemeine TK-Verkehrsdatenspeicherung verboten ist. Erwägen lässt sich jedoch, ob die negative Formulierung in Rn. 108 („Hingegen untersagt Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta einem Mitgliedstaat nicht, eine Regelung zu erlassen …, sofern …“)[35] auch die Deu-

---

[33] Vgl. im nationalen Kontext m.w.N. *A. von Ungern-Sternberg*, BeckOK BVerfGG, 4. Edition (Stand: 01.12.2017), § 31 Rn. 38 f.

[34] BVerfG, Beschl. v. 26.3.2017, 1 BvR 3156/15, juris, Rn. 1.

[35] Siehe auch die insoweit gleichlaufende englische Urteilspassage (Verfahrenssprache): “However, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.”

tung zulässt, dass eine den folgenden Rn. 109 ff. entsprechende Regelung jedenfalls als unionsrechtskonform anzusehen, nicht aber jede andere denkbare Regelung kategorisch ausgeschlossen ist. Die Passage formuliert ja nicht etwa, dass das Unionsrecht nur oder ausschließlich Regelungen zulasse, die den folgenden Anforderungen entsprechen.

cc) Verbleibendes Prozessrisiko

Vor dem Hintergrund des Obiter Dictums besteht ein nicht zu vernachlässigendes Prozessrisiko. Sollte der EuGH über die Unionsrechtskonformität der deutschen Regelung zu befinden haben, ist nicht auszuschließen, dass der EuGH das Obiter Dictum als abschließend bestätigt und etwa in einem Vertragsverletzungsverfahren (Art. 258 ff. AEUV) einen Unionsrechtsverstoß der Bundesrepublik Deutschland feststellt.[36]

5. Das Gutachten des EuGH vom 26.7.2017 zum Fluggastdatenabkommen mit Kanada

Von besonderer Bedeutung für den vorliegenden Zusammenhang ist, dass der EuGH in seinem nach dem Tele2-Urteil vom 21.12.2016 ergangenen Gutachten 1/15 zum Fluggastdatenabkommen mit Kanada vom 26.7.2017[37] kein generelles unionsgrundrechtliches Verbot einer Vorratsdatenspeicherung ausgesprochen hat.[38] Zwar hat der EuGH, wie bereits in den Urteilen Digital Rights und Tele2, eine restriktive Position eingenommen und eine generelle fünfjährige Speicherung der Passagierdaten für grundrechtswidrig erklärt (Rn. 204 ff.); allerdings hat er eine Speicherung für den Aufenthaltszeitraum in Kanada für zulässig erachtet, um die Daten zur Bekämpfung respektive Verfolgung terroristischer Straftaten und schwerer Kriminalität verwenden zu können, unabhängig davon, ob die nach Kanada einreisende Person in einem zumindest mittelbaren Bezug zu Gefahren respektive Straftaten steht. Dies stellt eine bedeutsame Lockerung gegenüber der Rechtsprechung zur TK-Verkehrsdatenspeicherung dar. Ein generelles unionsrechtliches Verbot der Vorratsdatenspeicherung besteht jedenfalls nicht.[39]

---

[36] Vgl. im Übrigen zu weiteren möglichen Konsequenzen der Unionsrechtswidrigkeit wie Schadensersatzansprüchen EuGH, verb. Rs. C-231–233/06, Slg. I-2007, 5149, Rn. 40 – Jonkman. Freilich die Voraussetzungen eines unionsrechtlichen Staatshaftungsanspruchs ablehnend Deutscher Bundestag, Wissenschaftliche Dienste, Ausarbeitung WD 7 – 3000 – 191/16, S. 22.

[37] EuGH, Avis 1/15, ECLI:EU:C:2016:656, Accord PNR UE-Canada. Umfassend hierzu *F. Wollenschläger*, Stellungnahme zum Gesetzentwurf der Bundesregierung – Entwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz – FlugDaG), BT-Drs. 18/11501, im Rahmen der Expertenanhörung des Innenausschusses, Ausschussdrucksache 18(4)869 E, abrufbar unter https://www.bundestag.de/blob/503972/b3a24577851f69297a0d0068d6a7c605/18-4-869-e-data.pdf.

[38] Dazu und zum Folgenden *F. Wollenschläger*, EuZW 2017, S. 913 (914).

[39] Vgl. auch *C. Kuner*, VerfBlog, 2017/7/26: "At the same time, the Court pulled back a bit from the prohibition in Tele2 against 'general and indiscriminate retention' of data (see para. 103 of that judgment), and found that interference with

Freilich können die Aussagen zur Fluggastdatenverarbeitung nicht unbesehen auf den Kontext der TK-Verkehrsdatenspeicherung übertragen werden. Denn letztere zeichnet sich angesichts der Streubreite und Aussagekraft der TK-Verbindungsdaten durch eine stärkere Eingriffsintensität aus. Gegenläufig ist allerdings auch zu berücksichtigen, dass die Fluggastdatenspeicherung insofern eingriffsintensiver ist, als die Speicherung beim Staat selbst erfolgt und nicht, wie bei der TK-Verkehrsdatenspeicherung, bei den Telekommunikationsunternehmen, zumal der Staat auf diese Daten nur unter qualifizierten Voraussetzungen zugreifen darf.

Im Urteil in der Rs. Schrems vom 6.10.2015 klang demgegenüber noch ein allgemeines Verbot an, wenn es heißt:

> Nicht auf das absolut Notwendige beschränkt ist eine Regelung, die generell die Speicherung aller personenbezogenen Daten sämtlicher Personen, deren Daten aus der Union in die Vereinigten Staaten übermittelt wurden, gestattet, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des verfolgten Ziels vorzunehmen und ohne ein objektives Kriterium vorzusehen, das es ermöglicht, den Zugang der Behörden zu den Daten und deren spätere Nutzung auf ganz bestimmte, strikt begrenzte Zwecke zu beschränken, die den sowohl mit dem Zugang zu diesen Daten als auch mit deren Nutzung verbundenen Eingriff zu rechtfertigen vermögen (vgl. in diesem Sinne, in Bezug auf die 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 [ABl. L 105, S. 54], Urteil Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 57 bis 61).[40]

6. Bewertung des Gesetzentwurfs

Unabhängig davon, wie man den Inhalt des Tele2-Urteils und dessen rechtliche Konsequenzen für den deutschen Gesetzgeber bewertet, ist hinsichtlich des hier zu begutachtenden Gesetzentwurfs schließlich festzuhalten, dass dieser mit seiner vollständigen Aufhebung der Regelungen der TK-Verkehrsdatenspeicherung über das unionsrechtlich (wie im Übrigen auch über das verfassungsrechtlich) Gebotene hinausgeht. Denn der EuGH hat in jenem Urteil ausdrücklich anerkannt, dass das Unionsrecht „einem Mitgliedstaat nicht [untersagt], eine Regelung zu erlassen, die zur Bekämpfung schwerer Straftaten vorbeugend die gezielte Vorratsspeicherung von Verkehrs- und Standortdaten ermöglicht, sofern die Vorratsdatenspeicherung hinsichtlich Kategorien der zu speichernden Daten, der erfassten elektronischen Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt ist“ (Rn. 108).

---

the fundamental rights to privacy and data protection may, under the right circumstances, be justified by a general objective of the EU such as the fight against terrorism, even though this involved a data retention period of five years.”

[40] EuGH, Rs. C-362/14, ECLI:EU:C:2015:650, Rn. 93 – Schrems.

Für den Regelungsspielraum des deutschen Gesetzgebers ist im Übrigen auch die noch ausstehende Entscheidung des BVerfG zu den hier inmitten stehenden TKG-Regelungen entscheidend.

München, den 12. Juni 2018

Gez. Prof. Dr. Ferdinand Wollenschläger

Anlage: Stellungnahme zur Einführung einer Speicherpflicht für Verkehrsdaten (BT-Drs. 18/5088; 18/5171; 18/4971) vom 17.9.2015

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).