18. Wahlperiode

Deutscher Bundestag

Ausschuss für Recht und Verbraucherschutz

Wortprotokoll
der 64. Sitzung

Ausschuss für Recht und Verbraucherschutz
Berlin, den 21. September 2015, 16:04 Uhr
Berlin, Paul-Löbe-Haus, Saal 4.900

Vorsitz: Renate Künast, MdB

Tagesordnung - Öffentliche Anhörung

Einziger Tagesordnungspunkt **Seite 12**

a) Gesetzentwurf der Fraktionen der CDU/CSU und SPD

Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

BT-Drucksache 18/5088

Federführend:
Ausschuss für Recht und Verbraucherschutz

Mitberatend:
Innenausschuss
Finanzausschuss
Ausschuss für Wirtschaft und Energie
Ausschuss für Verkehr und digitale Infrastruktur
Ausschuss für Menschenrechte und humanitäre Hilfe
Ausschuss Digitale Agenda
Ausschuss für die Angelegenheiten der Europäischen Union

Berichterstatter/in:
Abg. Dr. Volker Ullrich [CDU/CSU]
Abg. Christian Flisek [SPD]
Abg. Halina Wawzyniak [DIE LINKE.]
Abg. Katja Keul [BÜNDNIS 90/DIE GRÜNEN]

b) Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

BT-Drucksache 18/5171

Federführend:
Ausschuss für Recht und Verbraucherschutz

Mitberatend:
Innenausschuss
Finanzausschuss
Ausschuss für Wirtschaft und Energie
Ausschuss für Verkehr und digitale Infrastruktur
Ausschuss für Menschenrechte und humanitäre Hilfe
Ausschuss Digitale Agenda
Ausschuss für die Angelegenheiten der Europäischen Union

Gutachtlich:
Parlamentarischer Beirat für nachhaltige Entwicklung

Berichterstatter/in:
Abg. Dr. Volker Ullrich [CDU/CSU]
Abg. Christian Flisek [SPD]
Abg. Halina Wawzyniak [DIE LINKE.]
Abg. Katja Keul [BÜNDNIS 90/DIE GRÜNEN]

c) Antrag der Abgeordneten Jan Korte, Dr. André Hahn, Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE.

Auf Vorratsdatenspeicherung verzichten

BT-Drucksache 18/4971

Federführend:
Ausschuss für Recht und Verbraucherschutz

Mitberatend:
Innenausschuss
Ausschuss für Menschenrechte und humanitäre Hilfe
Ausschuss Digitale Agenda

Berichterstatter/in:
Abg. Dr. Volker Ullrich [CDU/CSU]
Abg. Christian Flisek [SPD]
Abg. Halina Wawzyniak [DIE LINKE.]
Abg. Katja Keul [BÜNDNIS 90/DIE GRÜNEN]

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

Montag, 21. September 2015, 16:00 Uhr

Anwesenheitsliste

gemäß § 14 Abs. 1 des Abgeordnetengesetzes

Ordentliche Mitglieder	Unterschrift	Stellvertretende Mitglieder	Unterschrift
CDU/CSU		**CDU/CSU**	
Grindel, Reinhard		Bosbach, Wolfgang	
Harbarth Dr., Stephan		Brandt, Helmut	
Heck Dr., Stefan		Fabritius Dr., Bernd	
Heil, Mechthild		Frieser, Michael	
Heveling, Ansgar		Gutting, Olav	
Hirte Dr., Heribert		Hennrich, Michael	
Hoffmann, Alexander		Jörrißen, Sylvia	
Hoppenstedt Dr., Hendrik		Jung Dr., Franz Josef	
Launert Dr., Silke		Lach, Günter	
Luczak Dr., Jan-Marco		Lerchenfeld, Philipp Graf	
Monstadt, Dietrich		Maag, Karin	
Seif, Detlef		Noll, Michaela	
Sensburg Dr., Patrick		Schipanski, Tankred	
Steineke, Sebastian		Schnieder, Patrick	
Sütterlin-Waack Dr., Sabine		Stritzl, Thomas	
Ullrich Dr., Volker		Strobl (Heilbronn), Thomas	
Wanderwitz, Marco		Weisgerber Dr., Anja	
Wellenreuther, Ingo		Woltmann, Barbara	
Winkelmeier-Becker, Elisabeth			

Ordemann, Tim

Hoffmann, Thorsten

Stand: 17. September 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)

Montag, 21. September 2015, 16:00 Uhr

Anwesenheitsliste

gemäß § 14 Abs. 1 des Abgeordnetengesetzes

Ordentliche Mitglieder	Unterschrift	Stellvertretende Mitglieder	Unterschrift
SPD		**SPD**	
Barley Dr., Katarina		Binding (Heidelberg), Lothar	
Bartke Dr., Matthias		Crone, Petra	
Brunner Dr., Karl-Heinz		Hartmann (Wackernheim), Michael	
Drobinski-Weiß, Elvira		Högl Dr., Eva	
Fechner Dr., Johannes		Lischka, Burkhard	
Flisek, Christian		Miersch Dr., Matthias	
Franke Dr., Edgar		Müller, Bettina	
Hakverdi, Metin		Özdemir (Duisburg), Mahmut	
Jantz, Christina		Schieder, Marianne	
Müntefering, Michelle		Steffen, Sonja	
Rohde, Dennis		Vogt, Ute	
Wiese, Dirk			
Dörmann, Martin			
DIE LINKE.		**DIE LINKE.**	
Lay, Caren		Binder, Karin	
Petzold (Havelland), Harald		Jelpke, Ulla	
Wawzyniak, Halina		Pitterle, Richard	
Wunderlich, Jörn		Renner, Martina	
BÜNDNIS 90/DIE GRÜNEN		**BÜNDNIS 90/DIE GRÜNEN**	
Keul, Katja		Beck (Köln), Volker	
Künast, Renate		Kühn (Tübingen), Christian	
Maisch, Nicole		Mihalic, Irene	
Ströbele, Hans-Christian		Notz Dr., Konstantin von	

Stand: 17. September 2015
Referat ZT 4-Zentrale Assistenzdienste, Luisenstr. 32-34, Telefon: +49 30 227-32659, Fax: +49 30 227-36339

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

Montag, 21. September 2015, 16:00 Uhr

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

Fraktionsmitarbeiter

Name (Bitte in Druckschrift)	Fraktion	Unterschrift
KÜHNAU	CDU/CSU	
Leopold	Grüne	
SIMONEIT	SPD	
HEUBACH	SPD	
Krüger, Imke	CDU/CSU	
Cohr, Silke	CDU/CSU	
Pohl, Jörn	Grüne	
STADOWY, JOHANNES	CDU/CSU	
Keller, Jens	BÜ90/Grüne	
Padst, Simon	-"-	
Piallat, Chris	BÜ90/Grüne	
Schlueter, Lisa	SPD/Büro Flisek	

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

Bundesrat

Land	Name (bitte in Druckschrift)	Unterschrift	Amts-bezeichnung
Baden-Württemberg			
Bayern	Rottmann		ORR
Berlin			
Brandenburg			
Bremen	Vera Bünsow-Cuke	Bünsow-Cuke	SR'in
Hamburg			
Hessen	HANSWILL		RR
Mecklenburg-Vorpommern			
Niedersachsen	Batruch		Rd.
Nordrhein-Westfalen			
Rheinland-Pfalz	WOLF		Rin
Saarland			
Sachsen	BITTERMANN		StA
Sachsen-Anhalt			
Schleswig-Holstein			
Thüringen	Bieder		RLG

Tagungsbüro

Sitzung des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss)
Montag, 21. September 2015, 16:00 Uhr

Ministerium bzw. Dienststelle (bitte in Druckschrift)	**Name** (bitte in Druckschrift)	Unterschrift	**Amts-bezeichnung**
BK-Amt	Dr. Unzeitig, Stefanie		RD'in
BMJV	LANGE		PSt
BMWi	KUJAWA		RR'in
BMJV	Dr. BECKER		RDin
BMJV	LEY		StAin
BMJV	DR. WENZEL		RDn
BMJV	Rülke, Kai		RD
BMJV	Steinige, R.		PrA
BMJV	Claus, S.		Ri'in
BMI	Krüger		RinR
"	Hensel		ORR
BMJV	Berg-Schlicke		RDn
BMJV	Korte		MDg'in
BMF	Kutzschbach		RD
BPrA	Pieper		MR

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 Montag, 21. September 2015, 16.00 Uhr

Name	Unterschrift
Dr. Nikolaus Berger Richter am Bundesgerichtshof, 5. Strafsenat, Leipzig	
Christoph Frank Deutscher Richterbund e. V. (DRB), Vorsitzender, Oberstaatsanwalt in Freiburg i. Br.	
Rainer Franosch Hessisches Ministerium der Justiz, Wiesbaden, Oberstaatsanwalt	
Dr. Heide Sandkuhl Deutscher Anwaltverein (DAV) e. V., Berlin, Vorsitzende des Ausschusses Gefahrenabwehrrecht, Rechtsanwältin	
Meinhard Starostik Rechtsanwalt, Berlin	
Frank Thiede Bundeskriminalamt Wiesbaden, Leiter der Beratungsstelle für polizeipraktische Rechtsfragen und Rechtspolitik	
Prof. Dr. Ferdinand Wollenschläger Universität Augsburg, Juristische Fakultät, Lehrstuhl für Öffentliches Recht, Europarecht und Öffentliches Wirtschaftsrecht	

Sprechregister Abgeordnete

Sprechregister Sachverständige

Die Vorsitzende **Renate Künast:** Ich wünsche Ihnen einen wunderschönen Montag und begrüße alle Abgeordneten aus unserem und aus den mitberatenden Ausschüssen und die sieben Sachverständigen. Schön, dass Sie unserer Einladung nachkommen konnten. Ich begrüße außerdem die Besucherinnen und Besucher auf der Tribüne. Wir beraten heute das Thema: Einführung einer Speicherfrist und einer Höchstspeicherfrist für Verkehrsdaten. Manche sagen auch Vorratsdatenspeicherung – das Wort ist kürzer. Uns liegen zwei Gesetzentwürfe der CDU/CSU-Fraktion und SPD-Fraktion dazu vor sowie ein Antrag der Fraktion die DIE LINKE., in dem gefordert wird, gänzlich auf die Vorratsdatenspeicherung verzichten. Wir haben ergänzend Stellungnahmen der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie des Hessischen Datenschutzbeauftragten verteilt. Das Thema diskutieren wir seit Jahr und Tag kontrovers. Dabei zeigen uns Entscheidungen des Bundesverfassungsgerichts (BVerfG) und des Europäischen Gerichtshofs (EuGH) Grenzen auf. Wir haben seitens der EU-Kommission noch Hinweise und Kritikpunkte in dem vorgesehenen Notifizierungsverfahren erhalten. Auf unsere Bitte hin sind die entsprechenden Unterlagen vom Bundesministerium der Justiz und für Verbraucherschutz (BMJV) übermittelt worden, ergänzend dazu auch eine vorläufige Bewertung des BMJV in tabellarischer Form. Jetzt komme ich zu Ihnen, meine Damen und Herren Sachverständige. Ihre Aufgabe ist es, uns klüger zu machen und in einigen Bereichen noch mehr an Hintergrundwissen und Einschätzungen zu geben. Zum Ablauf: Wir hören zunächst die Eingangsstatements der Sachverständigen. Dazu rufe ich Sie in alphabetischer Reihenfolge auf, in der Sie sitzen. Wir sagen immer: Ideal sind fünf Minuten. Über Ihnen ist eine Uhr. Wenn diese Uhr rote Zahlen schreibt, sieht es mit der Zeit schlecht aus. Wenn Sie zu etwas nicht kommen, sprechen Sie es kurz an, vielleicht haben wir in den Fragerunden die Möglichkeit, darüber zu sprechen. Und wie immer meine Bitte an die Kolleginnen und Kollegen, möglichst präzise Fragen zu stellen – eine Frage an höchstens zwei Sachverständige oder zwei Fragen an einen Sachverständigen. Die Sachverständigen notieren sich bitte, was sie gefragt werden. Wir sammeln die Fragen und werden dann eine Antwortrunde durchführen – in umgekehrter alphabetischer Reihenfolge. Danach folgen weitere Runden mit Fragen oder Nachfragen. Die Anhörung ist öffentlich, sie wird zur Anfertigung des Wortprotokolls durch das Sekretariat aufgezeichnet. Das Protokoll wird veröffentlicht. Die Anfertigung von Bild- und Tonaufnahmen im Übrigen ist nicht gestattet. So, wir sollten beginnen: Ich bitte zunächst Herrn Dr. Berger um sein kurzes Statement.

SV **Dr. Nikolaus Berger:** Sehr geehrte Damen und Herren, ich bedanke mich zunächst dafür, zur Anhörung eingeladen worden zu sein. Der Themenausschnitt, zu dem ich mich aus den unterschiedlichen Blickwinkeln eines Ermittlungs- und eines Revisionsrichters sachverständig äußern kann, ist die Bedeutung von Verkehrsdaten bei der Verbrechensaufklärung. Ich habe hierzu in meiner vorbereitenden Stellungnahme 20 Beispielsfälle aus der Gerichtspraxis herausgegriffen. Sie veranschaulichen exemplarisch, wie retrograd erhobene Daten zu Beginn eines Ermittlungsverfahrens häufig die einzigen Ermittlungsansätze sind und später beweiskräftige Indizien für eine Be- oder Entlastung eines Beschuldigten bilden können. Allein sieben der aufgeführten Verfahren wurden im laufenden Jahr durch Revisionsentscheidungen eines einzigen Strafsenats rechtskräftig abgeschlossen. Die ausgewählten Verfahren betreffen vor allem Tötungs- und Raubdelikte sowie Fälle schwerer Bandenkriminalität mobiler Tätergruppen. Dies sind Kriminalitätserscheinungen, bei denen die Bevölkerung ein besonders hohes Sicherheitsbedürfnis hat. Weder die Straftatopfer noch die Rechtsgemeinschaft als solche sollten in ihren Erwartungen auf Schutz des sozialen Nahraums und auf die Funktionstüchtigkeit der Strafrechtspflege als Teil des staatlichen Gewaltmonopols enttäuscht werden. Wo der Staat Gewalt durch Private im Einzelfall schon nicht präventiv verhindern kann, muss er zur Wahrung des Rechtsfriedens zumindest dafür sorgen, dass Verbrechen nicht ungestraft bleiben. Andernfalls droht unserer Grundordnung schwerer Schaden, sobald die Unverbrüchlichkeit der Strafnormen nicht hinreichend durch Sanktionierung schwerster Straftaten bekräftigt werden kann und sich Eigenmacht nicht mehr nur auf parallelgesellschaftliche Milieus von

Clans und Rockerbanden beschränkt. Die Beispielsfälle zeigen, dass der Rückgriff auf Verkehrsdaten nicht nur einen Hebel für weitere Ermittlungsschritte liefern und Indizien schaffen kann. Vielmehr erleichtern die Daten oftmals auch die Aufklärung von Tatserien und verhindern damit weitere Taten von Wiederholungstätern. Verkehrsdaten liefern Hinweise auf weitere Personen, die im unmittelbaren zeitlichen und örtlichen Zusammenhang mit der Tat im Kontakt zum Verdächtigen standen, und tragen so dazu bei, Täterstrukturen aufzuklären. Die Beispielsfälle erhellen im Übrigen, dass dort auch keine „Vermeidungsstrategien“ durch einfaches Ausschalten von Mobilgeräten gegriffen hätten: Bei spontanen Delikten fehlt es naturgemäß an solch planmäßigem Vorgehen. Hingegen sind mobil operierende Tätergruppen zur Tatdurchführung regelmäßig auch auf mobile Kommunikation angewiesen. Zusammenfassend lässt sich sagen, dass die alltägliche Justizpraxis die auch vom BVerfG 2011 und vom EuGH 2014 geteilte Annahme ständig bestätigt, dass eine Erhebung retrograder Verkehrsdaten ein wichtiges Aufklärungsinstrument bildet. Dem trägt die vom Regierungsentwurf vorgesehene Wiedereinführung einer Speicherpflicht von Telekommunikationsunternehmen Rechnung. Sie vermeidet, dass die Ergebnisse von Strafverfahren zufallsbedingt vom Zeitpunkt eines Ermittlungsbeginns und von der unterschiedlichen Praxis der Unternehmen hinsichtlich des Umfangs und der Dauer von Speicherungen abhängen. Zufallsbedingte Verfahrensergebnisse sind mit den – auch verfassungsrechtlichen – Anforderungen an eine gleichmäßige funktionstüchtige Strafrechtspflege unvereinbar. Kritisch zu sehen ist allerdings insbesondere, dass die Hürden für eine Verkehrsdatenabfrage mit dem Straftatenkatalog nach § 100g Abs. 2 der Strafprozessordnung (StPO) ebenso hoch sein sollen wie bei der – freilich ungleich tiefer in die Grundrechte eingreifenden – Anordnung einer Wohnraumüberwachung nach § 100c StPO. Die Hürden sollen damit noch höher sein als bei einer Überwachung von Kommunikationsinhalten nach § 100a StPO. Diese Beschränkung einer Erhebungsbefugnis läuft dem Gesetzeszweck effektiver Strafverfolgung zuwider. Sie erscheint innerhalb des Gefüges telekommunikationsbezogener Ermittlungsmaßnahmen systemwidrig. Sie ist auch nicht durch eine vom BVerfG vorgegebene verfassungsrechtliche Anforderung geboten. Nach der bisher geplanten Regelung sind daher nicht unerhebliche Schutzlücken zu erwarten. Ich danke für Ihre Aufmerksamkeit.

Die **Vorsitzende:** Herr Berger, das war vorbildhaft innerhalb der Zeit. Dann hat als nächster Herr Frank vom Deutschen Richterbund das Wort. Bitte.

SV **Christoph Frank:** Meine sehr geehrten Damen und Herren. Ich kann insgesamt auf die Stellungnahme des Deutschen Richterbundes vom Mai 2015 verweisen. Ich möchte einige Einzelpunkte aus dem Blick der Praxis ansprechen, die den verfassungsrechtlichen Auftrag aber auch den Anspruch hat, effektive Strafverfolgung in dem Bereich zu betreiben, den Herr Dr. Berger eben beschrieben hat. Die Erfahrungen der letzten Jahre zeigen, dass der Verdacht besteht, die Justiz überschreite rote Linien und gehe nicht sorgsam mit den Vorgaben des BVerfG und des EuGH um. Das belastet auch das in der Diskussion stehende Gesetz. Ein Kritikpunkt, den ich zunächst kurz ansprechen möchte, ist der Wertungswiderspruch in den Speicherfristen. Während die Verbindungsdaten, die aus Abrechnungsgründen gespeichert werden, weitere sechs Monate zur Verfügung stehen – wenn sie zur Verfügung stehen –, sind auf der anderen Seite für die Strafverfolgung Fristen von vier bzw. zehn Wochen vorgesehen, die für die Praxis nicht ausreichend sind. Wir brauchen Fristen, die sich in der Größenordnung von sechs Monaten bewegen. Das war auch in früheren Regelungen vorgesehen. Dies war nirgends für verfassungswidrig angesehen worden. Zum Straftatenkatalog: Der Straftatenkatalog ist aus unserer Sicht nicht schlüssig. Er enthält einerseits Straftaten, die unterhalb der Verbrechenslinie sind, andererseits fehlen Straftaten aus dem Katalog des § 100a StPO der inhaltlichen Telekommunikationsüberwachung, die als Verbrechenstatbestände ausgestaltet sind und nach unserer Auffassung geeignet sind, auch bei der Regelung des § 100g Absatz 2 StPO zu Grunde gelegt zu werden. Wir sehen aus Sicht der Praxis auch kritisch, dass der neue § 100g StPO, der besonders schweren Fälle vorsieht, an diese Regelungen anknüpft. Das würde voraussetzen,

dass die Staatsanwaltschaft bei der Beantragung und die Gerichte bei der Entscheidung über die Anträge der Staatsanwaltschaft bereits Prognosen abgeben, die regelmäßig zu Beginn der Ermittlungen nicht abgegeben werden können. Man sollte unbedingt an die Grundtatbestände entsprechend dem Katalog des § 100a Absatz 2 StPO anknüpfen, der vom Verfassungsgericht ausdrücklich mehrfach als verfassungsgemäß eingeordnet ist. Wir sehen auch ein Problem bei der Art der zu erhebenden Daten. Eine Rekonstruktion gerade der Telekommunikationsverbindungen ist nach der Rechtsprechung des Verfassungsgerichts für eine effektive Strafverfolgung und Gefahrenabwehr von besonderer Bedeutung. Wir haben höchst vielfältige Formen der Kommunikation, und deshalb ist es nicht nachvollziehbar, dass der Mail-Verkehr, also Verkehrsdaten von E-Mails und von Daten über aufgerufene Internetseiten, nicht in die Liste der zu speichernden Daten nach § 113b Absatz 5 TKG-Entwurf aufgenommen worden ist. Zu den Speicherfristen: Die kurze Speicherfrist von zehn Wochen für Verkehrsdaten und vier Wochen für Standarddaten ist – Herr Dr. Berger hat das schon angesprochen – weder verfassungsrechtlich geboten noch ermittlungstechnisch ausreichend. Die Dauer der Speicherfrist sollte nicht politisch, sondern nach den Bedürfnissen der Praxis bewertet werden. Zum Richtervorbehalt: Die Regelungen sehen einen erweiterten Richtervorbehalt vor, einen strengen Richtervorbehalt. Wir sind in einem klaren Bekenntnis zum Grundsatz des Richtervorbehalts, sehen aber in der Begründung des Gesetzentwurfs erneut die Aufgaben und Rolle der Staatsanwaltschaft nicht zutreffend dargestellt. Es gibt ein latentes diffuses Misstrauen in ihre Arbeit. Das beschädigt das Vertrauen in die Objektivität, die Rechtstaatlichkeit des Handelns und suggeriert ein rechtstaatliches Gefälle zwischen der Arbeit der Staatsanwaltschaft und der Gerichte. Das gibt es bei der ordnungsgemäßen Arbeit nach der StPO nicht. Die Praxis prüft verantwortungsvoll. Das belegen auch die Entscheidungen der Gerichte. Die erweiterte Begründungspflicht wird der Verantwortung, die die Gerichte bereits jetzt bei diesen Entscheidungen haben, nicht gerecht. Jede gerichtliche Entscheidung muss begründet werden, das ist geltendes Recht nach § 34 StPO. Eine qualifizierte Begründungspflicht würde in einer frühen Phase der Ermittlungen zu Verzögerungen führen.

Die **Vorsitzende:** Danke, Herr Frank. Dann hat jetzt Rainer Franosch vom Hessischen Ministerium der Justiz das Wort.

SV **Rainer Franosch:** Herzlichen Dank, meine sehr verehrten Damen und Herren. Ich bedanke mich zunächst für die Einladung und die Möglichkeit, Ihnen hier einige Dinge vortragen zu dürfen. Ich möchte mich aufgrund meiner Expertise im Bereich der Bekämpfung der Internetkriminalität, wo ich seit 1999 tätig bin, auf diesen Phänomenbereich beziehen und darlegen, inwieweit die Vorratsdatenspeicherung hier ein unverzichtbares Element ist. Ich habe in meiner vorbereitenden Stellungnahme ausgeführt, dass das, was wir als Internetkriminalität oder Cybercrime bezeichnen, in den vergangenen Jahren eine rasante Änderung erfahren hat. Wir reden nicht mehr nur von Straftaten, die Vermögensdelikte oder die Integrität von Daten betreffen. Wir reden davon, dass die organisierte Kriminalität sich dieses Mediums bedient, und dass es in diesem Medium Möglichkeiten für Straftäter gibt, sich Tatmittel zu beschaffen, wie sie früher undenkbar waren. Bei sämtlichen Straftaten, die über das Internet begangen werden, stellt die IP-Adresse des Täters regelmäßig den einzigen, immer aber den ersten, effizientesten und schnellsten Ermittlungsansatz dar. Gelingt bereits im ersten Ermittlungsschritt die Zuordnung einer IP-Adresse zu einem Anschlussinhaber nicht, laufen die Ermittlungen weitgehend ins Leere, weil regelmäßig keine anderen Spuren vorhanden sind. Man muss sich klarmachen, dass in aller Regel die Identifizierung eines Internetanschlussinhabers am Anfang des Verfahrens steht. Es geht darum, zunächst Anknüpfungstatsachen zu gewinnen, um überhaupt eine Person zu identifizieren und sodann weitere verdachtsabhängige Maßnahmen zu ergreifen. IP-Adressen sind in der Regel nur ein Indiz zur Identifizierung. Die eigentliche Täterüberführung gelingt erst später durch Maßnahmen der Telekommunikationsüberwachung, Inhaltsüberwachung, aber auch durch Durchsuchungsmaßnahmen. Ohne Vorratsdaten ist eine effektive Bekämpfung von Cybercrime nicht möglich. Der Ermittlungsansatz

IP-Adresse kann durch keinen alternativen Spurenansatz ersetzt werden. Deswegen kann auf die Vorratsdatenspeicherung nicht verzichtet werden. Die Regelung des Gesetzes trägt vom Grundsatz her diesem Gedanken Rechnung. Ich möchte jedoch nicht versäumen, einzelne Regelungen aus Sicht der Praxis kritisch zu betrachten. Insbesondere kann ich mich den Ausführungen meiner Vorredner anschließen. Die Speicherfristen, die im Gesetz vorgesehen sind, tragen dem Gebot einer effektiven Strafverfolgung nicht Rechnung. Es gibt unzählige Rechtstatsachen, die belegen, dass wir eine Speicherfrist von mindestens sechs Monaten in der Praxis benötigen. Dabei muss man sehen, dass häufig in Ermittlungsverfahren, die Cybercrime zum Gegenstand haben, Daten aus dem Ausland zugeliefert werden bzw. aus der Auswertung von Speichermedien stammen. Derartige Auswertungen lassen sich selten innerhalb von wenigen Wochen bewerkstelligen. Was den Straftatenkatalog betrifft, kann ich mich den Ausführungen meiner Vorredner anschließen. Es ist – aus meiner Sicht und aus Sicht der Praxis – nicht geboten, dass der Gesetzentwurf für den Zugriff auf Verkehrsdaten höhere Schranken auferlegt als für den Zugriff auf Inhaltsdaten. Die Rechtsprechung des BVerfG legt das nicht nah. Es ist auch kaum begründbar, dass es in einem Verfahren wegen gewerbsmäßigen Computerbetrug zukünftig weiterhin möglich sein soll, die Inhalte einer Internet-Telekommunikation zu überwachen, nicht jedoch auf Verkehrsdaten zuzugreifen. Insofern spricht alles dafür, den Straftatenkatalog des § 100a StPO, der vom Verfassungsgericht als verfassungsgemäß angesehen wird, auch der Vorratsdatenspeicherung zugrunde zu legen. In einem Punkt enthält der Gesetzentwurf einen Rückschritt gegenüber der derzeit geltenden Rechtslage. Im § 100g StPO ist geregelt, dass in der Neufassung der retrograde Rückgriff auf gespeicherte Standortdaten nicht mehr möglich sein soll. Mir erschließt sich nicht, inwieweit es verfassungsmäßig nunmehr geboten sein soll, den Rückgriff auf gespeicherte Standortdaten – wohlgemerkt nicht auf gespeicherte Vorratsdaten, sondern im Bereich des § 100g Absatz 1 StPO – auszuschließen. Das bedeutet eine erhebliche Einschränkung für die Arbeit der Praxis. Nicht schlüssig ist aus meiner Sicht auch, dass die E-Mail-Verkehrsdaten von der Vorratsdatenspeicherungsverpflichtung ausgenommen sind. Dafür sehe ich keine verfassungsmäßigen Grundlagen. Die E-Mail-Verkehrsdaten sind in der Praxis ein wichtiger Ansatz zur Identifizierung von Straftätern. Abschließend sei noch angemerkt, dass der § 113b StPO eine Speicherverpflichtung für Telekommunikationsdienste in eingeschränkter Weise mit sich bringt. Internetzugangsdienst und Telefonanbieter werden verpflichtet; ausgenommen sind Telemediendienste, die Telekommunikationsleistungen erbringen. Vielfach sind es nicht mehr nur Internetzugangsanbieter oder Telefonanbieter, die Telekommunikationsdienste im Internet anbieten, sondern eben auch Telemediendienste. Beispielsweise ist Facebook ein Telemediendienst. Hier werden vielfach Chatfunktionen oder Ähnliches angeboten. Insofern sollte man darüber nachdenken, dass diese Kanäle, die von den Tätern in der Praxis häufig genutzt werden, einer solchen Vorratsdatenspeicherungspflicht nicht unterliegen. Dies bedeutet eine Einschränkung der Strafverfolgungsmöglichkeiten. Ich bedanke mich für Ihre Aufmerksamkeit.

Die **Vorsitzende:** Danke Herr Franosch. Dann hat jetzt Frau Dr. Heide Sandkuhl vom Deutschen Anwaltverein das Wort. Bitte.

SVe **Dr. Heide Sandkuhl:** Meine Damen und Herren. Vielen Dank. Ich schließe mich meinen Vorrednern nicht an. Aus der Stellungnahme des Deutschen Anwaltvereins möchte ich kurz sechs Punkte hervorheben. Erstens: Kehrseite des dem Gesetzgeber eingeräumten Entscheidungs- und Beurteilungsspielraums ist die Darlegungslast. Der Sache nach bedeutet dies, dass der Gesetzgeber zur Rechtfertigung des beabsichtigten Eingriffs der Notwendigkeit unterfällt darzutun, dass und inwieweit es überhaupt zur Gefahrenabwehr und zur Strafverfolgung einer Speicherung der Telekommunikationsdaten von 80 Millionen Bundesbürgerinnen und Bundesbürger bedarf. Diese Darlegungslast erfüllt der Gesetzentwurf nicht. Vielmehr ist nach den bislang vorliegenden Untersuchungen – ich nenne nur Max-Planck-Institut und den Wissenschaftlichen Dienst des Deutschen Bundestages – davon auszugehen, dass die Vorratsdatenspeicherung für die Gefahrenabwehr und für die Aufklärungsquoten betreffend Straftaten praktisch keine

Auswirkung hat. Die soeben genannten Beispielsfälle will ich nicht in Abrede stellen. Mich wundert aber, dass bei einem solch schwerwiegenden Eingriff keine valide Untersuchung vorliegt, aus der sich die Rechtstatsachen ergeben, die einen solchen Eingriff überhaupt erforderlich machen. Nach der Rechtsprechung des BVerfG und des EuGH stellt die anlasslose Speicherung der Telekommunikationsverkehrsdaten einen besonders schweren Eingriff in Grundrechte dar. Daher muss – das wurde mehrfach in den Entscheidungen betont – die anlasslose Speicherung die absolute Ausnahme bleiben. Es darf ohne Erfüllung der Darlegungslast nicht von der Regel abgewichen werden, und es dürfen keine höchstpersönlichen Daten von Personen, die keinerlei Anhaltspunkte dafür bieten, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnten, gespeichert werden. Punkt zwei: Ungeachtet der Frage, ob nach der Entscheidung des EuGH vom 30. Juni 2014 überhaupt noch Raum für eine rechtlich zulässige Vorratsdatenspeicherung besteht, – es gibt Stimmen in der Literatur, die das bestreiten – bleibt festzuhalten, dass Berufsgeheimnisträger von der anlasslosen Vorratsdatenspeicherung auszunehmen sind. Dies berücksichtigt der Gesetzesentwurf nicht hinreichend. Während zum Beispiel nach § 113b Absatz 6 TKG des Entwurfs in Verbindung mit § 99 Absatz 2 TKG keine Daten von Personen, Behörden und Organisationen in sozialen und kirchlichen Bereichen gespeichert werden dürfen, werden die Berufsgeheimnisträger im Sinne von § 53 StPO von dieser Ausnahme nicht erfasst. Ein sachlicher Differenzierungsgrund ist jedoch nicht erkennbar – im Gegenteil. Sowohl die Telefonseelsorge, die Gesundheitsberatung, also all die Berufsgruppen, die in § 99 Absatz 2 TKG genannt werden, als auch die Tätigkeit der Berufsgeheimnisträger wie Ärzte, Anwälte, Abgeordnete etc. sind auf Vertrauen angelegt. Das verbindet sie. Wieso an dieser Stelle differenziert wird, erschließt sich nicht. Noch ein Hinweis: Zwar verbietet der § 100g Absatz 4 Satz 1 StPO im Entwurf die Erhebung von Verkehrsdaten, die sich gegen die Berufsgeheimnisträger im Sinne von § 53 StPO richtet. Jedoch – und jetzt kommt das, was wir kritisieren – wird das Erhebungsverbot daran geknüpft, dass die Erhebung von Verkehrsdaten voraussichtlich Erkenntnisse erbringen würde, über die die Berufsgeheimnisträger das Zeugnis verweigern dürften. Das heißt mit anderen Worten: Um die Frage zu entscheiden, ob das Daten sind, über die sie das Zeugnis verweigern dürfen, rückt man ziemlich dicht an den Inhalt der Telekommunikation heran. Dieser ist aber für die Verfolger ein absolutes Tabu. Diese Voraussetzung müsste daher dringend gestrichen werden. Drittens: Zu streichen ist § 113c Absatz 1 Nr. 3 TKG im Entwurf. Nach dieser Vorschrift dürfen die aufgrund der 113b TKG gespeicherten Daten durch den Erbringer öffentlich zugänglicher Telekommunikationsdienste für eine Auskunft auch nach § 113 Absatz 1 Satz 3 verwendet werden. Stellen im Sinne dieser Vorschrift sind aber unter anderem die Verfassungsschutzbehörden des Bundes, der Länder, der MAD und der BND. Im Ergebnis bedeutet das, dass die Erledigung von Auskunftsersuchen der Nachrichtendienste unter Berücksichtigung sowohl der Bestandsdaten als auch der Standortdaten erfolgt. Vierter Punkt: § 202 Absatz 3 StGB ermöglicht es den staatlichen Stellen, die Früchte illegaler Datenerhebung zu sichern. Das ist aber angesichts des bekanntgeworden Verdachts systematischer Ausspähung von Bürgern, Unternehmen und Amtsträgern durch ausländische staatliche Stellen ein ganz fatales Signal. Zudem ist es geboten, die Norm klarzustellen, soweit es um Journalisten geht, damit die weiter kritisch berichten können. Außerdem ist nicht einzusehen, dass der deutsche Gesetzgeber vorweg marschiert und nicht abwartet, bis auf Ebenen des EU-Rechts eine einheitliche Regelung geschaffen wird. Zuletzt: Im Gesetz fehlt eine Pflicht zur Evaluierung. Das Gesetz ist zeitlich nicht begrenzt. Handelt es sich aber um ein Gesetz, das auf einer Prognoseentscheidung beruht, ist es dringend geboten – schon aus Gründen der Selbstkontrolle der Legislative –, dass Berichts- bzw. Prüfungspflichten eingezogen werden. Vielen Dank.

Die **Vorsitzende:** Danke. Dann hat jetzt das Wort Meinhard Starostik, Rechtsanwalt in Berlin.

SV **Meinhard Starostik:** Frau Vorsitzende, meine Damen und Herren. Schönen Dank für die Gelegenheit meine Stellungnahme abzugeben. Ich

möchte mich auf die grundsätzlichen verfassungsrechtlichen Grenzen konzentrieren, die das BVerfG und der EuGH in ihren Entscheidungen zur Vorratsdatenspeicherung aufgezeigt haben. Die Frage steht im Raum: Wenn von Ermittlungsseite die positiven Seiten einer Vorratsdatenspeicherung aufgezeigt werden, können damit automatisch alle verfassungsrechtlichen Grenzen überschritten werden oder müssen wir solche noch einhalten? Zunächst ist es so, dass beide Verfassungsgerichte, das BVerfG und der EuGH die Eignung des Mittels bejaht haben. Das BVerfG hat bei der allgemeinen Verhältnismäßigkeitsprüfung auch die Erforderlichkeit bejaht. Es kommt dann aber bei der Verhältnismäßigkeitsprüfung im engeren Sinne dazu, dass gerade noch die Grenze dessen, was verfassungsrechtlich zulässig ist, erreicht ist, indem es in der Randnummer 210 der Entscheidungsgründe ausdrücklich darauf hinweist, dass eine solche Regelung eine Ausnahme bleiben muss, und dass die Luft für den Gesetzgeber bei weiteren ähnlichen Gesetzen sehr dünn wird. Die Vorratsdatenspeicherung dürfe kein Muster für ähnliche Gesetze sein. Das BVerfG greift damit eine Diskussion auf, die unter den Stichworten „additive Grundrechtseingriffe durch verschiedene Überwachungsmaßnahmen“ geführt wurde und die von Alexander Roßnagel das Label „Überwachungs-Gesamtrechnung“ bekommen hat. Der EuGH geht dagegen in seiner Verhältnismäßigkeitsprüfung weiter. Er sagt, dass ein Eingriff in Artikel 7 und 8 der Europäischen Grundrechtecharta vorliegt und für diesen Eingriff eine Beschränkung auf das absolut Notwendige erforderlich sei. Dieses absolut Notwendige sei an zwei Stellen überschritten. Zum einen, indem alle Daten aufgegriffen werden und auch Daten von Personen erfasst werden, die in keinerlei Zusammenhang mit Straftaten stehen. Zum anderen, indem keine Einschränkung zugunsten von Berufsgeheimnisträgern gemacht wurden; dazu haben wir schon Ausführungen gehört. Beide Verfassungsgerichte gehen auf die große Eingriffstiefe und auf die Gefährlichkeit von Missbrauch und Verwechslung ein. Ich darf an dieser Stelle daran erinnern, dass die Strafverfolgung ein sehr hohes verfassungsrechtliches Gut ist. Zur Rechtssicherheit gehört aber auch – seit dem 4. Zusatzartikel zur US-Verfassung – die Sicherheit der Bürger vor unberechtigten Zugriffen des Staates. Der Begriff der Rechtssicherheit hat diesen janusköpfigen Charakter. Das muss man berücksichtigen. Wenn wir die Regeln des BVerfG im Jahr 2015 anwenden, sind wir in der Situation, dass wir eine weitere Zunahme von Überwachungsregeln im rechtlichen und tatsächlichen Bereich haben. Ich darf daran erinnern, dass wir jedes Jahr ungefähr sieben Millionen automatisierte Bestandsdatenabfragen haben. Dazu kommen die manuellen Abfragen nach § 113 TKG. Ich darf daran erinnern, dass wir Kontenabfragen im Millionenbereich haben. Die Entscheidung des BVerfG zur Anti-Terror-Datei ging von 350.000 Abfragen allein in solch einer spezialisierten Datei aus. Und ich darf daran erinnern, dass wir im privaten Bereich noch erheblichere Datensammlungen haben, die dem Ermittlungszugriff der Ermittlungsbehörden grundsätzlich offen stehen: Daher ist die im Jahre 2010 vom BVerfG schon gesehene Gefahr einer Persönlichkeitsprofilbildung heute noch viel stärker gegeben. Jedenfalls müssen wir uns fragen, ob angesichts der bestehenden Überwachungsmöglichkeiten die Vorratsdatenspeicherung nicht „das Fass zum Überlaufen bringt“, wenn ich dieses Bild mal im verfassungsrechtlichen Sinne gebrauchen darf. Schärfer geht der EuGH an die Zulässigkeit der Vorratsdatenspeicherung heran. Er sagt, die Beschränkung auf das absolut Notwendige ist nicht gegeben. Allein dies ist meines Erachtens europarechtlich ein Grund um verfassungsrechtlich die Vorratsdatenspeicherung für unzulässig zu erklären. Der EuGH weist in seiner Entscheidung vor allem darauf hin, dass allein die ermittlungstechnische Notwendigkeit den Grundrechtseingriff nicht rechtfertigen kann. Es muss die Verhältnismäßigkeitsabwägung dagegen gestellt werden. Lassen Sie mich abschließend noch auf zwei Dinge hinweisen. Einmal Begründungsfrist: Das BVerfG hat schon in seinem Vorratsdatenspeicherungsurteil darauf hingewiesen, dass es eine gehaltvolle Begründung der Beschlüsse zur Auskunftserteilung erwartet. Und zum Berufsgeheimnis: In einer Kammerentscheidung des BVerfG wurde darauf hingewiesen, dass der Verkehr des Strafverteidigers mit seinem Mandanten schon verfassungsrechtlich vor jeder staatlichen Überwachung geschützt ist. Wir wissen heute, wie aussagekräftig die sogenannten

Verbindungsdaten sind, dass sie aussagekräftiger sein können als Inhaltsdaten. Deswegen bin ich der Meinung, dass die geplante Vorratsdatenspeicherung schon bundesverfassungsrechtlich und nicht erst europarechtlich unzulässig ist. Schönen Dank.

Die **Vorsitzende:** Danke sehr Herr Starostik. Jetzt hat Herr Thiede vom BKA das Wort.

SV **Frank Thiede:** Danke Frau Vorsitzende, meine Damen und Herren. Ich kann mich in weiten Teilen an das anschließen, was insbesondere die Kollegen Berger, Frank und Franosch im Blick auf die Notwendigkeit der Vorratsdatenspeicherung für die polizeiliche Arbeit gesagt haben. Ich will eine Sache vorweg nehmen, die von besonderer Bedeutung ist: Nämlich die Frage nach der Erforderlichkeit. Ich werde vermitteln, was wir seitens des Bundeskriminalamts für einen Eindruck von der Diskussion der Vorratsdatenspeicherung seit mittlerweile über zehn Jahren haben. Ich mache die rechtliche Beratung im Bundeskriminalamt für die Amtsleitung und das Innenministerium. Außerdem gehört die Beratung der Fachabteilung dazu und – bei rechtspolitischen Forderungen – das Zusammentragen dessen, was aus der polizeilichen Praxis von Bund und Länder gleichermaßen für notwendig erachtet wird. Bei keiner anderen rechtspolitischen Forderung tragen die Polizeien von Bund und Ländern mit ähnlicher Vehemenz und Dringlichkeit vor wie bei der Vorratsdatenspeicherung. Bereits im Jahr 2005 sind die ersten Fälle mit der Bitte an uns herangetragen worden, das in den politischen Raum einzubringen und darauf hinzuweisen, wie wichtig es ist, insbesondere mit Blick auf die IP-Adressen. Stichwort: Zunahme von Flatrate-Angeboten, was heute Standard ist. Wir haben zehn Jahre lang diesen Diskurs geführt. Ich möchte an dieser Stelle eine Lanze für alle Polizeibeamtinnen und Polizeibeamten in Bund und Ländern brechen. Glauben Sie nicht, dass uns hemdsärmelig berichtet wird, was man alles machen müsste. Es war vielmehr immer sehr ausgewogen – ausgewogen im Hinblick auf die Datenarten, aber auch im Hinblick auf die Speicherfrist. Bei den vielen Fällen, die wir zusammengetragen haben, ist keiner über das Ziel hinausgeschossen und hat jahrelange Speicherungen gefordert. Es ging immer um die sechs Monate, die das abbildeten, was dann auch später ins Gesetz einfloss, welche – aus unserer Sicht leider – vom Verfassungsgericht gekippt wurde. Das vorab als Information, was wir wahrnehmen im BKA. Die Fälle, die wir nach der Entscheidung des BVerfG 2010 zusammengetragen haben, beruhen auf einer Abfrage bei allen Polizeien in Bund und Ländern. Wir haben fast 100 Fälle ausgewählt, die den Bedarf belegen und zwar interessanterweise phänomenübergreifend. Es ist nicht so, dass nur ein Phänomenbereich repräsentiert ist, sondern es ist in allen Bereichen wichtig. Wir haben natürlich im Bundeskriminalamt ein eingeschränktes Feld der Ermittlungszuständigkeiten. Wir sind nicht für alle Straftaten zuständig, sondern nur für die, die in § 4 des BKA-Gesetzes unsere originäre Zuständigkeit begründen oder im Rahmen der Auftragszuständigkeit von uns bearbeitet werden. Dazu haben wir ein Jahr lang eine statistische Vollerhebung bei allen Beamtinnen und Beamten im Hause gemacht. Die Fälle und die statistische Erhebung beweisen, wie bedeutsam und wie eklatant die Defizite sind, die zutage getreten sind. Ich habe das in meinen Papieren zusammengetragen und verweise auf unseren Abschlussbericht, den wir auch auf unserer Homepage eingestellt haben. Wie stellt sich der vorliegende Referentenentwurf in der Praxis dar? Die grundsätzliche Aussage, die wir feststellen, ist: Ja, wir sind auf dem richtigen Weg. Es ist in weiten Teilen ein Fortschritt gegenüber dem Stillstand, den wir nach der Entscheidung des Verfassungsgerichts 2010 nun fünf Jahre ertragen mussten. Wir haben insbesondere bei der IP-Adresse eine deutliche Verbesserung, und auch die Voraussetzungen für die Praxis erscheinen noch erträglich. Schwieriger dürfte es sicherlich sein, bei der retrograden Erhebung von Verkehrsdaten im Blick auf die Standortdaten. Hier haben wir die Standortdaten retrograd überhaupt nicht mehr zur Verfügung. Bei den Funkzellendaten auch mit Einschränkungen, wenn auch nur die vier Wochen sicherlich ein Vorteil im Vergleich zur geltenden Rechtslage sind. Das als kurzes Intro von meiner Seite.

Die **Vorsitzende:** Danke, Herr Thiede. Dann hat als letzter in der Runde Professor Dr. Wollenschläger das Wort. Bitte.

SV **Prof. Dr. Ferdinand Wollenschläger:** Vielen Dank Frau Vorsitzende, meine Damen und Herren Abgeordneten. Ich denke, das Grundsatzproblem ist klar geworden. Auf der einen Seite steht die Verkehrsdatenspeicherung als wegen ihrer Anlasslosigkeit, Streubreite und auch wegen der Aussagekraft der Daten gewichtiger Grundrechtseingriff. Auf der anderen Seite stehen gleichrangige Verfassungsgüter, nämlich für eine effektive Strafverfolgung und für eine effektive Gefahrenabwehr zu sorgen, die nicht minder gewichtig sind. Deswegen hat das BVerfG in seinem schon mehrfach angesprochenen Urteil vom 2. März 2010 zwar die frühere Regelung der Vorratsdatenspeicherung für verfassungswidrig erklärt, aber eine Speicherung von Verkehrsdaten als solche nicht. Vielmehr erachtet das BVerfG die Speicherung von Verkehrsdaten für prinzipiell mit dem Grundgesetz vereinbar und hat insoweit auch Anforderungen in seinem Urteil formuliert: die bekannte Höchstspeicherdauer von sechs Monaten, die Beschränkung auf besonders wichtige Verwendungszwecke sowie die Gewährleistung von Datensicherheit, Transparenz sowie den Richtervorbehalt. Aus verfassungsrechtlicher Perspektive ist – im Detail habe ich es in meiner Stellungnahme dargelegt – als Grundsatz festzuhalten, dass kein Verfassungsverbot der Speicherung von Verkehrsdaten besteht. Es obliegt deshalb Ihnen als demokratisch legitimiertes Gesetzgebungsorgan, in Abwägung der Vor- und Nachteile eine rechtspolitische Entscheidung zu treffen. Diese muss die verfassungsrechtlichen Kautelen wahren, ist aber verfassungsrechtlich nicht in eine Richtung entschieden. Wenn man die Gesetzentwürfe anschaut und sie mit Blick auf ihre Verfassungskonformität bewertet, muss man sagen, dass – trotz des Klarstellungsbedarfs, den auch der Wissenschaftliche Dienst aufgezeigt hat –, die Gesetzesentwürfe die Anforderungen des BVerfG wahren. Sie bleiben sogar hinter den größten Möglichkeiten, die das BVerfG aufgezeigt hat, zurück. Das Ganze mag man, wie die Vorredner aus der Praxis, kritisieren. Aus meiner verfassungsrechtlichen Perspektive ist das aber kein Verfassungsproblem. Nächster Punkt: das Urteil des EuGH vom 8. April 2014. Da möchte ich auf zwei häufig anzutreffende Missverständnisse dieser Entscheidung eingehen. Erste Frage: Gilt diese Entscheidung überhaupt für die heutige Konstellation? Da ist zu beachten, dass die Grundrechte des Grundgesetzes zwar für den Bund und für die Bundesländer umfassend gelten, dass die europäischen Grundrechte aber zwar für die Europäische Union umfassend, für die Mitgliedstaaten aber nur dann gelten, wenn die Mitgliedstaaten im Anwendungsbereich des Unionsrechts handeln. Ob man davon nach Nichtigerklärung der Vorratsdatenspeicherungsrichtlinie noch sprechen kann, ist – obgleich es mit der E-Privacy-Richtlinie noch gewisse Anknüpfungspunkte gibt – fraglich. Zweites Missverständnis: Der EuGH hat in seinem Urteil vom 8. April die Vorratsdatenspeicherung nicht für europarechtswidrig erklärt, sondern er hat lediglich die frühere Richtlinie für europarechtswidrig erklärt, allerdings nur aufgrund einer Gesamtabwägung aller Umstände. Das Urteil beruht also auf einen anderen Ansatz als das des BVerfG. Der EuGH hat auch keinen genauen Fahrplan für ein weiteres Tätigwerden vorgegeben. Das heißt im Umkehrschluss, dass man nicht aufgrund einzelner problematisierter Aspekte auf die Unionsgrundrechtswidrigkeit der Verkehrsdatenspeicherung als solche schließen kann. Es braucht eine neue Gesamtabwägung. Dabei ist einerseits zu berücksichtigen, dass der EuGH – das ist schon mehrfach angeklungen – die besondere Eingriffsschärfe betont hat. Andererseits ist zu berücksichtigen, dass die jetzigen Gesetzesentwürfe weit hinter dem damaligen Rechtsrahmen zurückbleiben. Allein bei den Speicherfristen bewegen wir uns nicht bei 24 Monaten, sondern bei ungefähr einem Zehntel. Letzter Punkt: die in der letzten Woche bekanntgewordene Mitteilung der Europäischen Kommission. Dazu nur eine Sache – die dort kritisierte Speicherpflicht im Inland ist nicht als solche unionsrechtswidrig. Sie ist nur dann unionsrechtswidrig, wenn eine Speicherung im Ausland ein gleichwertiges Datenschutzniveau gewährleistet. Das ist jetzt zu überprüfen. Wenn diese Prüfung zu dem Ergebnis führt, dass im Ausland ein gleichwertiges Datenschutzniveau gewährleistet werden kann, würde das bedeuten, dass die Erfordernisse des BVerfG insoweit außer Kraft gesetzt würden, weil das Europarecht vorgeht. Vielen Dank.

Die **Vorsitzende:** Danke sehr, Herr Professor Wollenschläger. Ich habe schon zahlreiche Wortmeldungen. Ich würde vorschlagen, dass wir

eine Runde machen. Ich lese vor, wer sich alles gemeldet hat: Frau Winkelmeier-Becker, Herr Ullrich, Frau Keul, Frau Wawzyniak, Herr von Notz, Herr Ströbele. Das ist eine Runde, und dann machen wir die nächste. Einverstanden? Gut. Dann würde bei den Fragen Frau Winkelmeier-Becker anfangen.

Abg. **Elisabeth Winkelmeier-Becker** (CDU/CSU): Von mir zunächst herzlichen Dank an alle Sachverständigen, dass Sie uns so ausführlich Dinge aus Ihrer Praxis mitgegeben und Argumente und schriftliche Stellungnahmen – auf sehr hohem Niveau – eingereicht haben. Ich möchte gerne eine Frage an Herrn Frank und an Herrn Franosch richten, und zwar zum Stichwort „Straftaten von erheblicher Bedeutung“. Da hat die Europäische Kommission moniert, dass nicht klar sei, was darunter zu verstehen ist. Hat die Europäische Kommission möglicherweise Dinge, die bei uns gebräuchlich oder bekannt sind, übersehen? Dann haben Sie beide moniert, dass der Kreis der infrage kommenden Taten nicht ganz schlüssig sei. Vielleicht nennen Sie uns ein paar Beispiele, welche Arten von Delikten hier durchs Raster fallen, welche also nicht mit Rückgriff auf Vorratsdatenspeicherung ermittelt werden können, obgleich Sie vielleicht annehmen, dass es angezeigt wäre, weil es sich auch um schwere Straftaten handelt, für die wenig andere Ermittlungsansätze bestehen. Danke.

Die **Vorsitzende:** Danke. Herr Dr. Ullrich, dann Frau Keul.

Abg. **Dr. Volker Ullrich** (CDU/CSU): Vielen Dank. Meine Frage bezieht sich zunächst auf das Schreiben der Kommission hinsichtlich des Orts der Speicherpflicht. Es wird dargelegt, dass möglicherweise durch die Speicherpflicht im Inland die EU-Marktfreiheit verletzt wird. Die Frage ist aber, ob überhaupt der Anwendungsbereich des EU-Binnenmarktes eröffnet sein kann. Es handelt sich bei der vorliegenden Maßnahme um präventive und strafrechtlich-prozessuale Eingriffe, sodass es um klassische ausschließliche Aufgaben des Hoheitsbereiches eines Staates geht, die nicht unbedingt vom EU-Recht umfasst sein dürften. Die zweite Frage bezieht sich auf die immer wieder vorgebrachte „Anlasslosigkeit“. Wenn ich das Gutachten von Herrn Professor Wollenschläger richtig lese, ist eine Gesamtbetrachtung nötig. Durch die einschränkenden Vorgaben des Gesetzentwurfs und die Eingriffstiefe könne man im Ergebnis nicht mehr von einer anlasslosen Speicherung sprechen. Drittens würde mich interessieren, ob der Schutz der Berufsgeheimnisträger durch das Verwertungsverbot hinreichend sichergestellt werden kann. Meine Fragen richten sich an Herrn Professor Wollenschläger und Herrn Franke.

Die **Vorsitzende:** Danke Herr Dr. Ullrich. Dann hat Frau Keul und dann Frau Wawzyniak das Wort.

Abg. **Katja Keul** (BÜNDNIS 90/DIE GRÜNEN): Von meiner Seite erstmal vielen Dank für Ihre Stellungnahme. Ich hätte zwei Fragen an Frau Dr. Sandkuhl. Die eine Frage betrifft den Tatbestand der Datenhehlerei, den Sie nur kurz ansprechen konnten. Mich würde interessieren, ob der Absatz drei mit seiner Ausnahmevorschrift aus Ihrer Sicht dem Bestimmtheitserfordernis genügt, vor allem was die Frage der Journalisten oder Blogger betrifft. Ist das, was dort in Bezug auf berufliche Handlungen steht, bestimmt genug? Die zweite Frage bezieht sich auf die Berufsgeheimnisträger. Sie hatten ausgeführt, es sei nicht nachzuvollziehen, warum bestimmte kirchliche Beratungsstellen von der Speicherung ausgenommen werden können und beispielsweise Rechtsanwälte nicht. Wir haben nach der Stellungnahme der Kommission dazu eine Antwort und eine Bewertung der Bundesregierung bekommen. Da steht: „Von Speicherung ausgenommen werden können die Daten der Berufsgeheimnisträger nicht, weil sie – anders als Beratungsdienste – selbst verdächtig sein können, eine Straftat begangen zu haben“. Ist das so? Sind Anwälte tendenziell verdächtig, Straftaten zu begehen? Müssen wir sie deswegen vorsorglich speichern?

Die **Vorsitzende:** Frau Wawzyniak, Herr von Notz.

Abg. **Halina Wawzyniak** (DIE LINKE.): Die erste Frage geht an Herrn Dr. Berger, die zweite an Herrn Starostik. Zur ersten Frage will ich vorab kurz etwas ausführen. Herr Frank hat gesagt, es sei ermittlungstechnisch nicht ausreichend, was derzeit als Speicherdauer vorgesehen ist. Herr Franosch hat gesagt, es gebe unzählige Rechtstatsachen, die belegen, dass sechs Monate erforderlich sind. Herr Thiede hat aus der Studie des BKA zitiert. Er hat leider unterschlagen, dass

467 Telefonverbindungsdaten abgefragt wurden und 380 davon beantwortet werden konnten. Sie haben uns auf 26 Seiten 20 Einzelfälle präsentiert, auf deren Grundlage Sie sagen, die Vorratsdatenspeicherung sei erforderlich. Lediglich drei der Fälle bezogen sich allerdings auf die Zeit, wo es schon eine Vorratsdatenspeicherung gab. In einem Fall davon gab es geständige Angaben, in einem anderen Fall hat der Angeklagte der Datenerhebung freiwillig zugestimmt. Alle anderen Fälle, ohne Vorratsdatenspeicherung, sind immerhin irgendwie bis zur Anklage gekommen. Da ich mich der Position von Frau Dr. Sandkuhl anschließe, dass es eine gewisse Darlegungslast zur Erforderlichkeit der Vorratsdatenspeicherung gibt, frage ich Sie nochmal ganz konkret: Warum brauchen Sie die Vorratsdatenspeicherung? Es sind doch Angeklagte ermittelt worden. Herr Starostik, Sie haben das Urteil des BVerfG zitiert, auch im Hinblick auf den Ausnahmecharakter. Sie haben die Überwachungsgesamtrechnung eingefordert, die nach meiner Auffassung der Gesetzentwurf leider nicht berücksichtigt. Sie haben vorhin von den sieben Millionen Bestandsdaten gesprochen, die derzeit schon erhoben werden. Könnten Sie das alles noch einmal visualisieren? Im Buch von Malte Spitz „Was macht ihr mit unseren Daten“ ist das schon einmal ganz gut dargestellt worden. Was bedeutet es, wenn Standortdaten, wenn Verkehrsdaten, wenn Bestandsdaten gesammelt werden? Ist das im Rahmen einer Überwachungsgesamtrechnung überhaupt noch verhältnismäßig?

Die **Vorsitzende:** Herr von Notz, Herr Ströbele, Herr Fechner, Herr Flisek.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Frau Vorsitzende, meine Damen und Herren Sachverständigen. Herzlichen Dank für Ihre Einführungen. Eine kurze Vorbemerkung: Dieser Gesetzentwurf wird damit vorgestellt, dass er großen Rechtsfrieden über den Streit bringen wird. Ich sage das in Richtung der Befürworter der Vorratsdatenspeicherung. Bei dem, was Sie draufsatteln wollen, fällt es schwer zu glauben, dass mit so einem Gesetzentwurf irgendein Rechtsfriede in diesen Fragen kommen wird. Ich wundere mich auch, dass man außer Einzelfällen nichts an Statistik bei einem so gravierenden Grundrechtseingriff darlegen kann. Zwei Fragen: Nach meinen Erfahrungen im 1. Untersuchungsausschuss der 18. Wahlperiode spricht vieles dafür, dass praktisch alle Verkehrsdaten, die Bundesbürgerinnen und Bürger erzeugen, bereits von Geheimdiensten mindestens einmal komplett erfasst werden. Dazu kommen PNR- und Swift-Gesetze, die ebenfalls anlasslose Datenspeicherungen auslösen. Deswegen die Frage an Frau Dr. Sandkuhl, im Kenntnisstand des Jahres 2015: Was bedeutet das für die Überwachungsgesamtrechnung und die Tiefe des Grundrechtseingriffs, der durch anlasslose Speicherungen erfolgt? An Herrn Franosch: Ich hatte mir erhofft, Argumente bezüglich des EuGHs zu hören. Deswegen frage ich Sie, auch für die Berufsstände, die Sie hier vertreten: Was ist die Argumentation im Hinblick auf die Berufsgeheimnisträger? Wie sieht die Argumentation beim Richterverband im Hinblick auf den Schutz aus, den der EuGH zugesagt hat? Auch zum Argument des EuGH, dass Unbeteiligte mit erfasst werden, habe ich kein Wort zu gehört, warum das jetzt in Ordnung sein soll. Darum die Frage: Interessiert diese EuGH-Rechtsprechung nicht? Ist sie nicht relevant? Oder gibt es gute Argumente gegen sie?

Die **Vorsitzende:** Herr Ströbele.

Abg. **Hans-Christian Ströbele** (BÜNDNIS 90/DIE GRÜNEN):Danke, Frau Vorsitzende. Ich habe an den Vertreter des Richterbundes und des Bundesgerichtshofs oder an den Richter am Bundesgerichtshof als Befürworter die Frage: Wir tagen hier ja nicht im luftleeren Raum. Das ist der Saal, in dem wir jeden Donnerstag im NSA-Untersuchungsausschuss sitzen. Da beschäftigen wir uns intensiv damit, welche Gefahren eigentlich für deutsche Bundesbürger bestehen, wenn sie ihre Daten irgendwo hinterlassen. Da haben wir gelernt, dass beispielsweise bei der Privatfirma Telekom die Geheimdienste an Datenleitungen gehen, diese abzapfen, nach G-10-Kriterien filtern und dann in der einen oder anderen Form mit der NSA teilen. Da gab es beim Bundesnachrichtendienst, der das vollzogen hat, und bei der Telekom interne Bedenken – können wir das, dürfen wir das? Dann haben sie sich gedacht: Holen wir uns doch eine Bescheinigung des Bundeskanzleramtes ein: Die Telekom hat dann vom Kanzleramt einen Brief bekommen mit dem Inhalt, dass das schon in Ordnung und mit

dem Gesetz vereinbar sei. Dann wurde munter über Jahre hinweg einer der zentralen Datenverkehrsknotenpunkte in Frankfurt ausgeleitet. Nun kann man sagen: Die Deutschen sind ein bisschen obrigkeitsgläubig, aber bei anderen Firmen ist das anders. Damit haben wir uns auch in diesem Saal beschäftigt. Es hat eine US-Firma gegeben, die in Hilden im Rheinland ebenfalls so einen Server betreibt. Auch die wollten an die Daten ran, der Bundesnachrichtendienst sollte helfen, und dann hat die US-Firma, die diese Datenleitung betrieben hat, gesagt: Ok, wir machen das, weil unsere Vertrauensleute von der NSA in den USA uns gesagt haben: Das ist in Ordnung, das könnt ihr so machen. Worauf ich hinaus will: Haben Sie nicht in heutigen Zeiten – Sie lesen ja wahrscheinlich auch Zeitung, sehen Fern und bekommen so ein bisschen Besorgnis mit – Sorge, dass man mit dem Anlegen von riesigen Datenbanken Begehrlichkeit weckt und vollzieht? Deshalb muss man zu dem Schluss kommen: Sichere Daten sind eigentlich nur Daten, die nicht irgendwo gespeichert sind. Ist das eine Überlegung, die Sie berücksichtigen? Oder sagen Sie: Das waren Missgriffe. Das wird nie wieder vorkommen. Darauf können wir keine Rücksicht nehmen? Das ist die erste Frage. Die zweite Frage ist kürzer und bezieht sich auf die Berufsgeheimnisträger; sie geht an den Vertreter des Bundeskriminalamtes. Können Sie mir sagen, wie Sie feststellen, wenn Sie eine Nummer prüfen, ob jemand ein Rechtsanwaltsgespräch oder ein Abgeordnetengespräch führt oder nicht? Muss ich als Rechtsanwalt jedes Mal, wenn mich jemand anruft, sagen: Hören Sie mal, sagen sie gleich „Rechtsanwalt“ oder „Guten Tag, Herr Straf-verteidiger“. Oder sage ich umgekehrt dann auch immer: „lieber Mandant oder böser Mandant“, damit Sie wissen, dass es sich um ein Berufsgespräch handelt. Das heißt: Wie– als Bundestagsabgeordneter ist das Problem ähnlich – sortieren Sie bei einmal gespeicherten Telefongesprächen aus? Wie lange brauchen Sie dafür? Wie lange hören Sie da rein? Wie können Sie ausschließen, dass Sie doch andere Gespräche mitbekommen? Allein, dass über Straftaten gesprochen wird, wird nicht ausreichen, weil Sie das ja gerade suchen. Wie kann man sich das in der Praxis vorstellen?

Die **Vorsitzende:** Herr Fechner, bitte.

Abg. **Dr. Johannes Fechner** (SPD): Vielen Dank auch von mir an die Sachverständigen. Ich glaube, die ganze Bandbreite ist klar geworden. Die einen kritisieren, es wäre ein zu großer Eingriff in die Bürgerrechte. Mehrheitlich sagen die Sachverständigen sogar, der Entwurf gehe nicht weit genug. Ich glaube, wir haben hier einen sehr ausgewogenen Entwurf, der die Interessen der Strafverfolgung und die Bürgerrechte in Einklang bringt. Das will ich mal so festhalten. Ich hätte eine Frage an die Praktiker, an die Herren Dr. Berger und Thiede, weil an diesem Gesetzentwurf kritisiert wird, er würde nichts bringen. Auf der einen Seite – ein Eingriff in die Grundrechte, dem nicht gegenüber stehe, dass Straftaten aufgeklärt werden. Könnten Sie da anhand Ihrer Praxis darstellen, wie Sie das sehen? Lassen sich Straftaten dadurch aufklären? Welche Nachteile hatten Sie dadurch, dass das Instrument seit der Entscheidung des BVerfG nicht mehr zur Verfügung stand? Vielen Dank.

Die **Vorsitzende:** Herr Flisek bitte.

Abg. **Christian Flisek** (SPD): Danke, Frau Vorsitzende. Es gibt eine Reihe von Fragen, aber ich will mich in der ersten Runde ein bisschen kürzer halten. Zunächst einmal an den Herrn Dr. Berger und an den Herrn Thiede eine Frage. Herr Dr. Berger, Sie sprechen in Ihrer Stellungnahme das Thema „Evaluierung“ an. Mich interessiert, wie man nach einer langjährigen lebhaften Debatte – der Begriff „Rechtsfrieden“ ist schon gefallen, wenn auch in einem anderen Zusammenhang – als Gesetzgeber dazu beitragen kann, dass man empirisch fundierte Grundlagen darüber bekommt, ob ein solcher Gesetzentwurf weiterhilft, präventiv wie repressiv. Ist er in Bezug auf den Straftatenkatalog zielführend oder nicht? Sie haben in Ihrer Stellungnahme, Herr Dr. Berger, einen Untersuchungsmaßstab angedeutet. Ich würde Sie bitten, diesen Maßstab zu konkretisieren – was wäre aus Ihrer Sicht notwendig? Das Gleiche bitte ich Herrn Thiede zu tun, aus der Sicht des Bundeskriminalamtes. Umgekehrt gefragt: Wir haben eine Zeit hinter uns, nachdem wir die Urteile des Verfassungsgerichts hatten, wo eine solche Vorratsdatenspeicherung nicht zur Verfügung stand. Hat das bei Ihnen empirisch zu erkennbaren Defiziten geführt? An Herrn Professor Wollenschläger gerichtet die Frage: Ein

Begriff, der meines Erachtens noch nicht legal definiert ist, der aber hier überall auftaucht, ist der Begriff „Anlasslosigkeit“. Der Kollege Dr. Ullrich hatte da vorhin schon darauf hingewiesen. Allerdings glaube ich, dass sich die Frage, was ist anlasslos oder nicht, nicht aus einer Gesamtabwägung ergibt. Ich glaube, das haben Sie auf die Frage der Unverhältnismäßigkeit bezogen, nicht auf die Frage der Anlasslosigkeit. Könnten Sie uns den Begriff „Anlasslosigkeit“ als Wissenschaftler konturieren? Es steht so ein wenig der Gedanke dahinter, Anlasslosigkeit bedeutet ohne jeden Anlass. Jetzt gibt es aber zum Beispiel im präventiven Polizeigesetz Eingriffsnormen – etwa die Schleierfahndung, die als anlasslos etikettiert werden, wo aber die sogenannte Anlasslosigkeit doch eingeschränkt und begrenzt ist. Wenn man solche Definitionen und Eingrenzungen vornimmt, ist man dann aus der Anlasslosigkeit draußen, so wie diese vom BVerfG und vom EuGH verstanden wird? Was sind Konturen eines solchen Begriffes aus rechtsdogmatischer Sicht?

Die **Vorsitzende:** Danke. Das war die erste Runde. Jetzt kommt die große Herausforderung der Antwortrunde. Wir beginnen mit Herrn Professor Wollenschläger und er hat eine Frage von Herrn Ullrich und Herrn Flisek.

SV **Prof. Dr. Ferdinand Wollenschläger:** Vielen Dank Frau Vorsitzende. Ich fange mit den begrifflichen Fragen an, die Herr Flisek und Herr Ullrich angesprochen hatten: Was heißt Anlasslosigkeit? Kann man das wissenschaftlich definieren, oder wie soll man sich dieser Frage nähern? Mit dem Punkt der Anlasslosigkeit ist mit Blick auf die Speicherung von Verkehrsdaten der Umstand angesprochen, dass Verkehrsdaten von allen Personen zu speichern sind, ohne dass diese im Sinne eines konkreten Gefahrverdachts oder des Verdachts, dass konkret Straftaten begangen wurden, dazu einen Anlass geboten hätten. Die Anlasslosigkeit in diesem Sinne entscheidet aber noch nicht über das Schicksal der Vorratsdatenspeicherung – Anlasslosigkeit heißt nämlich nicht gleichzeitig Grundlosigkeit. Der Verkehrsdatenspeicherung liegt ein verfassungslegitimer Grund zugrunde: Man erhofft sich für Ermittlungen oder für Gefahrenabwehr relevante Daten, die man später einsetzen kann. Deswegen ist ein Grund vorhanden, auch wenn der Einzelne nicht zwingend einen Anlass zur Begehung von Straftaten oder zur Verwirklichung von Gefahrtatbeständen gesetzt hat. Ein letzter Punkt dazu: Sie hatten die Schleierfahndung angesprochen, die ein bisschen in der Nähe dieser Maßnahme steht, wo man daraus schließen würde, dass der Aufenthalt in sensiblen Bereichen Anlassgrund dazu ist, dass entsprechende polizeiliche Maßnahmen ergriffen werden dürfen. So kann man sich die Anlasslosigkeit vorstellen. Das leitet dann auch gleich über zu der Frage: Was bedeutet das europarechtlich? Das ist das, was Herr Abgeordneter Ullrich insbesondere in den Vordergrund gestellt hat. Da möchte ich mal zwei Punkte klarstellen. Zum ersten Punkt: Inwieweit ist hier Europarecht überhaupt relevant? Bei der Mitteilung der Kommission habe ich zumindest gestutzt, dass die Europäische Kommission davon ausgeht, dass auch beim § 100g Absatz 1 StPO, der nichts mit unserer Verkehrsdatenspeicherung zu tun hat, sondern mit der Abfrage von Daten, die zum geschäftlichen Verkehr gespeichert wurden, das Europarecht reinspielt. Die E-Privacy-Richtlinie, die auf diesen Vorgang Anwendung findet, stellt in Ihrem Art. 1 Abs. 3 klar, dass sie keine Anwendung auf Maßnahmen der Gefahrenabwehr und der Strafverfolgung findet, so dass der Abruf zu anderweitigen Zwecken gespeicherter Daten auf jeden Fall draußen ist. Diskutabel, wenn auch zweifelhaft, ist es mit der Verkehrsdatenspeicherung im Übrigen. Der letzte Punkt, den Sie angesprochen haben – was heißt das europarechtlich? Maßgeblich ist, wie das im Lichte der Rechtsprechung zu bewerten ist. Da kann man sagen: Der EuGH hat nicht über den hier zugrunde liegenden Gesetzentwurf entschieden, sondern über die frühere Richtlinie. Alle Aussagen bezüglich einer künftigen EuGH-Entscheidung bewegen sich im Bereich des Spekulativen, weil eine erneute Gesamtabwägung anzustellen ist. Wenn Sie Parlamentarier die Gesetzentwürfe verabschieden, muss sich die Frage stellen: Verstoßen Sie gegen Europarecht bei gewissenhafter Auslegung dieser Entscheidung? Und da ist meine Position, dass diese Entscheidung jedenfalls unionsgrundrechtlich vertretbar ist. Ein letzter Punkt, der damit zusammenhängt: die Berufsgeheimnis-

träger. Auch da stellt sich die Frage der Gesamtabwägung. Wenn man das EuGH-Urteil anschaut, findet sich ein Satz, der lautet: „Zudem sieht die Richtlinie keinerlei Ausnahmen vor, so dass sie auch für Personen gilt, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen.“ Daraus zwingende Differenzierungen zu folgern, dass schon eine Speicherung oder Übermittlung verboten sein muss oder dass umgekehrt ein Schutz auf Erhebungsebene nicht ausreichend ist, ist eine relativ weitgehende Interpretation dieser Urteilspassage. Es kommt vielmehr auf die Gesamtabwägung an, und bei dieser ist maßgeblich, dass wir einen Gesetzesentwurf haben, der hinter der Richtlinie deutlich zurückbleibt. Danke schön.

Die **Vorsitzende:** Danke, Herr Professor Wollenschläger. Dann hat jetzt Herr Thiede Fragen von Herrn Ströbele, Herrn Fechner und Herrn Flisek.

SV **Frank Thiede:** Herr Ströbele, Ihre Frage bezog sich auf Berufsgeheimnisträger – wie geht die Praxis damit um, im Hinblick auf das Beispiel Rechtsanwälte? Bei der Telefonüberwachung hört man rein und nimmt wahr, dass ein Telefonat stattfindet. Wenn ich eine Anschlussinhaberfeststellung mache und sehe, dass der Anschluss zu einem Rechtsanwalt gehört, dann ist das Prozedere – jedenfalls bei uns im Bundeskriminalamt – so, dass sofort die Alarmglocken angehen und geprüft wird – im Sinne von „Halt, hier bin ich im Bereich eines Berufsgeheimnisträgers“. Das ist vergleichbar mit dem Kernbereichsschutz. Da ist vorgesehen, dass die Informationen, die ins System eingegeben und mitgeschnitten werden, sozusagen gesperrt sind. Sie sind nicht mehr abrufbar. Dann wird mit dem sachleitenden Staatsanwalt abgestimmt, ob da etwas ist, was dem Beweisverwertungsverbot unterfällt und gegebenenfalls gelöscht werden muss. Das ist etwas, was in den Bereich des Berufsgeheimnisträgers fällt, das geklärt werden muss.

(Unverständlicher Zwischenruf)

SV **Frank Thiede:** Nein. Wenn festgestellt wird, dass sich das Gespräch darauf zubewegt, merken Sie das in der Tat und dann geht das Prozedere vonstatten. So muss es sein. Bei der Vorratsdatenspeicherung ist es – mangels Zuständigkeit und Expertise und einfach von der Logik her – nicht machbar, jeden Anschluss eines jeden potentiellen Berufsgeheimnisträgers in eine Liste einzutragen, die gepflegt werden müsste, um von vornherein die Speicherung der Vorratsdaten durch den Anbieter zu vermeiden. Ob und wie das technisch vonstattengehen soll, kann ich nicht beurteilen. Aber es scheint mir sehr fragwürdig. Insofern kann sich das nur auf die Auswertung erstrecken, um diesem Recht Rechnung zu tragen.

Dann die Frage von Herrn Fechner. Es ging um die Aufklärung und Erfahrungswerte der Praxis nach der Entscheidung des BVerfG im Jahr 2010. Ich trage jetzt nicht alle Fälle vor, die wir zusammengetragen haben. Ich glaube, Sie haben den Bericht zu diesen 91 Fällen auch bekommen. Wir bekommen immer noch einzelne Fälle. Das ist keine permanente Erhebung, sondern diese Fälle werden aus dem Haus, aber auch aus den Ländern an uns herangetragen. Wir machen zweimal im Jahr eine Zusammenstellung von Rechtstatsachen durch unsere Rechtstatsachensammel- und -auswertestelle (RETASAST). Das ist ein wichtiges Instrument. Da sind auch wieder einige Fälle dabei. Gerade wurde aus Hessen ein Fall zugeliefert. Es geht um Geheimnisverrat in einem ziemlich prominent – auch in den Medien – diskutierten und dargestellten Fall. Hintergrund ist Geldwäsche und Umsatzsteuerhinterziehung im Zusammenhang mit betrügerischem Handeln von Emissionsrechten der Deutschen Bank – das ist kein Geheimnis. Der Schaden für die Bundesrepublik beträgt 1,4 Milliarden Euro. Es geht darum, dass offenbar Beteiligte bei der Deutschen Bank schon vorab von geplanten Durchsuchungsmaßnahmen erfahren haben. Das heißt, das laufende Ermittlungsverfahren bezieht sich auf Geheimnisverrat und die Frage: „Wo ist das Leck?“ Dabei stellt sich die Frage: Bekommen Sie Daten und welche Qualität haben die Daten? Bekommen Sie von jedem Betreiber, bei dem Sie angefragt haben, die eingehenden und ausgehenden Telefonate oder vielleicht nur die ausgehenden, weil die eingehenden für die Abrechnungszwecke nicht relevant sind? Es gibt eine sehr unterschiedliche Speicherpraxis. Bekommen Sie die IMEI, also die Gerätekennung? Manche Betreiber machen das, andere nicht. Das ist ganz heterogen. Es ist oftmals auch ein

wichtiger Ermittlungsansatz, wenn Karten gewechselt werden und dann aufgrund der IMEI die Person zu ermitteln oder eine IMEI-Telefonüberwachung umzusetzen ist. Dann die Frage, wie weit die Daten zurückliegen – manchmal bekommen Sie sechs Monate, manchmal weniger. Dafür ist es wichtig, eine konsolidierte und harmonische Auskunftspraxis der Betreiber zu haben, damit es eben nicht – und das ist leider der Befund – vom Zufall abhängt, welche Dienstleistungen und welchen Anbieter der Beschuldigte nutzt. Beim einen bekommen Sie etwas, beim anderen nicht. Das ist das Dilemma, in dem wir uns befinden. Bei dem Fall mit dem Geheimnisverrat, den ich exemplarisch vorgestellt habe, kommen die Kolleginnen und Kollegen im Moment nicht weiter. Dann war die Frage von Herrn Flisek, wie man ohne Vorratsdatenspeicherung empirisch damit umgeht. Das deckt sich mit dem, was ich gerade zur Frage von Herrn Dr. Fechner ausgeführt habe. Wir haben von den Praktikern tagtäglich das Dilemma auf dem Tisch, dass sie – wenn sie bei den IP-Adressen nichts haben – die Ermittlungen auch gleich wieder einstellen können. Bei der Telekom kommen Sie mit sieben Tagen noch weiter, um den Anschlussinhaber zu ermitteln. Bei der Masse der Anbieter haben Sie die Speicherung von einem oder null Tagen, und dann kommen Sie mit der IP-Adresse gar nicht weiter.

Auch bei der Telefonie und den Funkzellendaten gibt es solche Erfahrungswerte, die nicht nur von uns im BKA festgestellt werden, sondern gerade auch von den Ländern. Sie müssen auch auf die Standortdaten zugreifen, in Form zumindest der Funkzellendaten, um die Zuordnung einer Person zu einem Ort zeitlich und regional begrenzt vornehmen zu können.

Die **Vorsitzende:** Können Sie bei der Beantwortung alle ein bisschen an die Zeit denken? Ich muss Sie, Herr Flisek, noch einmal auf die Liste nehmen. Bei den Anhörungen kommen immer viele Kollegen. Herr Starostik hat eine Frage von Frau Wawzyniak.

SV **Meinhard Starostik:** Es war die Frage nach der Eingriffstiefe und die Frage, was man aus den Verkehrsdaten herauslesen kann. Ich darf zu Beginn meiner Antwort nochmals das BVerfG zitieren, das sagt, dass es zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland gehört, die Freiheitswahrnehmung der Bürger nicht total zu erfassen und zu registrieren. Das ist ein ganz wichtiger Satz, den man bei allen Überlegungen vorweg stellen muss. Da geht es um die Frage: Was für einen Staat will man haben? Will man einen Staat, der vorgibt, möglichst viel Sicherheit zu erzeugen, indem er alles überwacht, oder will man einen Staat, der seinen Bürgern Freiheit lässt? Was man mit den Daten machen kann, ist bereits Gegenstand der mündlichen Verhandlung vor dem BVerfG gewesen. Ich habe damals die Massenverfassungsbeschwerde vertreten. Da hat die Gutachterin, Constanze Kurz, Beispielsdarstellungen gemacht, wie man die Verbindungsdaten auswerten kann, wie man aus der Abfolge der Gespräche und aus dem Zeitpunkt, wann ein Telefonat geführt wird, ermitteln kann, welche persönlichen Beziehungen zu dem anderen Gesprächspartner bestehen, welche Probleme möglicherweise da sind, wenn ein Gesprächspartner erst den Arzt anruft und dann eine Klinik oder ähnliche Dinge. Welche Probleme gibt es, wenn jemand erst seine Bank anruft und dann seinen Anwalt? Diese Aussagekraft der Verbindungsdaten ist damals noch als relativ abstrakte Gefahr gesehen worden. Deswegen habe ich vorhin in meiner Stellungnahme auch darauf hingewiesen, dass wir fünf Jahre weiter und fünf Jahre schlauer sind. Wir haben drei Beispielsdarstellungen gehabt, die auch in der Öffentlichkeit viel diskutiert worden sind. Einmal ist das der Abgeordnete des letzten Bundestages, Malte Spitz, der auf ZEIT ONLINE visualisiert hat, wie es aussieht, wenn man die gespeicherten Verbindungsdaten zusammenfasst und darstellt, wann er sich wohin bewegt hat und was er während dieser Zeit gemacht hat, welche SMS, welche Internetnutzung, mit wem er telefoniert hat. Ähnliches gibt es von einem Schweizer Nationalrat, Balthasar Glättli, und einem holländischen Akademiker, Ton Siedsma. Die beiden Letzteren sind veröffentlicht auf netzpolitik.org. Diese Darstellungen gehen doch ganz tief in den persönlichen Bereich. Denn die Daten, die dort erhoben sind, gehen rund um die Uhr. Man sieht, wann jemand mit Vertrauenspersonen telefoniert und wann jemand berufliche Kontakte aufgenommen hat. Diese Eingriffstiefe muss noch einmal neu erörtert werden. Man kann

nicht einfach auf dem Standpunkt stehen bleiben, der 2010 „State of the Art“ und Stand der Erkenntnis war. Schönen Dank.

Die **Vorsitzende:** Danke sehr. Dann ist jetzt Frau Dr. Sandkuhl mit Fragen von Frau Keul und Herrn von Notz an der Reihe.

SVe **Dr. Heide Sandkuhl:** Zum Thema „Datenhehlerei“ von Frau Keul und dem § 202d StGB, der ausweislich des Entwurfes eingeführt werden soll. Was als erstes auffällt: Das Gesetz, mit dem diese Normen eingeführt werden sollen, vermittelt den Eindruck der Datensicherheit – angeblich Höchstspeicherfristen. Da kann man den Eindruck gewinnen, es geht um den Schutz von Daten. Und dann kommt plötzlich ein Straftatbestand, der § 202d Absatz 1 StGB, die Datenhehlerei. Da kommt man ins Überlegen, denn wir haben schon die §§ 43 und 44 des Bundesdatenschutzgesetzes. Wenn man sich die Zahl der Fälle anschaut, die nach dieser Vorschrift verfolgt, respektive abgeurteilt wurden, waren das ziemlich wenige, sodass sich hier wieder die Frage der rechtstatsächlichen Notwendigkeit stellt. Aber – lassen Sie mich das als unerfreulich bezeichnen – was in Absatz 3 dann eingeführt werden soll, ist nichts anderes als die Legitimierung von illegal erlangten Daten – Stichwort: Ankauf von Steuer-CDs. Da heißt es nämlich in Absatz 3 Satz 1: „Absatz 1 gilt nicht für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen.“ Und dann: „Dazu gehören insbesondere 1. solche Handlungen von Amtsträgern oder deren Beauftragten, mit denen Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zugeführt werden sollen.“ Das ist nichts anderes als die Legitimierung dieses fragwürdigen Ankaufs. Es erstaunt deswegen, weil Herr Ströbele schon angedeutet hat, was er alles in Untersuchungsausschüssen gelernt hat. Wenn ich daran denke, was wir durch die Bekundungen von Herrn Snowden erfahren haben und wer wann wie welche Daten abgreift, und mir dann vor Augen halte, dass sich derjenige Amtsträger, der sich dieser Daten bedient, um sie einem Strafverfahren zuzuführen, nicht strafbar macht, finde ich das ein ganz fatales Signal und eine groteske Situation. Auf der einen Seite bekommt man offenbar die NSA-Folgen nicht in den Griff und auf der anderen Seite kommt eine Vorschrift, die es legitimieren würde, auch auf solchem Wege abgefangene Daten in ein Strafverfahren führen. Nummer 2 sagt – und jetzt, Frau Keul, komme ich zu Ihrer Frage: „solche beruflichen Handlungen der in § 53 Absatz 1 Satz 1 Nummer 5 StPO genannten Personen, mit denen Daten entgegengenommen, ausgewertet oder veröffentlicht werden“, fallen nicht unter diese Strafbarkeit. Da können sich Bestimmbarkeitsprobleme ergeben, insbesondere wenn es um die Journalisten geht, nämlich um die Frage: Was ist noch die berufliche Handlung des Journalisten? Da will ich Probleme nicht ausschließen. Dann haben Sie nach den Berufsgeheimnisträgern, § 100g StPO, im Entwurf Absatz 4 gefragt. Ich bin mir nicht sicher, ob ich Ihre Frage richtig verstanden habe. Die Vorschrift regelt zum einen eine Erhebungs-, aber auch ein Verwendungsverbot. Jetzt hatten Sie einen Einwand der Kommission angesprochen, der auf die Verstrickungsregelung hinausgeht. Ich glaube nicht, dass die EU-Kommission gemeint hat, Anwälte würden jetzt per se Straftaten begehen. § 100g StPO regelt zwar ein Erhebungsverbot, aber Sie dürfen nicht übersehen, dass – das läuft ja in einem zweistufigen Verfahren – zunächst einmal sämtliche Daten gespeichert werden sollen, also auch die der Berufsgeheimnisträger, etwa der Anwälte. Schützen will man sie dadurch, dass man ein Erhebungsverbot einführt. Wir kritisieren die Speicherung von Daten, die Berufsgeheimnisträger angehen: Das soll unterbleiben. Als Einwand wurde uns immer entgegengehalten, es sei nicht möglich, sämtliche Berufsgeheimnisträger zu erfassen. Das leuchtet mir aber insofern nicht ein, wenn man den § 99 TKG anschaut. In dem Entwurf ist geregelt ist, dass Berufsgruppen, die in § 99 TKG genannt sind, nicht von der Speicherung erfasst werden, etwa Telefonseelsorger. Aber wenn das möglich ist, ist es doch zum Beispiel bei den Anwälten viel leichter möglich. Es gibt Anwaltsverzeichnisse. Da stehen alle drin. Diese Differenzierung leuchtet mir nicht ein, denn das können Sie vergleichen: der Telefonseelsorger, der spezielle Gesundheitsberater und auch der Rechtsanwalt, der Arzt, aber auch der Abgeordnete – sämtliche Tätigkeiten sind auf Vertrauen angelegt. Das wäre wahrlich neu, wenn plötzlich Daten von Berufs-

geheimnisträgern gespeichert würden. Und noch einmal zu diesem – ich will es gutwillig sagen – Bemühen um Schutz und die Einführung eines Erhebungs-verbotes. Das hakt auch – warum? Das Erhebungsverbot setzt voraus, dass es sich um Daten handeln muss, die voraussichtlich Erkenntnisse erbringen würden, über die die Berufsgeheimnisträger das Zeugnis verweigern dürfen. Aber wie wollen Sie das feststellen? Sie müssten in den Inhalt schauen und sagen: Das betrifft jetzt das Anwalt-Mandats-Verhältnis. So kann das nicht funktionieren. Das geht viel zu weit in Richtung Inhaltskontrolle. Wenn man eine solche Regelung einführen wollte, müsste diese Zusatzvoraussetzung gestrichen werden. Die Norm darf nur so lauten, dass die Erhebung von Verkehrsdaten, die die Berufsgeheimnisträger im Sinne von § 53 StPO betreffen, unzulässig ist.

Ihre Frage, Herr von Notz, nach der Bedeutung der Vorratsdatenspeicherung für die Gesamtrechnung und die Tiefe des Grundrechtseingriffes. Lassen Sie mich das mit einem Zitat aus der Entscheidung des BVerfG kurz beantworten: „Ein besonders schwerer Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt.“ Mit anderen Worten: Mit der Vorratsdatenspeicherung wird etwas eingeführt, das unsere Rechtsordnung bislang nicht kennt. Sie kennen mit Sicherheit die Formulierungen aus dem Urteil des BVerfG und das, was das BVerfG hervorgehoben hat. Was kann das anrichten? Ein diffuses Gefühl des Beobachtetwerdens. Das kann so weit gehen, dass man sich als Bürger nicht mehr traut, seine Meinung zu äußern, und damit – kurz gesagt – die Demokratie gefährden. Durch die Vorratsdaten-speicherung würde die Möglichkeit geschaffen werden, und das darf man nicht aus dem Auge verlieren, sehr genaue Schlüsse auf das Privat-leben unbescholtener Bürgerinnen und Bürger, in Deutschland 80 Millionen an der Zahl, mithin auf Gewohnheiten des täglichen Lebens, Aufenthalts-orte, ausgeübte Tätigkeiten und soziale Beziehungen zu gewinnen. Danke.

Die **Vorsitzende:** Danke. Herr Franosch hat Fragen von Frau Winkelmeier-Becker und Herrn von Notz.

SV **Rainer Franosch:** Vielen Dank. Frau Winkelmeier-Becker – zur Straftat von erheblicher Bedeutung: Ich habe die Mitteilung der Europäischen Kommission gelesen. Hier ist davon die Rede, dass möglicherweise die Bezeichnung „Straftat von erheblicher Bedeutung“ nicht hinreichend abgegrenzt ist. Diese Bedenken greifen nicht durch, denn wir haben im Gesetzentwurf einen Katalog. Darüber hinaus gibt es eine Verfassungsgerichts-rechtsprechung dazu, was unter einer Straftat von erheblicher Bedeutung zu verstehen ist. Es gibt auch eine BGH-Rechtsprechung dazu. Das sind Straftaten, die mindestens mit drei Jahren bzw. mit einer Höchstfreiheitsstrafe von fünf Jahren versehen sind, so dass also hier die befürchtete Konturlosigkeit nicht gegeben ist. Was den Katalog im Gesetzentwurf betrifft, ist insbeson-dere festzustellen, dass die Straftaten des gewerbsmäßigen Betruges und Computerbetruges nicht erfasst sind. 74 Prozent aller Cybercrime-Delikte betreffen diesen Bereich. Das fällt komplett raus. Das sind Straftaten, die einen erheblichen Schaden anrichten, die auch im Katalog des § 100a Absatz 2 StPO enthalten sind. Darüber hinaus ist im neuen Katalog der § 184b Absatz 1 StGB nicht enthalten, das heißt die Verbreitung von Kinderpornographie. Wir haben nur § 184b Absatz 2 StGB im neuen Katalog. Das ist nur die bandenmäßige oder gewerbsmäßige Begehungsweise. Insofern fehlt das Verbreiten von Kinderpornographie im Rahmen des Absatzes 1. Der Absatz 1 ist immerhin mit einer Strafdrohung von drei Monaten bis zu fünf Jahren versehen. Ich kann nur noch einmal betonen, dass kein Anlass dafür besteht, den Katalog im neuen Gesetz abweichend von dem des § 100a Absatz 2 StPO zu formulieren. Das hat weder das BVerfG gefordert, noch ergibt sich dafür irgendein Hinweis. Es ist nicht nachvollziehbar, dass der Abruf von Verkehrsdaten, der nach der Verfassungsgerichtsrechtsprechung ein geringerer Eingriff ist als die Inhaltsüberwachung, stärkeren Schranken unterliegt als die Inhaltsüberwachung. Das ist unlogisch und nicht verfassungsmäßig geboten. Herr von Notz, Sie hatten nach dem Urteil des EuGH im Hinblick auf die Berufs-geheimnisträger gefragt. Wir haben von Herrn Professor Wollenschläger gehört, dass der EuGH eine Gesamtwürdigung vorgenommen hat und – anders als das BVerfG –nicht gesagt hat, dass es einen Fahrplan geben muss. Der EuGH hat uns keinen Fahrplan gegeben, sondern eine Gesamtabwägung vorgenommen, in denen

einzelne Punkte relevant sind. Das Abrufverbot genügt, um dem Schutz der Berufsgeheimnisträger Rechnung zu tragen. Wir dürfen eines nicht vergessen: Selbstverständlich stellt bereits die Speicherung der Daten einen Eingriff dar. Das ist aber die erste und viel geringere Stufe. Wir dürfen nicht vergessen, dass der Abruf immer anlassbezogen erfolgt. Der Abruf der Daten erfolgt verdachtsbezogen. In dem Moment, wo ich einen verdachtsbezogenen Abruf und einen Berufsgeheimnisträger habe, ist dem durch das Übermittlungsverbot ausreichend Rechnung getragen. Der EuGH hat nicht gefordert, das von der Speicherung auszunehmen. Natürlich gäbe es die Möglichkeit, bei den Telekommunikationsprovidern Listen zu führen, in denen sich Berufsgeheimnisträger eintragen lassen können. Warum soll das nicht gehen? Ich habe als Begründung gehört, das sei datenschutzrechtlich unzulässig. Das teile ich nicht. § 4a BDSG erlaubt eine Einwilligung. Das heißt, wenn ich mich als Berufsgeheimnisträger registrieren lasse, geht das. Ich glaube aber nicht, dass das geboten ist. Danke schön.

Die **Vorsitzende:** Herr Frank hat vier Fragen von Frau Winkelmeier-Becker, Herrn Ullrich, Herrn von Notz und Herrn Ströbele. Danach gibt es eine weitere Fragerunde.

SV **Christoph Frank:** Ich habe den Vorteil, Bezug nehmen zu können. Zu den Fragen von Frau Winkelmeier-Becker kann ich mich auf Herrn Franosch beziehen. Es gibt ein Gefälle zwischen § 100g Absatz 1 StPO und § 100g Absatz 2 StPO, der deutlich strengere Voraussetzungen bietet – gerade was den Straftatenkatalog angeht. Man könnte die Rechtsprechung zur Erheblichkeit von Straftaten, die eine Speicherung nach § 100g Absatz 1 StPO erlaubt, zur Sicherung finanzieller Interessen gespeicherter Daten, als Anleihe für den Gesetzgeber verstehen. Man könnte die Mindeststrafandrohung als Vorgabe nehmen, um den Begriff der erheblichen Bedeutung auszufüllen. Die Schlüssigkeit des Straftatenkatalogs ist nicht gegeben. Wir haben das in der schriftlichen Stellungnahme ausgeführt. Einige Tatbestände fehlen. Den Kinderpornografiebereich hat Herr Franosch genannt. Aufgenommen werden sollten ferner Computerstraftaten oder der Schutz des lauteren Wettbewerbs in § 17 UWG. Und auch der neue § 202d StGB, die Datenhehlerei, ist nicht in den Katalog aufgenommen. Es wäre richtig, wie das schon mehrfach betont worden ist, an den § 100a StPO anzuknüpfen. Der § 100a StPO, der eine deutlich weitergehende Qualität der Überwachung des Inhalts vom Telekommunikationsverkehr betrifft, ist verfassungsgemäß. Wenn man dann auch noch klarstellt, dass die Grundtatbestände Anknüpfungstatbestände sind, hat man ein in sich geschlossenes System. Um bei den Sexualdelikten zu differenzieren, sehe ich keine Begründung. Das mag an aktuellen kriminalpolitischen Überlegungen angeknüpft sein, überzeugt aber strafrechtsdogmatisch nicht. Die Fragen von Herrn Ullrich sind durch Herrn Professor Wollenschläger beantwortet. Herr von Notz hat den Rechtsfrieden angesprochen. Er fürchtet, dass die Neuregelung den Rechtsfrieden nicht befördert. Man kann natürlich grundsätzlich darüber sprechen, ob Strafrecht überhaupt diese Funktion übernehmen kann und ob Strafprozessrecht diese Funktion übernehmen kann. Es geht um Eingriffe des Staates, die aber begründet, gerechtfertigt und beauftragt sind durch die Verfassung. Eine effektive Strafverfolgung ist vom Staat zu leisten. Die Kautelen, die vorgesehen sind, gehen weit über das hinaus, was europarechtlich gefordert ist. Wir werden immer wieder nach Statistiken gefragt. Wir können keine Statistiken liefern, weil es immer um die Frage geht: Was wäre wenn? Diese Frage stellt sich jeder Polizeibeamte, der eben nicht die Anregung an uns heranträgt, Vorratsdatenspeicherungsdaten zu nutzen. Die Schere im Kopf ist überall angekommen und führt zu einem Vollzugsdefizit bei den Ermittlungen. Das ist aus unserer Sicht sehr bedenklich, weil es Strafbarkeitslücken bietet, weil es organisierter Kriminalität Möglichkeiten gibt, tätig zu werden, die man mit anderen Ermittlungsmitteln durchaus einschränken könnte. Zur Regelung zu den Berufsgeheimnisträgern: § 100g Absatz 4 StPO regelt das, was man regeln kann. Es sind alle Vorsichtsmaßnahmen getroffen, um sicherzustellen, dass das besondere Verhältnis zwischen Rechtsanwälten und den Mandanten geschützt ist und geschützt bleibt. Inwieweit technische Möglichkeiten bestehen, bereits die Datensammlung einzuschränken, vermag ich nicht zu beurteilen. Der Gesetzentwurf trägt das aber mit Überzeugung vor.

Zur Frage von Herrn Ströbele, ob wir in der Praxis und in den Stellungnahmen die Erfahrungen, die der NSA-Ausschuss derzeit macht, ausblenden: Natürlich machen wir das nicht. Wir sind nicht naiv und wir sehen durchaus, dass die Datenflut, die dadurch entsteht, dass Privatpersonen ihre Daten nahezu ungeschützt in einen Kommunikationsvorgang geben, selbstverständlich die Gefahr des Missbrauchs bietet. Beim Gesetz hier geht es aber darum, Regeln aufzustellen, wie die Strafverfolgungsbehörden, wie die Gerichte mit diesen Daten umgehen und sie nutzen können, wenn der konkrete Verdacht einer strafbaren Handlung besteht. Wir haben Regelungen in der StPO, die durch Verwertungsverbote Schutz für die Betroffenen bieten. Wenn Staatsanwaltschaften und Gerichte diese Bestimmungen so anwenden, wie sie der Gesetzgeber vorgegeben hat – und davon dürfen wir ausgehen –, ist ein Schutzniveau gegeben, das allen rechtsstaatlichen Anforderungen genügt.

Die **Vorsitzende:** Herr Dr. Berger, Sie sind der letzte in der Runde und haben Fragen von Frau Wawzyniak, Herrn Ströbele, Herrn Fechner und Herrn Flisek.

SV **Dr. Nikolaus Berger:** Zunächst zu der Frage, warum man die Vorratsdatenspeicherung braucht, obgleich in den von mir aufgeführten Fällen der Angeklagte ermittelt und verurteilt werden konnte. In den Fällen, die ich aufgeführt habe, war es ein glücklicher Zufall, dass die Daten gerade bei den Telefongesellschaften gespeichert worden sind, was eben vom Zeitpunkt der Tatentdeckung bzw. der Anzeigenerstattung abhing und von den wirklich vollkommen unterschiedlichen Speicherfristen. Diese reichen von wenigen Tagen bis zu mehreren Monaten, in denen unterschiedliche Gesellschaften Daten speichern. Niemand im Saal wird eine solche Zufälligkeit mit einer rechtsstaatlichen Justiz verbinden. Insofern zeigen diese Beispielsfälle zunächst nur auf, wie wichtig die Verkehrsdaten bei exemplarischen Deliktsbereichen zur Aufklärung waren, um überhaupt erst einmal den Tatverdächtigen zu identifizieren. Wenn man diese Verkehrsdaten nicht als geschäftlich noch gespeicherte Daten gehabt hätte, wären diese Delikte nicht aufgeklärt worden. Ich will jetzt einmal zu der Frage springen, welche Defizite es gegeben hat, seitdem es die Vorratsdatenspeicherung nicht mehr gibt. Für mich gab es zwei Augenöffner, die ich in meinem vorbereitenden Papier genannt habe. Das eine war der Mord ohne Leiche. Den hätte man ohne damals noch längerfristig gespeicherte Verkehrsdaten nicht aufklären können. Das zweite waren die Ermittlungen, und zwar jetzt in negativer Hinsicht, im NSU-Fall. Damit war ich per Zufall am Anfang als Ermittlungsrichter befasst. Ich hatte damals Frau Zschäpe vernommen. Da war die Ermittlungsakte noch ganz dünn und man erfuhr: Es gibt fünf oder sechs zerstörte Handys im Schutt des zerstörten Hauses bzw. des Wohnwagens. Mit großem Interesse habe ich mir angeschaut, ob man dazu etwas auswerten konnte. Das konnte man damals nicht. Ich habe jetzt gehört, man konnte hinterher bei der einen oder anderen SIM-Karte ermitteln, auf wen die ausgestellt war. Damals stellte sich mir schlagartig die Frage: Was hätte man machen können, wenn man von diesen verschiedenen Telefonen bzw. SIM-Karten die Daten hätte haben können? Die Frage, welche Lücken seither eingetreten sind, ist von Herrn Thiede beantwortet worden. Da gibt es Statistiken beim BKA. Beim Bundesgerichtshof als Revisionsinstanz bekommen wir nur die Fälle mit, in denen man zu Beginn des Verfahrens noch etwas hat erheben können. Insofern also Positivbeispiele, und davon habe ich eben einige exemplarisch aufgelistet. Beim Thema NSA-Zugriff schließe ich mich der Stellungnahme von Herrn Frank an. Das ist ein Punkt, der in die Verhältnismäßigkeitsabwägung eingestellt werden muss. Eine Evaluierungskommission sollte man – wenn ich das kritikwürdige Freiburger Gutachten betrachte – unbedingt mit Praktikern besetzen und diese nicht nur interviewmäßig anhören. Damit meine ich zum einen Praktiker, die den Anfang des Verfahrens beurteilen können, wo mit Daten überhaupt ein Ermittlungsverfahren gegen einen konkreten Verdächtigen zustande kommen kann. Zum anderen meine ich damit aber auch Praktiker, die beurteilen können, inwieweit Daten als Indiz im Rahmen einer Indizienkette am Ende des Verfahrens eine Rolle gespielt haben. Ich könnte mir vorstellen, dass man aus mehreren OLG- oder Landgerichtsbezirken, insbesondere beim Verfahrensbeginn, vielleicht bei den Ermittlungsrichtern ansetzt und Verfahren sammelt. Denn die Ermittlungsrichter sind

diejenigen, die die Beschlüsse über die Erhebung und dann die weitergehenden Beschlüsse gegebenenfalls über die Inhaltskontrolle fassen. Das sind die Stellen, bei denen das anfällt. Da kann man über einen bestimmten Zeitraum eine Erhebung machen. Ich bin sicher, man wird feststellen, dass es Alltag ist, dass diese Daten etwas nutzen.

Die **Vorsitzende:** Danke an die Sachverständigen. Jetzt haben wir schon fast zwei Stunden miteinander verbracht. Ich habe noch sechs Fragestellungen. Ich weiß nicht, ob noch ein oder zwei dazukommen. Das muss aber nicht sein. Wir machen eine Runde mit mehr Zeitdisziplin als in der ersten Runde. Ich meine nicht nur die Sachverständigen, sondern auch uns. Wir können ja auch lange Fragen stellen oder kurze. Jetzt habe ich Herrn Sensburg, Frau Künast, Herr Hakverdi, Herrn Flisek, Frau Winkelmeier-Becker, Herrn Fechner. Herr Flisek zieht seine Frage zurück – gut. Gibt es sonst neue Wortmeldungen? Das ist nicht der Fall, dann ist Herr Sensburg dran.

Abg. **Dr. Patrick Sensburg** (CDU/CSU): Ganz herzlichen Dank, Frau Vorsitzende. Ich mache es relativ kurz. Ich habe eine Frage an Herrn Franosch und eine Frage an Herrn Thiede. Zuerst die Frage an Herrn Franosch. Wenn ich die Einlassungen der Sachverständigen sehe, ist doch deutlich geworden, dass im Verhältnis fünf zu anderthalb eine klare Aussprache für das Speichern von Daten ist. Ich würde gerne noch einmal wissen: Wie entwickeln sich eigentlich die Straftaten im Internet? Man könnte fragen: Warum brauchen wir eigentlich diesen ganzen Aufwand? Können wir nicht mit klassischen Methoden entsprechende Straftaten ermitteln? Ich habe hier die ganze Zeit noch parallel im kriminalwissenschaftlichen Lehrbuch gewälzt und nach Methoden geschaut. Können Sie aus Ihrer Erfahrung aufzeigen, warum es möglicherweise bei manchen Straftaten ausschließlich die Chance gibt, durch retrogrades Betrachten eine Aufklärung oder das Verhüten weiterer Straftaten hinzubekommen? Es scheint ja selbst in anderen Fraktionen inzwischen festzustehen, dass im Internet Straftaten nicht existieren dürfen, die in der reellen Welt – wenn man es mal so sagen darf – existieren. Da hat es auf jeden Fall in den letzten Tagen mehrere Statements aus der Fraktion BÜNDNIS 90/DIE GRÜNEN gegeben, wo gesagt worden ist: Das, was sonst verboten ist, darf auch im Internet nicht stattfinden. Das scheint ein gewisser Lernprozess bei manchen gewesen zu sein.

(Unverständlicher Zwischenruf)

Abg. **Dr. Patrick Sensburg** (CDU/CSU): Ich wollte auch gar nicht lustig sein, Herr Kollege. Das ist eine klare Aussage aus Ihrer Fraktion gewesen, von Herrn Özdemir übrigens. Ich freue mich, wenn ein gewisser Erkenntnisgewinn vorhanden ist. Von daher würde ich gerne von Herrn Franosch etwas mehr Aufklärung in dieser tatsächlichen Hinsicht haben. Von Herrn Thiede würde ich gerne wissen, warum nicht der „Quick Freeze“ funktioniert. Warum kann ich nicht Daten in einem bestimmten Zeitpunkt einfach speichern und wieder auf die zurückgehen? Warum gerade das Retrograde? Das ist in Ihren Ausführungen angeklungen, das würde ich aber gerne mehr beleuchtet wissen.

Abg. **Renate Künast** (BÜNDNIS 90/DIE GRÜNEN): Ich sehe, dass die Meinungen hier fünf zu zwei sind. Ich habe dafür aber auch eine Erklärung mit Blick auf die Benennung der Sachverständigen. Das wollte ich mal für das Protokoll andeuten und zu Herrn Dr. Berger sagen: Sie haben bei den beiden Fällen bezüglich Frau Zschäpe und den Handys gesagt: Was hätte man alles haben können, wenn man besser oder mehr bezüglich der Inhalte oder Verkehrsdaten hätte erfragen können? Ich kann mir jetzt nicht verkneifen zu sagen: Was hätte man alles haben können, wenn man schon ungefähr zehn Jahre vorher fachlich besser gearbeitet hätte und vielleicht mal eine TKÜ beantragt hätte. Zu meinen Fragen: Einmal will ich eine Frage an Herrn Frank stellen, weil ich die Sorge habe, dass all die Schutzmaßnahmen oder Schutzmechanismen, von denen Sie gesprochen haben, in der Realität gar nicht funktionieren. Sie haben gesagt, die Schutzmaßnahmen, auch für Berufsgeheimnisträger, seien in dem Gesetzentwurf getroffen worden, obwohl Sie nicht wissen, inwieweit etwas technisch möglich ist. Das war für mich ein Widerspruch. Entweder sind alle Maßnahmen getroffen – dann muss man aber wissen, dass es technisch möglich ist, auch gegen den Zugriff der *Five-Eyes*-Staaten und der NSA. Ich sehe das als Mangel bei der Benennung der Sachverständigen an, da die Frage, ob diese

Sicherheit entstehen kann, nicht geklärt ist. Sie haben außerdem gesagt, dass es Sicherheit gebe und durch Staatsanwälte und Richter ein hohes Schutzniveau gewährleistet werde: Meine Sorge gilt einem leerlaufenden Richtervorbehalt. Gibt es überhaupt Untersuchungen zu der Frage, wie oft in der Praxis Anträge von Richtern und Richterinnen abgelehnt worden sind? Es dürfte ja nicht so sein, dass immer stattgegeben wird, weil Staatsanwälte und Polizei so toll arbeiten. Dann würde der Richtervorbehalt keinen Sinn ergeben. Es erfordert ja einiges an Prüfung. Meine zweite Frage geht an Herrn Professor Wollenschläger zur Gesamtbetrachtung. Bei der Frage der Vereinbarkeit mit der Rechtsprechung geht es immer um die Gesamtbetrachtung und Gesamtbelastung der Menschen durch Überwachung und die Konsequenzen für die Freiheit. Das BVerfG hat sinngemäß gesagt: Du musst dich frei fühlen, um kommunizieren zu können und nicht das Gefühl haben, in all deinen Lebensäußerungen überwacht zu sein. Damit muss man sich auseinandersetzen. Da muss man eine Balance hinbekommen. Wir müssen das in ein grundgesetzliches Gesamtgefüge einbinden. Dazu gehört die Gesamtbetrachtung aller Belastungen. Wo ist in dieser Gesamtbetrachtung all das geblieben, was wir seit Snowden wissen? Isoliert sagt die Gesamtbetrachtung, dass das alles keine hohe Belastung ist, dass es gespeichert und technisch nach neuesten Stand gesichert sei. Wer von uns glaubt aber, dass die NSA nicht dennoch zugreifen könnte? Bei der Gesamtbetrachtung müsste darauf eingegangen werden, dass eine noch so versuchte sichere Speicherung in Deutschland für die NSA durchsichtig sein kann und zwar für alle, die vier oder sechs Wochen gespeichert werden und für die Berufsgeheimnisträger sowieso. Das ist beinahe ein „Angebot“ an die NSA: Hier ist die Stelle, die du hacken musst, um Berufsgeheimnisträger, einschließlich Abgeordneter, zu kriegen und deren Kontakte. Angela Merkels Handy wurde abgehört, andere auch. Auf diesen Bereich, den ich mal die „Post-Snowden-Ära“ nenne, und was das eigentlich heißt, ist von Ihnen keiner eingegangen.

Abg. **Metin Hakverdi** (SPD): Meine erste Frage geht an Herrn Frank und Herrn Franosch. Was spricht vor dem Hintergrund der sehr dynamischen technischen Entwicklung dagegen, in fünf Jahren zu sagen: Das Gesetz läuft aus, und dann schauen wir, ob es etwas gebracht hat oder nicht. Vielleicht gibt es dann technische Entwicklungen, die andere Dinge vollkommen unsinnig machen. Die klassische „sunset legislation“ ist zwar unserer Rechtskultur nicht inhärent, aber wir haben ein paar Beispiele dafür. Die nächste Frage geht insbesondere an Frau Dr. Sandkuhl und Herrn Starostik. Können Sie uns einen Hinweis geben, wie wir ganz praktisch eine mögliche Evaluierung oder ein Fazit ziehen können. Herr Dr. Berger hat das sehr konkret gemacht; bei den anderen wünsche ich mir das, zum Verfahren, zu materiellen Kriterien. Ich maße mir nicht an zu wissen, was in fünf Jahren ist, sowohl von der rechtlichen Entwicklung als auch von der technischen Seite her gesehen. Rechtlich ist das an das Kriterium der Notwendigkeit gebunden. Aber wir sind alle keine Propheten. Mich würde freuen, dazu aus der Praxis ein paar Vorschläge zu hören.

Die **Vorsitzende**: Jetzt haben Frau Winkelmeier-Becker und Herr Fechner das Wort.

Abg. **Elisabeth Winkelmeier-Becker** (CDU/CSU): Vielen Dank. Ich hätte noch einmal eine Frage an Herrn Franosch und an Herrn Thiede. Wir hatten eine Zeit lang die Vorratsdatenspeicherung. Mich würde interessieren, ob es in dieser Zeit etwas gegeben hat, wo das schiefgelaufen ist. Ist etwas gehackt worden? Sind Daten unberechtigt abgefragt worden? Hat sich jemand beschwert? Und: Was muss denn derjenige befürchten, der im Zusammenhang mit einer Person erscheint, deren Daten abgerufen worden sind? Was ist der *worst case* für denjenigen, der dann – ohne selbst verstrickt zu sein – auf so einer Liste erscheint?

Die **Vorsitzende**: Danke. Herr Fechner.

Abg. **Dr. Johannes Fechner** (SPD): Ich hätte eine Frage zur jüngsten Kritik der EU-Kommission an der Speicherpflicht im Inland an Herrn Professor Wollenschläger und an Herrn Dr. Berger. Der Gesetzentwurf setzt sich bei § 113b StPO intensiv mit dieser Abwägung auseinander. Wie fällt Ihre Abwägung aus? Ist es ein Eingriff in die Grundrechte, beziehungsweise wird die Dienstleistungsfreiheit ungerechtfertigt beeinträchtigt? Oder muss man nicht sagen, dass der Schutz der Daten, den ich durch die Inlandsspeicherung unzweifelhaft besser unter Kontrolle habe, als

wenn im Ausland die Speicherung stattfindet, diesen Eingriff in die Dienstleistungsfreiheit rechtfertigt?

Die **Vorsitzende**: Dann sind wir durch und fangen wieder vorne bei Herrn Dr. Berger mit den Antworten an. Sie hatten eine Frage passend von Herrn Fechner.

SV **Dr. Nikolaus Berger**: Auf mich bezog sich die letzte Frage, die Herr Professor Wollenschläger vorhin beantwortet hatte. Ich selber kann nur die Einschätzung von mir geben, dass wir in Deutschland den höchsten Sicherheitsstandard haben und ich es deswegen begrüße, wenn der Gesetzentwurf in der Hinsicht so bleiben würde, wie er ist.

SV **Christoph Frank**: Vielleicht zur Klarstellung: Wenn ich vorher gesagt habe, dass ich die Kontrollmöglichkeiten nicht einschätzen kann, dann bezog sich das auf die Speicherung im Vorfeld, auf die Speicherung von Daten von Berufsgeheimnisträgern, um sie bereits im Bereich der Speicherung auszuschließen. Nur darum ging es mir. Die anderen Schutzmechanismen funktionieren aus meiner Überzeugung und werden künftig funktionieren. Es gibt natürlich Anträge von Staatsanwälten, die abgelehnt werden. Eine Statistik gibt es dazu nicht. Aber wir haben durch die Konzentration der Zuständigkeit der Ermittlungsrichter seit einigen Jahren eine Sensibilisierung und eine Qualitätssteigerung erreicht. Die Ermittlungsrichter in Deutschland kommen dem Ideal nahe, das in Frankreich für die gleiche Funktion den Begriff „Rechtsstaatsrichter“ vorsieht. Die heißen dort ausdrücklich so, und eine Prüfung durch den Ermittlungsrichter vermittelt ein hohes Maß an Qualität. Man muss allerdings sehen – Sie haben das selbst angesprochen, deshalb kann ich es aufgreifen –, dass die Belastung der Gerichte in diesem Bereich sehr hoch ist. Wir haben eine betriebswirtschaftliche Messung der Arbeit von Richtern. Die sieht in einer Gesamtkalkulation für die Tätigkeit des Ermittlungsrichters eine viel zu geringe Zeit für die Entscheidung des Einzelfalls vor. Aber die wenigen Anträge, die es gibt, werden sehr ausführlich, häufig nach Rückfragen geprüft, und in einer durchaus erheblichen Zahl abgelehnt. Eine letzte Bemerkung zu dieser Frage: Ich habe von der Schere in den Köpfen gesprochen. Die Schere in den Köpfen bedeutet, dass auf allen Stufen der Prüfung höchst sorgfältig gearbeitet wird, weil man weiß, wie kritisch das Instrument der Nutzung von Vorratsdaten gesehen wird.

Zum Vorschlag, das Gesetz mit einem zeitlichen Verfallsdatum zu versehen: Das wäre ein neuer Weg für Regelungen der StPO, von dem ich gar nichts halte. Wir brauchen gerade in diesem Bereich Rechtssicherheit. Wir brauchen für die Praxis das Vertrauen, dass sie mit diesen schwerwiegenden Eingriffen in die persönlichen Rechte weiterhin gut und verlässlich umgeht. Inwieweit eine Evaluierung Sinn machen würde, vermag ich nicht zu beurteilen. Ich sehe es aber kritisch, weil es nicht genug statistisches Material geben wird, das man im Sinne einer objektiven Auswertung bewerten könnte. Die Frage ist immer: Was wäre gewesen wenn? Und diese Frage stellt sich den Gerichten ex post. Da ist man ohnehin immer schlauer, so dass die eigentlich entscheidende Frage, was können wir erreichen, wenn wir Regelungen haben, nicht beantwortet werden kann.

Die **Vorsitzende**: Danke sehr. Der nächste ist Herr Franosch. Er hat Fragen von Herrn Sensburg, Herrn Hakverdi und Frau Winkelmeier-Becker.

SV **Rainer Franosch**: Vielen Dank. Zunächst zur Frage von Herrn Sensburg zur Entwicklung von Straftaten im Internet. Ich habe in meiner vorbereitenden Stellungnahme schon dargelegt, dass wir im Bereich der Internetkriminalität eine Steigerung haben, was die Menge und die Intensität angeht. Man muss unterscheiden zwischen internetabhängigen Straftaten, die des Internets bedürfen, wie Angriffe auf Netzstrukturen usw. Zum anderen ist das Internet ein Tatmittel. Insbesondere in Bezug auf letzteres muss man anerkennen, dass die Möglichkeit der Nutzung von Anonymisierungstechniken wie „Tor“ dazu geführt hat, dass wir im Dark-Net einen enormen Markt haben, über den Möglichkeiten bestehen, die es vor zehn Jahren noch nicht gegeben hat, sich virtuell zu Banden zusammenzufinden, Straftaten zu planen und Tatmittel sowie Tatpläne auszutauschen. In diesem Bereich sind wir auf IP-Adressen angewiesen. Wenn es uns in Ermittlungsverfahren gelingt, im Tor-Netzwerk die Anonymität zu brechen, was durch erheblichen technischen Aufwand hin und wieder gelingt, erlangen wir

lediglich IP-Adressen. Gelingt es uns nicht in einem allerersten Schritt, diese einem Anschlussinhaber zuzuordnen, sind die Ermittlungen am Ende. Bei jeder Straftat, die das Tatmittel Internet benutzt, ist es so, dass ich als Anknüpfungspunkt eine IP-Adresse habe. Kann ich diese schon nicht zuordnen, ist eine Ermittlung nicht möglich. Ich möchte auch das Wort von Herrn Frank von der Schere im Kopf aufgreifen. Ich habe dazu einen Beispielsfall in meiner einleitenden Stellungnahme aufgeführt, der deutlich macht, warum die Statistiken Schall und Rauch sind. Die Schere im Kopf bedeutet: Wenn ein Polizeibeamter im Rahmen eines Ermittlungsverfahrens 200 IP-Adressen hat, die aber schon zu alt sind, wird er keine 200 unbekannten Verfahren einleiten, weil das Arbeit für die Mülltonne ist. Das ist der Punkt, warum all diese Statistiken nichts taugen. Die leiten gar nicht erst ein. Es wird auch kein Verfahren eingeleitet gegen einen Kinderpornographen, der mit 500 Leuten kommuniziert hat, wenn diese 500 IP-Adressen sieben Monate und damit veraltet sind. Ich habe sie nicht in der Statistik. Diese ganzen Erhebungen und PKS taugen nichts. Das Einzige, was hilft, ist eine Sammlung von Rechtstatsachen, in dem man Fälle zusammenstellt. Herr Hakverdi, was die Befristung von Gesetzen angeht: In Hessen machen wir das. Wir haben zumindest befristete Rechtsverordnungen. Im Bereich der StPO wäre das in der Tat Neuland. Ob man das machen kann, weiß ich nicht, aber grundsätzlich sollte man zukünftige Entwicklungen berücksichtigen. Ich halte es für absolut notwendig, eine begleitende Evaluation dieser Neuregelung einzuführen. Ich habe meinen Standpunkt deutlich gemacht. Für den Bereich der Internetkriminalität greifen die Speicherfristen und der Straftatenkatalog zu kurz. Hier wird man bei der Begleitung feststellen können, dass es jedenfalls in diesem Bereich wenig bis nichts bringt. Insofern würde ich mir wünschen, dass man es evaluiert und noch einmal überdenkt, wie man es praxisgerechter ausgestaltet. Von daher wäre ich dieser Idee gegenüber durchaus aufgeschlossen. Zu Frau Winkelmeier-Becker und möglichen Fehlern: Als wir die Vorratsdatenspeicherung hatten, ist kein einziger Fall bekanntgeworden, in dem Datenbanken bei den Providern gehackt worden wären. Es ist auch kein Fall eines Datenlecks bekannt geworden. Wir müssen uns eines klar machen: Die Geheimdienste interessieren sich nicht für die Daten, die die Telekommunikationsprovider im Zuge der Vorratsdatenspeicherung speichern. Die Geheimdienste haben ganz andere Methoden. Die machen bei den Providern einen Abgriff der Inhaltsdaten. Darüber hinaus infizieren sie einzelne, als Zielpersonen ausgemachte Menschen mit trojanischen Pferden und Schadsoftware, so dass auch hier ganz andere Möglichkeiten bestehen. Die Datenbanken, die bei den Providern in Ausführung der Vorratsdatenspeicherung entstehen, sind für Geheimdienste komplett uninteressant. Insofern glaube ich, dass dieser Missbrauchsgesichtspunkt völlig überzogen dargestellt wird. Als wir die Vorratsdatenspeicherung hatten, gab es keine Fälle, und ich bezweifle auch, dass es sie geben wird. Wir müssen uns klar machen: Diese Daten, die da erhoben werden bzw. nicht gelöscht werden, dürfen von den Providern sowieso zu Abrechnungszwecken gespeichert werden. Was soll einem Geheimdienst eine Datenbank nutzen, die auflistet, wer welche IP-Adresse benutzt hat. Das ist nur relevant, wenn man bereits einzelne Vorgänge zuordnen kann. Das Missbrauchspotenzial ist aus meiner Sicht also überzogen.

Die **Vorsitzende**: Danke, Herr Franosch. Frau Dr. Sandkuhl hat eine Frage von Herrn Hakverdi.

SVe **Dr. Heide Sandkuhl:** Zum Thema Evaluierung will ich Folgendes sagen: Es ist das Mindeste, dass man – sollte ein solches Gesetz kommen – eine Evaluierung vorsieht. Gerade, wenn hier dargestellt wird, Statistiken seien nur Schall und Rauch, konkrete Zahlen gebe es nicht. Meine Damen und Herren, ich darf daran erinnern, was hier passiert. Hier werden Daten von Menschen gespeichert, die nicht den geringsten Anlass für eine Straftat oder Sonstiges gegeben haben. Das Ganze droht jetzt offenbar auf eine Prognoseentscheidung des Gesetzgebers hinauszulaufen. Es ist die vornehmlichste Pflicht, dass geprüft wird, ob dieser besonders schwere Eingriff, den wir in dieser Form noch nie hatten, auch erforderlich und notwendig war. Das ist das Mindeste. Und wenn Sie so wollen, von mir auch nur hilfsweise vorgetragen, weil ich das grundsätzlich für nicht regelungswürdig halte.

Ich darf außerdem daran erinnern, dass das Bundesamt für Justiz dem Max-Planck-Institut einen Auftrag gegeben hatte, zu prüfen, welche Lücken sich durch den Wegfall der Vorratsdatenspeicherung ergeben. Wer, wenn nicht das Max-Planck-Institut soll sich – was die Unabhängigkeit und Unbefangenheit angeht – mit diesen Fragen auseinandersetzen? Das Max-Planck-Institut hat festgestellt, dass bestimmte Daten nicht erfasst worden sind, dass es offenbar als zu kostenträchtig angesehen worden ist, statistische Erhebungen einzuholen. Dann frage ich mich, warum eigentlich? Das kann man doch machen. Das gibt es doch in vielen anderen Verfahren auch, dass man prüfen kann, wie oft und zu welchem Zweck diese Maßnahme angeordnet worden ist. Das finde ich überhaupt nicht kompliziert. Mich wundert, dass so darüber hinweg gegangen wird. Vielleicht mag das nicht gerne gesehen werden, dass nach Wegfall der Vorratsdatenspeicherung durch die Entscheidung des BVerfG vielleicht gar keine Lücken entstanden sind? Eines noch zum Schluss: Wenn Sie von einer Tätervernunft ausgehen und ein Täter weiß, dieses Gesetz gibt es jetzt. Meinen Sie nicht, dass er Möglichkeiten findet, das zu umgehen? Meinen Sie nicht, dass er Internetcafés, Hotels, sonstige WLAN-Anschlüsse nutzen kann, um Botschaften zu übermitteln? Es wird als das heilige Mittel dargestellt; es ist aber ganz leicht auszuhebeln. Von daher kann ich immer noch oder weiterhin nur die Erforderlichkeit anzweifeln. Vielen Dank.

Die **Vorsitzende**: Danke. Jetzt ist Herr Starostik an der Reihe mit einer Frage von Herrn Hakverdi, bei dem mir auf den Zettel schauend aufgefallen ist, wie virtuos er vier Fragen gestellt hat. Herr Starostik und dann Herr Thiede.

SV **Meinhard Starostik**: Ich kann mich im Wesentlichen anschließen. Ich muss sagen: Ich habe mich sehr gewundert. Ständige Rechtsprechung des BVerfG ist, dass der Gesetzgeber bei neueren technischen Entwicklungen eine Beobachtungspflicht hat und die Möglichkeiten schaffen muss, ggf. nachzubessern, indem er nach einem gewissen Zeitraum die Gesetze überwacht. Dazu kann man das von Anfang an wissenschaftlich begleiten. Das sei nur hilfsweise gesagt und ist nicht ganz der Schwerpunkt meiner Bedenken, weil ich mit meinen Bedenken viel früher ansetze.

Die **Vorsitzende**: Danke. Herr Thiede mit Fragen von Herrn Sensburg und Frau Winkelmeier-Becker.

SV **Frank Thiede**: Herr Dr. Sensburg, die Frage des „Quick Freeze“ ist nicht erstmalig gestellt worden, sondern in der letzten Legislaturperiode mehrfach an uns herangetragen worden: Ist das nicht eine mildere Maßnahme, die man als Alternative zur Vorratsdatenspeicherung nutzen könnte? Die Antwort hat das BVerfG eigentlich schon gegeben. Es hat nämlich in einer Randziffer gesagt, dass es eine mildere Maßnahme ist, aber nicht gleichermaßen geeignet ist. Damit war für uns die Sache relativ klar. Wenn Daten im Rahmen einer retrograden strafverfolgerischen Ermittlung erhoben werden müssen, können sie schlecht schon vorher eingefroren werden. Das ist physikalisch und logisch nicht denkbar. Es gibt Fälle, in denen ab dem Zeitpunkt der Kenntniserlangung – das Verfahren läuft schon – anlassbezogen Daten gespeichert werden. Das haben wir jetzt schon mit der geltenden Rechtsgrundlage § 100g StPO. Die zweite Frage, Frau Winkelmeier-Becker, da schließe ich mich dem an, was Herr Franosch schon sagte. In den rund zwei Jahren, als die Vorratsdatenspeicherung galt, ist uns kein Fall bekannt, in dem Missbrauch getrieben wurde. Es ist allerdings in der mündlichen Verhandlung und der Urteilsverkündung beim BVerfG deutlich geworden, dass auf Seiten der Betreiber im Hinblick auf die Datensicherheit gesetzliche und organisatorische Vorkehrungen getroffen werden müssen, damit diese Vorratsdaten noch sicherer gespeichert werden als die Abrechnungsdaten. Ich bin kein Fachmann für die technischen Anforderungen an Datensicherheit bei der Speicherung bei Betreibern, gehe aber davon aus, dass diese Voraussetzungen von diesen gesetzlichen Vorgaben erfüllt werden.

Abg. **Elisabeth Winkelmeier-Becker** (CDU/CSU): Meine Frage war noch: Was kann jemandem passieren, der in Ermittlungsmaßnahmen gerät, weil er auf der Telefonliste eines möglichen Täters gestanden hat?

SV **Frank Thiede**: Nur zum Verständnis: Es geht darum, dass ich gegen Beschuldigte ermittle,

Daten erhebe nach § 100g StPO und einen anderen Betroffenen habe?

Abg. **Elisabeth Winkelmeier-Becker** (CDU/CSU): Ja, oder man macht eine Funkzellenabfrage und da ist jemand drin, der mit keinem Delikt etwas zu tun hat. Der nur zur selben Zeit am selben Ort war.

SV **Frank Thiede**: Das bezieht sich auf die Frage der Funkzellendatenabfrage. Das Gesetz sieht eine Funkzellendatenabfrage vor. Wenn es Abrechnungsdaten sind, dann geht es nach dem § 100g Abs. 1 StPO. Wenn es Vorratsdaten sind, dann müssen die Katalogtaten vorliegen. Bei der Funkzellendatenabfrage können auch unbeteiligte Dritte betroffen sein. Allerdings ist es ein relativ kurzes Zeitfenster, in dem die Daten erhoben werden, und zwar lokalisiert auf einen bestimmten Bereich. Diese Daten werden gelöscht, wenn sie nicht mehr erforderlich sind.

Die **Vorsitzende**: Der letzte in der Reihe ist Herr Professor Wollenschläger mit Fragen von Herrn Fechner und mir.

SV **Prof. Dr. Ferdinand Wollenschläger**: Zunächst zu Ihren beiden Fragen nach dem Überwachungsplus und der NSA. Das Überwachungsplus hat Herr Starostik mit der Figur des additiven Grundrechtseingriffs angesprochen. Das kann und muss man bei einer Gesamtabwägung berücksichtigen. Wenn wir mit Blick auf die Gesetzentwürfe von einem Überwachungsplus sprechen und addieren, dann müssen Sie natürlich auch subtrahieren, was diese Gesetzentwürfe hinter den früheren Regelungen hinsichtlich der Speicherdauer, dem eingeschränkten Straftatenkatalog, den vorgesehenen Ausnahmen zurückbleiben. Da gibt es durchaus auch ein Überwachungsminus. Den zweiten Punkt: NSA, hat Herr Franosch mit viel mehr Ermittlungs- und Facherfahrung beantwortet, als ich das könnte. Mir selbst sind Ermittlungsmöglichkeiten …

Die **Vorsitzende**: Ich wollte aber Ihre rechtliche Antwort. Er sieht die NSA ja auch nicht.

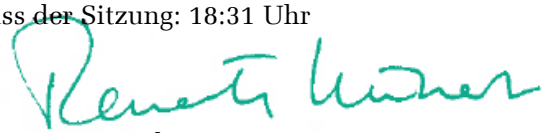
SV **Prof. Dr. Ferdinand Wollenschläger**: … Ermittlungsmöglichkeiten der NSA unbekannt. Wobei ich mir nicht vorstellen kann, dass die Verkehrsdatenspeicherung zu einem Plus führt, so dass es in rechtlichen Bewertungen nichts durchschlagend ändern würde. Letzter Punkt. Herr Fechner, es war gut, dass Sie die Inlandsspeicherung noch einmal angesprochen haben, weil mir bei Ihrer Frage aufgefallen ist, dass ich Herrn Ullrichs Frage insofern nicht beantwortet habe. Ich hatte aber ja eingangs schon gesagt: Die Pflicht zur Inlandsspeicherung ist eine Beschränkung der Dienstleistungsfreiheit. Beschränkung der Dienstleistungsfreiheit heißt nicht, dass sie per se europarechtswidrig ist, sondern sie kann gerechtfertigt werden. Sie kann gerechtfertigt werden aus Gründen des Datenschutzes. Die Mitteilung der Kommission hat eine leicht überschießende Tendenz, weil suggeriert wird, dass das europarechtlich abschließend harmonisiert sei. Wenn man jetzt allerdings in die Randnummern 66 und 67 des Urteils des EuGH schaut, hält der EuGH klar fest, dass der bestehende sekundärrechtliche Rahmen, insbesondere die E-Privacy und die Datenschutzrichtlinie, gerade nicht zum adäquaten Datenschutz ausreicht, weshalb der EuGH auch gefordert hat, es müsse sekundärrechtlich, also europarechtlich, mehr Datensicherheit sichergestellt werden. Aufgabe des Gesetzgebers ist, für eine entsprechende Datensicherheit zu sorgen. Das kann man dadurch tun, dass man das auf die Speicherpflicht im Inland beschränkt. Man muss sich europarechtlich fragen lassen, ob aus Gründen des freien Dienstleistungsverkehrs eine Speicherung im Ausland zuzulassen ist, aber nur, wenn ein adäquater Datensicherheitsstandard sichergestellt ist. Das werden Sie jetzt – das Bundesjustizministerium ist vermutlich im Austausch – mit der Europäischen Kommission klären müssen. Meine Zweifel: Wenn Sie ausländische Anbieter haben, können Sie die Datensicherheit nur durch privatrechtliche Verträge sicherstellen, weil Sie als deutsche Überwachungsbehörden auf Sanktionierungen im Wege von Ordnungswidrigkeiten nicht im Ausland zugreifen können. So könnte man diese Rechtfertigungsmöglichkeit durchaus für gegeben erachten. Das hängt von den Detailausgestaltungen ab. Es bestehen zwei Möglichkeiten: Entweder kommt man jetzt zu einer Einigung im Austausch mit der Europäischen Kommission. Wenn nicht, wird mit Blick auf mögliche Vertragsverletzungsverfahren zu überlegen sein, ob man sich auf den Standpunkt stellt,

Anforderungen der Datensicherheit können, weil der Schutz im Ausland nicht effektiv sichergestellt werden kann, nicht gewahrt werden. Es ist deshalb beschränkt auf die Inlandsspeicherung, und dies ist gerechtfertigt. Da gilt das Gleiche wie für das Urteil des EuGH zur Vorratsdatenspeicherung. Wie ein erneutes Urteil aussehen wird, ist im Bereich des Spekulativen, wobei Sie sich auf gute Rechtfertigungsgründe berufen können.

Die **Vorsitzende**: Danke. Das war die letzte Antwort an der Stelle. Vielleicht sind noch nicht alle Fragen beantwortet. Bei mir zumindest nicht.

Ich glaube, dass Verkehrsdaten unterschätzte Daten bei der Frage sind, welche Profile man damit erstellen kann, sonst wären auch nicht alle so scharf darauf. Die sind mindestens so spannend wie inhaltliche Daten. Es bleibt die Frage, was technisch neuester Stand und technisch machbar ist. Das heißt also: Mindestens die Fragen und noch ein paar andere haben wir auf alle Fälle in der nächsten Lesung und Auswertung dieser Anhörung im Ausschuss. Ich danke den Damen und Herren Sachverständigen und schließe die Sitzung.

Schluss der Sitzung: 18:31 Uhr



Renate Künast, MdB
Vorsitzende

Anlagen: Stellungnahmen der Sachverständigen

Stellungnahme

zum Regierungsentwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten*

Ermittlungstaktische und beweisrechtliche Bedeutung von Verkehrsdaten

– ein Einblick in die Ermittlungs- und Verfahrenspraxis der Strafverfolgungsbehörden und Gerichte

Verfasser: *Richter am Bundesgerichtshof Dr. Nikolaus Berger, Leipzig/Hamburg* **

Während sich die Diskussion über eine erneute Einführung von Höchstspeicherfristen für Verkehrsdaten zunächst darauf konzentriert hatte, ob vor dem Hintergrund der Rechtsprechung des Bundesverfassungsgerichts und des Europäischen Gerichtshofs überhaupt rechtliche Realisierungsmöglichkeiten für dieses Ermittlungsinstrument bestehen und solche durch die Bundesregierung im Regierungsentwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 15. Juni 2015 (BT-Drs. 18/5171) – mit guten Gründen – anerkannt worden sind, scheint sich der Schwerpunkt der öffentlich geführten Kontroverse zu verlagern:

Nunmehr drängt die Frage in den Vordergrund, ob die Möglichkeit eines anlassbezogenen Zugriffs der Strafjustiz auf die bei den (privaten) Telekommunikationsprovidern anfallenden und von ihnen anlasslos zu speichernden Verkehrsdaten überhaupt einen hinreichenden Nutzen hat, der einen mit einer solchen Datenspeicherung auf Vorrat verbundenen Eingriff in grundrechtlich geschützte Rechtsgüter – auch nicht Tatverdächtiger – und ihren Aufwand rechtfertigen kann. Angesprochen ist damit die Frage der Verhältnismäßigkeit, die der Regierungsentwurf u.a. dadurch gewährleisten will, dass Vorratsdaten von den Strafverfolgungsorganen nur zur Aufklärung „besonders schwerer Straftaten“, die auch im Einzelfall besonders schwer wiegen, und auch nur erhoben werden dürfen, „soweit die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert

* Anhörung des Ausschusses für Recht und Verbraucherschutz am 21. September 2015

** Der *Verf.* ist Mitglied des 5. (Leipziger) Strafsenats des BGH; bis Juni 2013 war er Mitglied des 2. Strafsenats des BGH und über vier Jahre Ermittlungsrichter beim BGH.

oder aussichtslos wäre“ (§ 100g Abs. 2 Satz 1, Abs. 3 StPO RegE). Immer wieder ist zu lesen und zu hören, dass retrograd zu erhebende Verkehrsdaten, die vor Beginn eines Ermittlungsverfahrens in zeitlicher Nähe zu einer Straftat angefallen sind, in der Praxis der Strafverfolgungsorgane keine oder allenfalls eine untergeordnete Bedeutung zukomme, sodass selbst eine zeitlich eng begrenzte Vorratsdatenspeicherung gegen das verfassungsrechtliche Übermaßverbot verstoße. Hierzu wird als Referenz regelmäßig auch ein Gutachten der kriminologischen Abteilung des Freiburger Max-Planck-Instituts für ausländisches und internationales Strafrecht aus dem Jahr 2011 zu möglichen Schutzlücken durch den Wegfall der Vorratsdatenspeicherung herangezogen.[1]

Deshalb soll hier anhand von Beispielsfällen aus jüngerer Zeit, wie sie im Alltag richterlicher Berufspraxis[2] vorkommen, die ermittlungstaktische Bedeutung der Verkehrsdaten für die Tataufklärung durch die Strafverfolgungsbehörden und für die Beweisführung der Strafgerichte dargestellt werden (**I.**). Dazu sollen die in den Strafverfahren abgeurteilten Taten bzw. (soweit ein rechtskräftiges Verfahrensergebnis noch nicht vorlag) die den Ermittlungsverfahren zugrundeliegenden Tatvorwürfe mit groben Strichen skizziert und der Einsatz der Verkehrsdaten und seine Folgen für den Verfahrensausgang dargelegt werden. Die Darstellung erhebt nicht den Anspruch einer empirischen Untersuchung. Vielmehr soll anhand von konkreten Fällen veranschaulicht werden, wie die Erhebung von Verkehrsdaten einerseits zu Beginn eines Ermittlungsverfahrens als ebenso sicherer wie effizienter Ermittlungsansatz und andererseits im Hauptverfahren vor Gericht als beweiskräftiges Indiz für einen Tatnachweis oder auch zu einer Verdachtsentkräftung zugunsten eines Beschuldigten bei der Aufklärung schwerster Straftaten beitragen kann.

[1] „Schutzlücken durch Wegfall der Vorratsdatenspeicherung? – Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten“, Max-Planck-Institut für ausländisches und internationales Strafrecht, Freiburg, 2. erweiterte Fassung, 2011.

[2] Zusätzlich zu Fällen, die Gegenstand von Revisionsverfahren beim BGH waren und auch mit dem StR-Aktenzeichen des betreffenden Verfahrens gekennzeichnet sind, haben maßgeblich zu der Sammlung exemplarischer Fälle mit weiteren Verfahren aus dem Bezirk des Hanseatischen Oberlandesgerichts Hamburg Staatsanwalt Dr. Gerwin Moldenhauer und Richter am Oberlandesgericht Marc Wenske beigetragen; ihnen danke ich für ihre Unterstützung.

Weiter wird zu den – empirisch nicht belastbaren – Erkenntnissen des Max-Planck-Instituts Stellung genommen und kurz beleuchtet, welchen Schwierigkeiten eine begrüßenswerte Evaluation einer Wirksamkeit der Neuregelung der Verkehrsdatenspeicherung ausgesetzt sein dürfte (**II.**). Eine überwiegend zustimmende Stellungnahme wird der Verfasser im Rahmen seines Fazits (**III.**) geben.

I. Einblick in die Ermittlungspraxis deutscher Strafverfolgungsbehörden

1. Verfahrensbeispiele

Nachstehend werden aus verschiedenen Deliktsbereichen der Schwerkriminalität Beispielsfälle knapp mit Verfahrensgegenstand und Bedeutung der Verkehrsdaten als Ermittlungsansatz und/oder Beweistatsache für die Beweiswürdigung dargestellt. Es handelt sich – wie nochmals zu unterstreichen ist – nicht um systematisch erhobene oder ganz außergewöhnliche Fälle, sondern um alltägliche Strafverfahren im Bereich der Schwerkriminalität, mit denen die Staatsanwaltschaften der Länder und die Landgerichte regelmäßig befasst sind. Verfahren aus der Senatstätigkeit des *Verf*., die im laufenden Kalenderjahr abgeschlossen wurden, sind den Deliktsgruppen jeweils vorangestellt worden, um nicht zuletzt schon durch deren bloße Anzahl die Relevanz eines Zugriffs auf retrograd zu erhebende Verkehrsdaten für die Verbrechensaufklärung zu illustrieren.

a) Raubdelikte

(1) Verfahrensgegenstand: Das Landgericht Hamburg verurteilte die Angeklagten rechtskräftig wegen Raubes (§ 249 StGB) in Tateinheit mit gefährlicher Körperverletzung (§ 224 Abs. 1 Nr. 4 StGB) zu Freiheitsstrafen von fünf Jahren und von drei Jahren sechs Monaten.[3] Die beiden aus Rumänien stammenden, sich illegal an verschiedenen Wohnorten in Deutschland aufhaltenden Täter hatten in Hamburg einen 78-jährigen Rentner aus einem Bus bis in den

[3] LG Hamburg, Urteil vom 17.3.2015, Az. 611 KLs 18 - 14-3100 Js 341/14; BGH, Beschluss vom 1.9.2015 – 5 StR 349/15.

Hausflur seines Wohnhauses verfolgt, um ihm seinen Goldschmuck zu rauben. Einer der Täter versetzte dem Geschädigten überraschend von hinten einen Faustschlag ins Gesicht und beide traten sodann auf das bewusstlos zu Boden gegangene Opfer ein, das u.a. eine Kieferfraktur und ein Schädel-Hirn-Trauma erlitt. Mit einer Beute von rd. 1.300 Euro flohen sie anschließend in unterschiedliche Richtungen vom Tatort, wobei einer der Täter die U-Bahn benutzte und sich auf seiner Flucht telefonisch mit dem Komplizen zu einer Beuteteilung am Hauptbahnhof verabredete.

Ermittlungstaktische Bedeutung von Verbindungsdaten: Beide Täter waren zunächst bei der Beobachtung des späteren Opfers im Bus von der dortigen Videokamera abgebildet worden. Einer der Täter wurde auf seinem Fluchtweg auch von den Überwachungskameras an der dem Tatort nahegelegenen U-Bahn-Haltestelle sowie der U-Bahn aufgenommen. Dem Videofilm war zu entnehmen, dass er dabei mehrfach telefonierte. Nach Ausmessung von drei für den Tatort und den Fluchtweg relevanten Funkzellen wurde vom Ermittlungsrichter die Herausgabe der dort in dem Tat- und Fluchtzeitfenster von 30 Minuten angefallenen und auf der Grundlage des § 96 Abs. 1 TKG gespeicherten Verkehrsdaten angeordnet. Zur Verhältnismäßigkeit führte der Ermittlungsrichter in seinem Beschluss gemäß § 100g Abs. 1 Nr. 1, Abs. 2 i.V.m. § 100b Abs. 1 Satz 1, Abs. 2 StPO aus, dass es mittels einer Auswertung der Funkzellendaten auf Überschneidungen möglich sei, den Täteranschluss festzustellen; Rechte Dritter seien nicht erheblich betroffen, da die erlangten Daten nur bei einer Übereinstimmung aufgeschlüsselt würden. Anhand der von Providern mitgeteilten Verkehrsdaten konnte festgestellt werden, dass insgesamt 13 Mobiltelefonnummern in zwei der drei untersuchten Funkzellen Verbindungen im Abfragezeitraum hatten. Bei einem weiteren gezielten Abgleich mit den Daten aus den Videoaufzeichnungen der Hochbahn blieb nur eine Mobilnummer übrig, die dem mit der U-Bahn Flüchtenden zugeordnet werden konnte. Über den von diesem Anschluss während der U-Bahnfahrt viermal angerufenen Mobilanschluss ließ sich die Mobilfunknummer des Mittäters ermitteln. Allein dessen Anschluss war auch in der Folgezeit noch aktiv.

Insbesondere durch eine ermittlungsrichterlich angeordnete Überwachung der unter dieser Mobilnummer geführten Telekommunikation nach § 100a Abs. 1, Abs. 2 Nr. 1k StPO ergaben sich Hinweise auf die Identität des diesen Anschluss nutzenden (zweiten) Täters, der nach seiner Identifizierung rd. zehn Wochen nach der Tat festgenommen werden konnte. Er gestand bereits in seiner ersten polizeilichen Vernehmung die Tat und benannte später auch seinen Mittäter.

Andere von den Ermittlungsbehörden hier zusätzlich gewählte Maßnahmen zur Täteridentifizierung (u.a. eine Öffentlichkeitsfahndung und ein Abgleich der sichergestellten DNA-Spuren mit der DNA-Analyse-Datei) waren leergelaufen. Ohne den kurzfristigen Rückgriff auf die bei Netzbetreibern noch vorhandenen Verkehrsdaten nach § 96 TKG hätte das Verbrechen nicht aufgeklärt werden können. Beweisrechtlich, also zum späteren Tatnachweis in der Hauptverhandlung vor dem Landgericht, spielten die zu Identifizierungszwecken erhobenen Verkehrsdaten keine nennenswerte Rolle mehr.

Im Hinblick auf die im Regierungsentwurf (RegE) vorgesehene Wiedereinführung einer Pflicht zur Speicherung von Mobilfunk-Verkehrsdaten in § 113b TKG (RegE) und zur Möglichkeit ihrer Erhebung in § 100g Abs. 2 StPO (RegE) ist anzumerken: Hätte sich im Laufe der Ermittlungen noch innerhalb der Vierwochenfrist des § 113b Abs. 1 Nr. 2 TKG (RegE) der Verdacht einer Tatserie mit gleichartig brutal ausgeführten, aber noch keinen Qualifikationstatbestand erfüllenden Verbrechen des Raubes ergeben, hätten die Ermittlungsbehörden selbst bei noch vorhandenen Vorrats-Standortdaten etwa für die betreffenden weiteren Tatorte darauf keinen Zugriff erhalten können, weil eine Funkzellenabfrage nach § 100g Abs. 3 Satz 2 StPO (RegE) nur zur Aufklärung der im Straftatenkatalog in § 110g Abs. 2 Satz 2 Nr. 1g StPO (RegE) enthaltenen qualifizierten Raubdelikte ermittlungsrichterlich hätte angeordnet werden können.

(2) Verfahrensgegenstand: Den Angeklagten lag in einem Verfahren der Staatsanwaltschaft Hamburg ein besonders schwerer Raub zur Last (§ 250 Abs. 2 Nr. 1 StGB).[4] Nach dem Anklagevorwurf forderten sie den Geschädigten auf, sein Mobiltelefon herauszugeben, und schlugen ihm – als er sich weigerte – mit einer Flasche derart auf den Kopf, dass er bewusstlos zu Boden stürzte. Anschließend entwendeten die Angeklagten dem Opfer das Mobiltelefon und veräußerten es noch am selben Tage.

Beweisrechtliche Bedeutung von Verbindungsdaten**:** Die Angeklagten schwiegen im Ermittlungsverfahren. Der hinreichende Tatverdacht wurde in der Anklageschrift gestützt auf die Aussage einer Zeugin, die das Mobiltelefon wenige Stunden nach der Tat von den Angeklagten gekauft und noch in folgenden Nacht verschenkt haben sollte. Bei dem Beschenkten konnte die Tatbeute schließlich im Rahmen einer Durchsuchung aufgefunden werden. Die Aussage der Zeugin wurde bestätigt durch Verkehrsdaten: Mit Hilfe der Gerätenummer (IMEI-Nummer) des gestohlenen Mobiltelefons konnte ermittelt werden, dass die beschenkte Person das dem Geschädigten entwendete Mobiltelefon mit seiner eigenen SIM-Karte betrieben hatte.

(3) Verfahrensgegenstand**:** Die Staatsanwaltschaft Hamburg legte den Angeklagten einen schweren Raub zur Last (§ 250 Abs. 1 Nr. 1b StGB).[5] Nach dem Anklagevorwurf klingelten sie an der Tür einer bettlägerigen älteren Dame. Nach Öffnen der Tür durch die Angestellte eines Pflegedienstes drückte einer der Täter ihr eine Hand auf den Mund, um sie am Schreien zu hindern. Sodann drängte er sie in das Innere der Wohnung und befragte sie nach Bargeld. Anschließend wurde die Angestellte gefesselt und geknebelt und die Täter flüchteten mit Bargeld.

Ermittlungstaktische und beweisrechtliche Bedeutung von Verbindungsdaten: Die schweigenden Angeklagten – die persönliche Kontakte zum Pflegedienst unterhielten – wurden erheblich belastet durch die Ergebnisse der Ver-

[4] Az. 3411 Js 497/14; nachfolgend: Urteil des LG Hamburg vom 3.6.2015, Az. 628 KLs 3/15.
[5] Az. 4290 Js 52/11; nachfolgend: Urteil des LG Hamburg vom 8.7.2014, Az. 617 Ns 15/13.

kehrsdatenauswertung ihrer Mobiltelefone. Danach wurden zwischen ihnen insbesondere zur Tatzeit und unmittelbar danach mehrere Telefonate geführt; die Geovisualisierung der Verbindungsdaten – eine graphische Aufbereitung der verschiedenen Standorte von Funkzellen, in denen die Mobilfunkanschlüsse eingeloggt waren – zeigte, dass sich ein Angeklagter zur Tatzeit in unmittelbarer Nähe des Tatorts aufgehalten hatte.

(4) Verfahrensgegenstand: Das Landgericht Hamburg hat den Angeklagten rechtskräftig vom Vorwurf des besonders schweren Raubes (§ 250 Abs. 2 StGB) freigesprochen.[6] Die Staatsanwaltschaft hatte mit ihrer Anklage dem Angeklagten vorgeworfen, gemeinsam mit zwei Mittätern einen Pizza-Boten nachts in einen Hinterhalt gelockt, dort überfallen und ihm mit Gewalt und unter Vorhalt von Waffen Bargeld, Papiere und Mobiltelefone geraubt zu haben. Als Nutzer der Mobilfunknummer, die zur vorgeblichen Essensbestellung beim Pizza-Service verwendet wurde, war der Angeklagte ermittelt worden.

Beweisrechtliche Bedeutung von Verbindungsdaten: Der Angeklagte hatte im Ermittlungsverfahren und in der Hauptverhandlung vor der Strafkammer geschwiegen. Besondere Bedeutung kam in diesem „Indizienprozess“ namentlich den erhobenen Verkehrsdaten betreffend den Mobilanschluss zu, von dem aus eine Pizzabestellung aufgegeben worden war. Die verwendete Telefonnummer war mit einer 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 oder 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 allerdings nur dann tragfähig sein, wenn mit Gewissheit auszuschließen war, dass eine andere Person Zugriff auf den Anschluss hatte.

[6] LG Hamburg, Urteil vom 13. Dezember 2013, Az: 624 KLs 11/12 – 4181 Js 1/12

Bis zum letzten Hauptverhandlungstag am 13. Dezember 2013 schien die Beweisaufnahme die Schlussfolgerung von den Verkehrsdaten auf die Täterschaft des Angeklagten nahezulegen. Einem im Rahmen des Schlussvortrags des Verteidigers gestellten Beweisantrag betreffend den Standort des Tathandys drei Tage vor der am 28. Dezember 2011 begangenen 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. Zusammen mit dem Umstand, dass der Mobiltelefonanschluss am Abend unmittelbar vor der Tat am Wohnort der Freundin eines weiteren Tatverdächtigen eingeloggt war, der engen Kontakt zur Familie des Angeklagten hatte, schwächte dies „das Beweiszeichen in ganz empfindlicher Weise“. Denn es konnte, wie die Strafkammer in den Urteilsgründen ausgeführt hat, „nunmehr nicht sicher ausgeschlossen werden, dass ein Dritter möglicherweise auch am Tatabend Zugang zu dem Mobilfunkanschluss hatte“.

b) Erpressungsdelikte

(1) Verfahrensgegenstand: Der Angeklagte ist vom Landgericht Hamburg rechtskräftig u.a. wegen versuchter räuberischer Erpressung in zwei Fällen (§§ 253, 255, 249 Abs. 1, 22, 23 StGB) zu einer Gesamtfreiheitsstrafe von drei Jahren verurteilt worden.[7] Der Verurteilung zugrunde lagen u.a. Todesdrohungen, die der Angeklagte im Rahmen von Streitigkeiten über gegen ihn erhobene Forderungen aus seiner Tätigkeit als Box-Promoter u.a. per SMS an zwei seiner Gläubiger zur Abwendung von Zwangsvollstreckungsmaßnahmen übermittelte. Die geschädigten Gläubiger gingen auf die Drohungen nicht ein, wobei einer von ihnen bereits am Tag nach der Tat Strafanzeige erstattete. Daher konnten die gemäß § 96 TKG gespeicherten Verkehrsdaten u.a. des zur Übermitt-

[7] LG Hamburg, Urteil vom 1.9.2014, Az. 603 KLs – 6500 Js 21/13; BGH, Beschluss vom 19.5.2015 – 5 StR 154/15.

lung der Drohungen genutzten Mobilfunkanschlusses nach § 100g Abs. 1 StPO noch erhoben werden.

Beweisrechtliche Bedeutung von Verbindungsdaten: Der Angeklagte hatte zunächst geschwiegen und sich später dahin eingelassen, dass jemand anderes die betreffenden Nachrichten versandt haben müsse. Die Strafkammer hat den Angeklagten auf Grund folgender, maßgeblich auf die Verkehrsdaten gestützter beweiswürdigender Erwägungen als überführt angesehen:

> *„(...) Der Angeklagte wird insbesondere belastet durch die ... Verbindungsdaten zu der Rufnummer 49176XXX. 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 ... bei der Durchsuchung des Wohnhauses des Angeklagten ... 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 49176XXX 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 ... des Providers O. ... Diese Funkzelle deckt nach der Funkzellenausmessung des Landeskriminalamtes ... auch den Bereich H.-Straße in G., der Wohnanschrift des Angeklagten, ab.*
>
> *Zur Tatzeit am 6. Januar 2013 waren nach der 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 ..., einem Funkturm in T., 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 T. eingeloggt, teils in die Funkzelle des Providers V. mit der Zellkennung LAC/Zell-ID 409/15001, einem Funkmast in W. mit den Koordinaten ..., 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 W."

(2) Verfahrensgegenstand: Die Staatsanwaltschaft Hamburg legt dem Angeklagten eine besonders schwere räuberische Erpressung zur Last (§§ 253, 255, 250 Abs. 2 Nr. 1 StGB).[8] Nach dem Anklagevorwurf stellte er ein Scheinangebot über den Verkauf eines Kraftfahrzeugs auf der Internetplattform „mobile.de" zum Preis von 40.000 Euro ein. Er einigte sich telefonisch mit einem Interessenten über den Verkauf und verabredete sich mit ihm und dessen Lebensgefährtin. An dem abgelegenen Treffpunkt hielt der Angeklagte dem Kaufinteressenten einen Revolver an den Kopf, verlangte Bargeld und drohte für den Fall einer Weigerung, den Geschädigten und dessen Lebensgefährtin zu erschießen. Der Geschädigte händigte ihm das Geld aus.

Beweisrechtliche Bedeutung von Verbindungsdaten: Noch am Tatabend eingeleitete Fahndungsmaßnahmen blieben erfolglos. Eine Identifizierung des Angeklagten 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 zuvor erhobenen Verkehrsdaten bestätigt. Denn anhand der Verkehrsdaten zu der vom Täter gegenüber dem Geschädigten verwendeten Rufnummer konnte ermittelt werden,

[8] StA Hamburg, Az. 3400 Js 39/15

wo sich der Nutzer des Anschlusses vor der Tat aufgehalten hatte. Dies war überwiegend ein Bereich Hamburgs in der Nähe zur Wohnanschrift des Angeklagten, auf den die Zeugenhinweise abzielten.

c) Mord- und Totschlagsdelikte

(1) Verfahrensgegenstand: Die Angeklagte ist vom Landgericht Saarbrücken wegen Anstiftung zum Mord sowie wegen versuchter Anstiftung zum Mord (§§ 211, 26 StGB) rechtskräftig zu lebenslanger Freiheitsstrafe als Gesamtstrafe verurteilt worden.[9] Der abgeurteilten Anstiftung zum Mord lag zugrunde, dass die Angeklagte den von ihr als Täter rekrutierten F. gegen Geldzahlung dafür gewann, den ursprünglich mit ihr befreundeten Geschäftspartner P. zu töten. Sie wollte sich hierdurch von erheblichen Schulden bei P. befreien und zugleich Zugriff auf eine im Todesfall an einen ihrer Familienangehörigen auszuzahlende Lebensversicherungssumme erhalten. Zur Vorbereitung der Tat verabredete die Angeklagte ein Treffen zwischen dem mit der Tötung beauftragten F. und dem späteren Tatopfer P., dem die Angeklagte als Legende vortäuschte, bei dem Termin ihre Schulden durch eine Zahlung von F. an P. begleichen zu wollen. Die Angeklagte stimmte mit beiden Männern durch diverse Telefonate und Kurznachrichten ab, dass die vorgebliche Geldübergabe am Abend des 23. Mai 2013 auf einem leerstehenden, dem F. zugänglichen Anwesen stattfinden sollte. Dort tötete F. den P. Zu der umfänglichen (im Ergebnis aber erfolglosen) Tatspurenbeseitigung des F. gehörte, dass er das Handy des Tatopfer P. in einem Fluss beseitigte und die Angeklagte aufforderte, ihre Handydaten zu löschen; auch führte er an seinem eigenen Handy einen „Datenreset“ durch. Die von F. mit dem Fahrzeug des Opfers an einen abgelegenen Ort transportierte Leiche des P. wurde zwei Wochen nach der Tat entdeckt und führte zur Bildung einer Mordkommission „P.“, der es gelang, die nach § 96 TKG gespeicherten Verkehrsdaten der bei Tatbegehung und der Nachtat-Kommunikation verwandten Mobilfunkgeräte sowie der tatrelevanten Funkzellen noch zu erheben.

[9] LG Saarbrücken, Urteil vom 4.2.2015, Az. 2 Ks 1/14 – 7 Js 901/13; BGH, Beschluss vom 18.8.2015 - 5 StR 249/15.

Beweisrechtliche Bedeutung von Verbindungsdaten: Die Angeklagte bestritt in der Hauptverhandlung vor der Strafkammer ihre Tatbeteiligung. Seine Überzeugung davon, dass die Angeklagte den Mordauftrag erteilt hatte, bildete sich das Landgericht im Wesentlichen aufgrund der geständigen Aussage des bereits rechtskräftig für den Mord an P. verurteilten und nunmehr als Zeuge vernommenen F. Angesichts der hier gegebenen besonderen Aussagekonstellation[10] hielt es das Landgericht – zu Recht – für bedeutsam, dass die Angaben des Belastungszeugen F. durch die Auswertung der Telekommunikationsverbindungsdaten bestätigt wurden. Hierzu führte das Landgericht in seiner Beweiswürdigung u.a. aus:

> *„Die verlesenen Daten belegen allein für den Tattag, dass zwischen der Angeklagten und dem Opfer 18 Telekommunikationsverbindungen wechselseitigen Ursprungs zu verzeichnen waren und zwischen der Angeklagten und dem Zeugen F. 13 derartige Verbindungen. … Hingegen gibt es keine unmittelbaren Verbindungen zwischen dem Zeugen F und dem P. Insbesondere um den Zeitpunkt der Tötung herum ist feststellbar, dass die Angeklagte wechselseitig und jeweils in unmittelbarem Zusammenhang den P. und den F. mit SMS-Nachrichten kontaktierte und auf diese Weise beide zum Tatort hin „fernsteuerte“ sowie beide über deren jeweiligen Aufenthaltsort bzw. Eintreffzeitpunkt informierte. … Insofern sind sämtliche, objektiv festgestellten Telekommunikationsverbindungen zwischen dem F. und der Angeklagten am Tatabend vollständig in Einklang zu bringen mit dem von dem Zeugen F. geschilderten Tatablauf; dies in zeitlicher wie auch in örtlicher Hinsicht. Denn auch die Funkzellenauswertung bestätigt das von dem Zeugen F. angegebene Bewegungsprofil, beginnend mit dem Weg hin zur B.straße, der Verweildauer am Tatort sowie der sich anschließenden Fahrt nach H. … Auch die Angaben des Zeugen F., er habe die Angeklagte spätestens bei dem unmittelbar nach der Tötung stattfindenden Treffen in H. hiervon unterrichtet, finden ihre Bestätigung in der Auswertung der Telekommunikationsdaten. So gab es im Zeitraum zwischen dem 19.12.2012 und dem 23.5.2013 zwischen der Angeklagten und dem Mordopfer P. 374 Telekommunikationsverbindungen. Allein … 18 (fallen) auf den 23.5.2013, den Tag der Ermordung. Die von der Angeklagten am 23.5.2013 um 20:06 Uhr ver-*

[10] Ihr war in einem ersten Verfahren vor dem LG Saarbrücken nicht hinreichend Rechnung getragen worden und hatte im ersten Revisionsdurchgang vor dem 5.Strafsenat zu einer Aufhebung des landgerichtlichen Urteils geführt, vgl. BGH, Beschluss vom 27.8.2014 – 5 StR 259/14 – bei juris

sandte SMS-Nachricht an den in der für die B.straße in S. maßgeblichen Funkzelle eingeloggten Anschluss des Mordopfers, der sich unmittelbar, 35 Sekunden später, eine SMS-Nachricht an den Zeugen F. anschloss, stellt jedoch die allerletzte dieser 374 Verbindungen dar, die sodann abrupt aufhören. Auch E-Mail-Verkehr findet ab diesem Zeitpunkt nicht mehr statt. Die Kammer ist daher überzeugt, dass weitere Verbindungen unterblieben, weil die Angeklagte vom Tod des P. wusste."

(2) Verfahrensgegenstand: Der Angeklagte ist vom Landgericht Chemnitz wegen Totschlags (§ 212 StGB) zu einer Freiheitsstrafe von neun Jahren verurteilt worden.[11] Der in D. lebende Angeklagte und seine Freundin H., die mit dem späteren Tatopfer in Ch. eine Scheinehe führte, stachen gemeinsam im Rahmen einer streitigen Auseinandersetzung in der Wohnung des Opfers auf dieses jeweils mit einem Messer ein und verletzten es tödlich. Nachdem sie gemeinsam geflüchtet waren, bemerkte die gesondert Verfolgte H., dass sie während der Tat ihre goldene Kette verloren hatte. Sie bat den Angeklagten, nochmals in die Wohnung zu gehen und das Schmuckstück zu holen. Der Angeklagte brach daraufhin etwa 30 Minuten nach dem Verlassen des Tatortes über eine Balkontür erneut in die Wohnung ein, ohne jedoch die später unter dem Leichnam sichergestellte Kette zu finden.

Beweisrechtliche Bedeutung von Verbindungsdaten: Der Angeklagte bestritt in der Hauptverhandlung vor der Strafkammer seine Tatbeteiligung und behauptete, er habe schon vor dem Tod des Geschädigten dessen Wohnung verlassen – nämlich etwa drei Stunden vor dem festgestellten Tatzeitpunkt. Zu dem nachfolgenden Einbruch in die Tatwohnung erklärte er, hierzu von H. gedrängt worden zu sein, nachdem sie „ihn dann kontaktiert (habe)".

Ihre Überzeugung davon, dass der Angeklagte (Mit-)Täter des Totschlags war, stützte die Strafkammer maßgeblich auch auf die Auswertung der Telekommunikationsdaten. Danach war aufgrund fehlender Telefonverbindungen zwischen den Handys der Beteiligten ausgeschlossen, dass H. nach einer von ihr allein begangenen Tat den Angeklagten telefonisch hätte kontaktiert haben

[11] LG Chemnitz, Urteil vom 27.11.2014, Az. 1 Ks 210 Js 1692/14; BGH, Beschluss vom 3.6.2015 – 5 StR 145/15.

können, um ihn nach mehrstündigen Aufenthalt in der für ihn fremden Stadt Ch. nochmals zu treffen und zur Suche nach dem verlorenen Schmuckstück aufzufordern. Zudem ergab die Verkehrsdatenauswertung, dass sich der Angeklagte jedenfalls noch über zwei Stunden nach seinem angeblichen Verlassen des späteren Tatortes mit seinem Handy in der die Wohnanschrift des Tatopfers abdeckenden Funkzelle befand.

(3) Verfahrensgegenstand: Die Angeklagte ist vom Landgericht Berlin wegen Mordes in Tateinheit mit Raub mit Todesfolge (§§ 211, 251 StGB) zu einer Freiheitsstrafe von zwölf Jahren verurteilt worden.[12] Der aus Serbien stammende Angeklagte reiste mit seinem Komplizen N. häufiger nach Deutschland und ins angrenzende Ausland zur gemeinsamen Begehung von Straftaten. Im April 2013 beschlossen sie zusammen mit den Mittätern T. und M., in Berlin einen Juwelier unter Einsatz eines Revolvers mit selbst gebautem Schalldämpfer zu überfallen. Der Angeklagte suchte mit M. am Vormittag des 29. April 2013 das für den Überfall ausgewählte Geschäft auf, wo M. den Juwelier sogleich erschoss. Der Angeklagte nahm Schmuckstücke aus den Auslagen an sich und floh zusammen mit seinen drei Komplizen nach Serbien, wo man die Beute für 43.000 Euro veräußerte.

Ermittlungstaktische Bedeutung von Verbindungsdaten: Die Kriminalpolizei ermittelte im Anschluss an das Verbrechen durch eine Abfrage der Verkehrsdaten, die in der den Tatort abdeckenden Funkzelle angefallen waren, serbische Telefonnummern, die zur Tatzeit genutzt worden waren. Die Datenerhebung ergab, dass um 10.58 und um 10. 59 Uhr zwei Verbindungen mit der Rufnummer 00381-65543XXXX in Tatortnähe stattgefunden hatten. Im Rahmen eines Rechtshilfeersuchens wurden die serbischen Behörden um Hilfe bei der Ermittlung der Anschlussinhaber gebeten. Die serbische Polizei teilte mit, dass sie vier Personen wegen des Raubmordes für tatverdächtig halte und benannte den Angeklagten und seine drei Mittäter. Der Angeklagte wurde als Anschlussinhaber der angefragten Telefonnummer 00381 65543XXXX bezeichnet.

[12] LG Berlin, Urteil vom 8.10.2014, Az. 234 Js 228 / 14 Ks 7/14; BGH, Beschluss vom 25.2.2015 – 5 StR 119/15.

Nachfolgend gab das serbische Innenministerium bekannt, der Angeklagte und die drei Tatverdächtigen N., M. und T. als seine Begleiter seien am 19. April 2013 aus Serbien aus- und am 30. April 2013 wieder eingereist. Im Rahmen eines weiteren Rechtshilfeersuchens legte der Angeklagte vor einem serbischen Ermittlungsrichter ein Geständnis ab und stellte sich in Kenntnis des gegen ihn erlassenen Haftbefehls den deutschen Strafverfolgungsbehörden.

Ohne den kurzfristigen Rückgriff auf die bei Netzbetreibern noch vorhandenen Verkehrsdaten nach § 96 TKG hätte das Verbrechen nicht aufgeklärt werden können. Zum späteren Tatnachweis in der Hauptverhandlung vor dem Landgericht spielten die zu Identifizierungszwecken erhobenen Verkehrsdaten keine Rolle mehr.

(4) Verfahrensgegenstand: Das Landgericht Köln hat den Angeklagten – nunmehr rechtskräftig – in dem aufsehenerregenden Fall eines „Mordes ohne Leiche“ gemäß § 211 StGB zu lebenslanger Freiheitsstrafe verurteilt.[13] Der Verurteilung lag als Sachverhalt zugrunde, dass der Angeklagte spätestens Ende März 2007 beschloss, seine von ihm getrennt lebende philippinische Ehefrau L. zu töten. Er wollte die Folgen der Trennungssituation für seine Umgangsmöglichkeit bezüglich des gemeinsamen Kindes nicht hinnehmen und befürchtete weitere Zahlungsverpflichtungen. Vor dem Hintergrund von Plänen seiner Ehefrau, zu einem Verwandtenbesuch auf die Philippinen zu reisen, sah er die Möglichkeit, ihr Verschwinden als freiwilligen Aufenthaltswechsel darzustellen. Am 18. April 2007 telefonierte das spätere Tatopfer L. mit einer Freundin. Sie beendete das Telefonat um 14.45 Uhr mit dem Hinweis, dass ihr Ehemann erscheine. Der Angeklagte suchte zu diesem Zeitpunkt L. auf und tötete sie noch am selben Tag, um das Sorgerecht für das gemeinsame Kind zu erhalten und Unterhaltszahlungen an L. einzusparen. Einzelheiten zum Tatort und zur Art und Weise der Tatausführung der Tötung blieben ungeklärt. Bis zu seinem Ar-

[13] LG Köln, Urteil vom 10.1.2013, Az. 111 Ks 1/12; BGH, Urteil vom 30.12.2014 – 2 StR 439/13, NStZ 2015, 291 s. auch zur vorhergehenden Urteilsaufhebung im 1. Revisionsdurchgang BGH, Urteil vom 22.12.2011 – 2 StR 509/10, BGHSt 57, 71.

beitsbeginn am nächsten Morgen beseitigte der Angeklagte auch die Leiche seiner Ehefrau so, dass sie bis heute nicht gefunden wurde.

Beweisrechtliche Bedeutung von Verbindungsdaten: Nach dem spurlosen Verschwinden der Ehefrau des Angeklagten am 18. April 2007 versuchte die Polizei zunächst lediglich aufgrund einer Vermisstenanzeige ihren Aufenthaltsort zu ermitteln. Erst nachdem sich Mitte August 2007 erhebliche Widersprüche in den Angaben des Angeklagten zu der von ihm vorgetäuschten Legende des Verschwindens ergeben hatten, wurde ein Ermittlungsverfahren wegen des Verdachts eines Tötungsdelikts eingeleitet. Erst ab Ende September 2007 wurden retrograde Verbindungsdaten zu dem Handy des Tatopfers und weiteren verdachtsrelevanten Handys erhoben und Funkzellenauswertungen für Empfangsbereiche durchgeführt, in denen die Tatausführung und eine spätere Leichenbeseitigung nahelag.

Trotz der aufgrund der verstrichenen Zeit teilweise vorgenommenen Datenlöschung bei dem Provider des Mobilfunkanschlusses des Tatopfers L. ergab die Auswertung der noch verfügbaren Verkehrsdaten, dass ihr seit dem Nachmittag des 18. April 2007 ausgeschaltet gewesenes Handy am frühen Morgen des 19. April 2007 für wenige Minuten noch einmal eingeschaltet war, bevor es für immer das Netz verlor. Das Handy der L. befand sich dabei in einer Funkzelle, die Teile eines Hafenbeckens sowie ein Baustellengelände abdeckte, auf dem zu diesem Zeitpunkt die Bodenplatte einer Tiefgarage noch nicht vollständig gegossen war; nach der Wertung des Landgerichts handelte es um ideale Ablageorte für eine Leiche. Ebenfalls am frühen Morgen des 19. April 2007 befand sich auch das Handy des Angeklagten in der betreffenden Funkzelle. Ausweislich der Funkzellenkontakte dieses Mobiltelefons hatte der Angeklagte noch vor Beginn seiner Frühschicht seine Wohnung verlassen und war kurz darauf dorthin zurückgekehrt. Diese Standortdaten wertete das Landgericht in diesem „Indizienprozess“ als Beweiszeichen dafür, dass der Angeklagte bis in die frühen Morgenstunden damit beschäftigt war, die Leiche und Spuren seiner ermordeten Frau verschwinden zu lassen.

Nach Wegfall der Vorratsdatenspeicherung aufgrund der Entscheidung des BVerfG vom 2. März 2010 hätten retrograd die nicht schon zu Vertragszwecken gespeicherten Standortdaten zu den verfahrensrelevanten Mobilfunkanschlüssen nicht mehr erhoben werden können. Bei der nunmehr im Regierungsentwurf (RegE) vorgesehene Vierwochen-Frist für eine Speicherung von Standortdaten in § 113b Abs. 1 Nr. 2 TGK (RegE) wäre wegen des späten Beginns der Ermittlungen wegen eines Tötungsdelikts im vorliegenden Fall ein wesentlicher Teil der beweisrelevanten Verkehrsdaten bereits gelöscht gewesen.

(5) Verfahrensgegenstand: Das Landgericht Würzburg verurteilte den Angeklagten in dem sog. „Autobahnschützen"-Fall wegen vierfachen versuchten Mordes, gefährlicher Körperverletzung und vorsätzlichen gefährlichen Eingriffs in den Straßenverkehr zu einer Gesamtfreiheitsstrafe von zehn Jahren und sechs Monaten.[14] Über 760-mal schoss der Täter in den Jahren 2008 bis 2013 deutschlandweit aus seinem LKW im fließenden Verkehr zumeist auf andere LKW und auf Transporter. Eine PKW-Fahrerin wurde schwer verletzt. Tatorte waren überwiegend Autobahnen.

Ermittlungstaktische und beweisrechtliche Bedeutung von Verbindungsdaten: Zunächst kamen die Ermittlungsbehörden durch eine massenhafte Erfassung von Autokennzeichen an mehreren Autobahnabschnitten dem Angeklagten auf die Spur. Daraufhin wurden zu der Mobilfunknummer des Verdächtigen die Verkehrsdaten erhoben, wobei den Ermittlungsbehörden der „glückliche" Umstand zugute kam, dass der Verdächtige den Mobilfunkanschluss eines Anbieters hatte, der die abrechnungsrelevanten Daten 90 Tage lang speicherte. Die erhobenen Daten glichen sie mit den Funkzellen mutmaßlicher Tatörtlichkeiten und Tatzeiten auf Hunderten von Kilometern deutscher Autobahnen ab. So ließen sich mit Hilfe der Standortdaten weitestgehend Übereinstimmungen mit den relevanten Tatstrecken und Tatzeiten feststellen und konnte die Anwesenheit des Angeklagten an einigen eindeutig festgestellten Tatorten zur Tatzeit

[14] LG Würzburg, Urteil vom 30.10.2014, Az. 801 Js 9341/13.

auch noch retrograd dokumentiert werden. Dadurch erhärtete sich der Tatverdacht.

Im weiteren Verfahren machte der Angeklagte zum äußeren Tatgeschehen weitgehend geständige Angaben. Beweisrechtlich hatte daher die zur Identifizierung des Täters beitragende Erhebung der Verkehrsdaten in der Hauptverhandlung vor dem Landgericht nur noch insoweit Bedeutung, als die Datenauswertung die teilgeständige Einlassung des Angeklagten bestätigte.

(6) Verfahrensgegenstand: Das Landgericht Flensburg verurteilte den Angeklagten, dem ursprünglich mit der Anklage ein versuchter Totschlag zur Last gelegt worden war, wegen gefährlichen Eingriffs in den Straßenverkehr (§ 315b StGB) in Tateinheit mit gefährlicher Körperverletzung (§ 224 StGB) zu einer Freiheitsstrafe.[15] Der zur Tatzeit als „Präsident“ der Rockerbande „Hells Angels“ in Flensburg fungierende Angeklagte erfuhr in der Nacht zum 23. September 2009 per Mobiltelefon, dass sich diverse Mitglieder der verfeindeten Rockerbande „Bandidos“ auf dem Rastplatz einer nahegelegenen Autobahnraststätte aufhielten. Er führte in den nächsten Minuten diverse Mobilfunkgespräche mit dem Ziel, möglichst schnell viele Mitglieder der „Hells Angels“ an die Autobahn heranzuführen, denn der von den Kutten tragenden „Bandidos“ begangene Gebietsverstoß sollte nicht hingenommen werden. Nachdem die Mitglieder der „Bandidos“ zur Weiterfahrt aufgebrochen war, folgten ihnen der Angeklagte und weitere Mitglieder der „Hells Angels“ mit mehreren Fahrzeugen. Der Angeklagte überholte den Konvoi der „Bandidos“ und streifte dabei vorsätzlich eines von deren Motorrädern. Dessen Fahrer stürzte hierdurch und wurde lebensgefährlich verletzt. Wenige Minuten nach der Tat und seiner Flucht vom Tatort meldete sich der Angeklagte mobiltelefonisch bei einem befreundeten Inhaber einer Kfz-Reparaturwerkstatt, um sein baldiges Erscheinen anzukündigen.

[15] LG Flensburg, Urteil vom 29.4.2011, Az. I Ks 1/10 – 109 Js 18703/09; BGH, Beschluss vom 11.1.2012 – 4 StR 523/11, BeckRS 2012, 03177.

Ermittlungstaktische und beweisrechtliche Bedeutung von Verbindungsdaten: Im Ermittlungsverfahren und in der Hauptverhandlung machten sämtliche unmittelbaren Tatzeugen von ihrem Recht zur Auskunftsverweigerung Gebrauch. Der Tatnachweis beruhte im Wesentlichen auf der Auswertung der retrograden Verkehrsdaten des Mobilfunkverkehrs des Angeklagten, der zwei Mobiltelefone mit sich führte und verwendete, und weiterer den „Hells Angels“ zuzuordnender Personen. Diese nach § 113a TKG a.F. gespeicherten Verkehrsdaten unterfielen der früheren (Übergangs-)Regelung der Vorratsdatenspeicherung[16] und konnten aufgrund der seinerzeit noch gültigen Speicherpflicht der Mobilfunkbetreiber noch erhoben werden. Insbesondere belegten die Geodaten, die bei Gesprächsverbindungen oder Verbindungsversuchen abgespeichert wurden, ein eindeutiges und synchrones Bewegungsbild der beiden Mobiltelefone des Angeklagten. Ohne den seinerzeit noch möglichen Rückgriff auf Vorratsdaten, deren Beweiswert auch im Revisionsverfahren noch thematisiert wurde,[17] hätte das Gewaltdelikt nicht aufgeklärt werden können.

(7) Verfahrensgegenstand: Das Landgericht Darmstadt verurteilte den Angeklagten wegen Mordes in Tateinheit mit Raub mit Todesfolge (§§ 211, 251 StGB) und mit unerlaubter Ausübung der tatsächlichen Gewalt über eine Kriegswaffe (§ 22a Abs. 1 KWKG) sowie wegen weiterer Waffendelikte zu einer lebenslangen Freiheitsstrafe als Gesamtstrafe und stellte die besondere Schwere der Schuld fest (§§ 211, 57a Abs. 1 Ziff.2 StGB).[18] Der Angeklagte lockte das Opfer unter dem Vorwand einer angeblichen Lieferung gestohlener Computer nachts auf ein abgelegenes Grundstück in Offenbach. Nachdem er den Interessenten erschossen und dessen Bargeld entwendet hatte, versenkte er die Leiche mit Unterstützung eines Mitarbeiters seines Unternehmens in einem Fluss. Die Leiche wurde erst nach einigen Wochen entdeckt.

[16] Im Erhebungszeitpunkt galt die durch die einstweilige Anordnung des BVerfG vom 11.3.2008 (1 BvR 256/08, BVerfGE 121, 1) vorläufig modifizierte gesetzliche Regelung des § 100g StPO.
[17] BGH, Beschluss vom 11.1.2012, aaO.
[18] LG Darmstadt, Urteil vom 1.12.2005, Az. 11 Ks - 1200 Js 82718/04; BGH, Beschluss vom 17.1.2007 – 2 StR 208/06.

Beweisrechtliche Bedeutung von Verbindungsdaten: Ausgangspunkt der Ermittlungen war eine Vermisstenanzeige der Ehefrau des Opfers. Sie war es auch, die den ersten Hinweis auf den Täter gab. Aufgrund der Gesamtumstände ging die Staatsanwaltschaft schon vor der Entdeckung der Leiche von einem Tötungsdelikt aus und leitete ein Ermittlungsverfahren ein. Zu den ersten Ermittlungsschritten gehörte die Erhebung der Verkehrsdaten zu den Mobilfunktelefonen des Opfers und des Täters. Im Ergebnis konnte der Täter aufgrund der Verbindungs- und vor allem der Standortdaten überführt und der Tatort festgestellt werden, an dem später eine Patronenhülse gefunden wurde. Die Aussagen des anfänglich als Gehilfen verdächtigen Mitarbeiters des Angeklagten bestätigten das Ergebnis der Auswertung der Verkehrsdaten. Ohne die Verkehrsdaten wäre der Tatnachweis nicht zu führen gewesen. Zudem entlasteten sie den Mitarbeiter, der seine Tatbeteiligung von Anfang an bestritten hatte, für dessen Tatbeteiligung aber anfangs gewichtige Beweiszeichen sprachen. Mittels der Standortdaten konnten die bestehenden Verdachtsmomente ausgeräumt und das Verfahren gegen ihn sodann eingestellt werden. Die Verkehrsdaten waren in diesem Fall mithin für eine umfassende Aufklärung sowohl be- als auch entlastender Tatumstände von entscheidender Bedeutung. Hervorzuheben ist, dass sich auch hier die noch vorhandene Möglichkeit einer Verkehrsdatenerhebung zugunsten eines Beschuldigten auswirkte.

d) Bandendiebstahl

(1) Verfahrensgegenstand: Das Landgericht Braunschweig hat die Angeklagten rechtskräftig wegen mehrfachen schweren Bandendiebstahls (§ 244a Abs. 1 StGB) und weiterer Diebstahlsdelikte zu mehrjährigen Gesamtfreiheitsstrafen verurteilt.[19] Sie hatten sich zusammengeschlossen, um jeweils nachts in Nord- und Ostdeutschland in die Geschäftsräume insbesondere von Postgebäuden einzubrechen. Bei der sich über einen zweimonatigen Zeitraum erstreckenden Serie von insgesamt 17 Einbrüchen erbeuteten sie in 13 Fällen Bargeldbeträge in drei- und vierstelliger Höhe.

[19] LG Braunschweig, Urteil vom 27.1.2015, Az. 1 KLs 72/14 – 201 Js 330161/14; BGH, Beschluss vom 15.8.2015 – 5 StR 274/15.

Ermittlungstaktische und beweisrechtliche Bedeutung von Verbindungsdaten: Zu den ersten drei innerhalb einer Nacht in Niedersachsen begangenen Einbrüchen hatte die Polizei für die Tatorte jeweils eine Funkzellenabfrage veranlasst und die erhobenen Daten untereinander verglichen. Für den ersten und den dritten Tatort waren jeweils für zwei Mobilfunknummern Gesprächsverbindungen verzeichnet. Eine Anschlussinhaberabfrage ergab, dass die Anschlüsse auf eine nicht existente Person angemeldet waren. Aus den Verkehrsdaten für die beiden Handys, die mit den festgestellten Mobilfunknummern verwendet worden waren, ergab sich – bezogen auf deren IMEI-Nummern –, dass in eines der Geräte tagsüber eine auf einen der Angeklagten registrierte SIM-Karte eingelegt war; außerdem zeigten die erhobenen Verkehrsdaten auf, dass beide Handys in der Tatnacht auch in eine Funkzelle in der Nähe des zweiten Tatorts eingeloggt waren. Damit konnte eine Verbindung zwischen den drei Einbrüchen hergestellt werden. In der Folgezeit konnte über Telefonate des bereits identifizierten Tatverdächtigen auch der Nutzer des zweiten Handys ermittelt und weiter festgestellt werden, dass beide Angeklagten auch bei Begehung von drei weiteren Einbrüchen untereinander und mit anderen Tatbeteiligten telefonierten. Nach dem 17. Einbruch konnten die Angeklagten schließlich auf frischer Tat festgenommen werden.

Ohne den kurzfristigen Rückgriff auf die bei Netzbetreibern noch vorhandenen Verkehrsdaten nach § 96 TKG hätte die Tatserie nicht aufgeklärt werden können. Beweisrechtlich hatten die zur Identifizierung der Täter führenden Verkehrsdaten in der Hauptverhandlung vor dem Landgericht nur noch insoweit Bedeutung, als sie die übereinstimmenden Geständnisse der Angeklagten bestätigten.

(2) Verfahrensgegenstand**:** Das Landgericht Kiel hat die Angeklagten rechtskräftig wegen mehrfachen schweren Bandendiebstahls (§ 244a Abs. 1 StGB) zu Gesamtfreiheitsstrafen verurteilt.[20] Die fünf aus Albanien stammenden Verurteilten verübten in der Umgebung von Kiel eine Reihe von Wohnungseinbrüchen.

Ermittlungstaktische Bedeutung von Verbindungsdaten: Im Rahmen von Ermittlungen gegen eine weitere albanische Tätergruppierung wurde die Polizei auf die von den Angeklagten gebildete Bande aufmerksam. Anhand einer Verkehrsdatenerhebung zu zwei von den Angeklagten genutzten Handys ließen sich hinreichend konkrete Erkenntnisse zu den an der Bandenabrede Beteiligten gewinnen, sodass als weitere Ermittlungsmaßnahmen eine Überwachung der Telekommunikation und Observationen ermittlungsrichterlich angeordnet werden konnten. Im Rahmen einer Observation wurden sie auf frischer Tat ertappt. In der Hauptverhandlung vor dem Landgericht legten die Angeklagten überwiegend Geständnisse ab. Zum Tatnachweis spielten die zu Identifizierungszwecken erhobenen Verkehrsdaten keine nennenswerte Rolle mehr.

(3) Verfahrensgegenstand**:** Die Angeklagten sind vom Landgericht Hamburg rechtskräftig unter anderem wegen schweren Bandendiebstahls in mehreren Fällen (§ 244a Abs. 1 StGB) sowie wegen unerlaubter Ausübung der tatsächlichen Gewalt über eine Kriegswaffe (§ 22a Abs. 1 KWKG) zu mehrjährigen Gesamtfreiheitsstrafen verurteilt worden.[21] Sie hatten sich zusammengeschlossen, um gewerbsmäßig 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.

[20] LG Kiel, Urteile vom 1.12. und 9.12.2014, Az. 10 KLs 21/14 u. 47/14 – 593 Js 11540/14; BGH, Beschlüsse vom 4.8.2015 – 5 StR 279/15 u. 280/15.
[21] LG Hamburg, Urteil vom 28.2.2012, Az. 616 KLs 17/11 - 6600 Js 30/11.

Ermittlungstaktische und beweisrechtliche Bedeutung von Verbindungsdaten: Die Überwachungskameras eines der geschädigten Betriebe zeichneten zwar das Tatgeschehen auf. Anhand der Überwachungsbilder war allerdings eine Identifizierung der Täter wegen deren Maskierung nicht möglich. Auf dem Videofilm war indes erkennbar, 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 bei 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 so überführten Angeklagten gestanden in der Hauptverhandlung die Taten überwiegend.

(4) Verfahrensgegenstand**:** Das Landgericht Münster verurteilte die Angeklagten rechtskräftig wegen einer Vielzahl von Diebstahls- und Computerbetrugsdelikten zu mehrjährigen Gesamtfreiheitsstrafen.[22] Die Angeklagten verübten zahlreiche Einbruchsdiebstähle, im Wesentlichen in öffentliche Gebäude wie Kindergärten, Schulen oder kirchliche Einrichtungen. Jeweils einer der Angeklagten hatte die Aufgabe, seinen Mittäter zum Tatort zu fahren und ihn zu sichern, während der Komplize in die jeweiligen Tatobjekte einbrach. Die Angeklagten sorgten in den Fällen, in denen sie beteiligt waren, auch für den Absatz der Beute. Während der Ausführung der einzelnen Taten stand der den Einbruch ausführende Mittäter jeweils über Mobiltelefon mit seinen Komplizen in ständiger Verbindung, um gegebenenfalls unverzüglich gewarnt werden zu können.

[22] LG Münster, Urteil vom 7.12.2009, Az. 8 KLs 81 Js 187/09 (17/09); BGH, Beschluss vom 4.11.2010 – 4 StR 404/10, NJW 2011, 467.

Beweisrechtliche Bedeutung von Verbindungsdaten: Im weiteren Verfahren machten die Angeklagten weitgehend geständige Angaben, die teilweise allgemein gehalten waren. Beweisrechtlich hatte daher die ursprünglich zur Identifizierung der Täter erfolgende Erhebung der Verkehrsdaten in der späteren Hauptverhandlung noch insoweit Bedeutung, als sie die teilgeständige Einlassung des Angeklagten bestätigten. Diese nach § 113a TKG a.F. gespeicherten Verkehrsdaten unterfielen der früheren (Übergangs-)Regelung der Vorratsdatenspeicherung und konnten aufgrund der seinerzeit gerade noch gültigen Speicherpflicht der Mobilfunkbetreiber noch erhoben und verwertet werden. [23]

e) Betäubungsmittelhandel

Verfahrensgegenstand: Das Landgericht Hamburg hat die Angeklagten rechtskräftig u.a. wegen Handeltreibens mit Betäubungsmitteln in nicht geringer Menge in mehreren Fällen zu mehrjährigen Freiheitsstrafen verurteilt (§ 29a BtMG).[24] Sie erwarben gemeinschaftlich insgesamt etwa 150 kg Marihuana in den Niederlanden, verbrachten das Rauschgift sodann nach Hamburg und verkauften es dort weiter. Dabei gingen sie arbeitsteilig vor: Drei Täter waren an den Beschaffungsfahrten in die Niederlanden beteiligt, während ein weiterer Täter 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 einer ermittlungsrichterlich nach § 100a StPO angeordneten Überwachung und Aufzeichnung der Telekommunikation einem konkreten Beschuldigten zugeordnet werden konnte, mit Hilfe von in den Niederlanden im

[23] Siehe oben Fn.16 und zum vorliegenden Fall auch BGH, Beschluss vom 4.11.2010 – 4 StR 404/10, aaO.: Die Revisionsrüge der Verwertung der Standortdaten blieb erfolglos.
[24] LG Hamburg, Urteil vom 26.5.2011, Az. 626 KLs 2/11 u. 7/11 - 6004 Js 232/10.

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 zuzuordnenden Mobilfunkanschlüsse ein Rückschluss auf ihre Abwesenheit vom Bundesgebiet möglich. Denn während der Zeiträume der vorgeworfenen Beschaffungsfahrten waren keine Daten im deutschen Mobilfunknetz angefallen. Dies korrespondierte mit einer Abrede, die im Zuge der Gesprächsüberwachung – nach § 100a StPO – mitgeschnitten worden war. Hiernach war zwischen den Angeklagten vereinbart worden, ihre Mobiltelefone während der Beschaffungsfahrten auszuschalten und in Hamburg zu belassen. Für in früheren Zeiträumen naheliegend durchgeführte Beschaffungsfahrten konnte auf Verkehrsdaten der von den Angeklagten in Deutschland verwendeten Mobiltelefone nicht mehr zurückgegriffen werden.

f) Betrug – „Enkeltrick“

Verfahrensgegenstand: Der Angeklagte wurde durch das Landgericht Hamburg rechtskräftig wegen des mehrfach begangenen Verbrechens eines banden- und gewerbsmäßig begangenen Betrugs (§ 263 Abs. 5 StGB) in der Begehungsweise eines „Enkeltricks“ zu einer Gesamtfreiheitsstrafe von drei Jahren und acht Monaten verurteilt.[25] Bei dieser sehr verbreiteten Betrugsart rufen mobile, häufig aus dem Ausland operierende Täter bei betagten Personen an und spiegeln ihnen vor, in einem verwandtschaftlichen Verhältnis zu ihnen zu stehen und dringend Geld zu benötigen. Häufig erleiden die Opfer schwerwiegende finanzielle und seelische Schäden. Im vorliegenden Fall erbeutete die Bande knapp 70.000 Euro. Der Angeklagte reiste jeweils aus seiner Heimat Litauen in das Bundesgebiet ein, um bei den Geschädigten in deren Wohnungen Bargelder abzuholen.

[25] LG Hamburg, Urteil vom 14.12.2012, Az. 622 KLs 20/12 - 6500 Js 75/12.

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.

g) Brandstiftung

Verfahrensgegenstand: Das Landgericht Hannover hat den Angeklagten rechtskräftig wegen schwerer Brandstiftung (§ 306a Abs. 1 StGB) zu einer Freiheitsstrafe von drei Jahren und sechs Monaten verurteilt.[26] Der Angeklagte hatte sich am Abend des 2. November 2009 gegen 19.00 Uhr in die Wohnung des kurzzeitig abwesenden Geschädigten begeben, wo er mit dessen Einverständnis bis zum Vortage gewohnt hatte. Er wollte die Wohnung durch Brandlegung zerstören. Um fahrlässiges Handeln des Geschädigten vorzutäuschen, schaltete er in der Küche eine Herdplatte an, auf die er einen brennbaren Gegenstand legte. Danach legte er in der Schlafecke des Wohnraums Feuer, das, wie beabsichtigt, auf das Bett übergriff; Hitzeschäden und Rauchgasablagerungen machten die gesamte Wohnung unbenutzbar. Während der Löscharbeiten erschien der Angeklagte und erklärte einem Polizeibeamten, er sei gekommen, um Medikamente zu holen, die er bei seinem Auszug zurückgelassen habe.

Beweisrechtliche Bedeutung von Verbindungsdaten: Der Angeklagte hatte sich in der Hauptverhandlung dahin eingelassen, er sei erstmals nach Beginn der Löscharbeiten am Gebäude eingetroffen. Um die von ihm benötigten Medi-

[26] LG Hannover, Urteil vom 23.4.2010, Az. 46 KLs 6503 Js 92914/09 (31/09); BGH, Urteil vom 13.1.2011 – 3 StR 332/10, BGHSt 56, 127.

kamente zu holen, habe er eine Bahn um 18.55 Uhr ab H. genommen; daher könne er nicht schon zur Zeit der Brandentstehung in S. gewesen sein. Daraufhin hatte das Landgericht mit Beschluss vom 15. Februar 20010 – und damit kurz vor der Aufhebung der (Übergangs-)Regelung zur Vorratsdatenspeicherung durch Urteil des BVerfG vom 2. März 2010 – die Erhebung der beim Mobilfunkprovider gespeicherten Verkehrsdaten des Mobiltelefonanschlusses des Angeklagten angeordnet. Zur Begründung führte es aus, ohne die Datenerhebung, welcher der Angeklagte zugestimmt habe, werde die Aufklärung seines Aufenthalts zur Tatzeit wesentlich erschwert.

Nach Auswertung der erhobenen Standortdaten, die das Mobilfunkunternehmen – eigener Auskunft zufolge – lediglich noch aufgrund seiner gesetzlichen Verpflichtung nach § 113a TKG vorgehalten und für eigene Zwecke nicht mehr benötigt hatte, hielt das Landgericht die Einlassung des Angeklagten für widerlegt. Dabei hat es sich unter anderem darauf gestützt, dass das Mobiltelefon des Angeklagten bereits ab 19.00 Uhr mehrfach an einem zwischen der Wohnung des Geschädigten und dem Bahnhof S. stehenden Funkmast eingeloggt war. Zugleich stellten die Standortdaten ein gewichtiges Indiz dafür dar, dass sich der Anklagte zur Tatzeit am Tatort aufhielt. Damit hätte ohne die (gerade noch) verfügbaren Vorratsdaten der Tatnachweis durch das Landgericht nicht geführt werden können, was im weiteren Verfahren zur Folge hatte, dass mit der Revision in erster Linie die Verwertung der Standortdaten – allerdings erfolglos – gerügt wurde.

2. Zusammenfassende Überlegungen

Die Reihe von Verfahren, in denen beispielhaft die Erhebung von Verkehr- und insbesondere von Standortdaten zur Verbrechensaufklärung in unterschiedlichen Bereichen der Schwerkriminalität beitrug, ließe sich unbegrenzt fortsetzen. Denn bisher waren trotz des Beweismittelverlusts, zu dem der Wegfall gespeicherte Vorratsdaten nach der Entscheidung des BVerfG vom 2. März 2010 geführt hat, in vielen Fällen glücklicherweise noch die von den Providern

zu geschäftlichen Zwecken nach § 96 TKG gespeicherten Verkehrsdaten vorhanden, wodurch bei Aufklärung von Seriendelikten sich zugleich weitere schwere Straftaten der Wiederholungstäter verhindern ließen.[27] Dies darf allerdings nicht darüber hinwegtäuschen, dass in einer Vielzahl von Fällen durch die Aufhebung der gesetzlichen Regelung zur Vorratsdatenspeicherung schwerste Delikte nicht aufgeklärt werden konnten, wie eine Untersuchung des BKA aus dem Jahr 2011 zu den Auswirkungen des Wegfalls der Mindestspeicherungsfristen erschreckend anschaulich gezeigt hat.[28]

Die vorstehend dargestellten 20 Verfahrensskizzen belegen, dass sich Verkehrsdaten teilweise als Indizien zum unmittelbaren Tatnachweis eignen; in der überwiegenden Anzahl der Fällen dienen sie als erster Ermittlungsansatz und wirken sie als Hebel für weitere Ermittlungsschritte. Die Daten liefern grundsätzlich Hinweise auf weitere Personen, die im unmittelbaren zeitlichen und örtlichen Zusammenhang mit der Tat im Kontakt zum Verdächtigen standen, und tragen so dazu bei, die Täterstrukturen aufklären. Ferner können sie Schlüsse auf die jeweilige Anwesenheit eines Verdächtigen an bestimmten Orten zu bestimmten Zeiten tragen, Rückschlüsse auf dessen Reisewege – etwa

[27] Ein anschauliches jüngeres Beispiel aus der Medienberichterstattung liefert etwa der vor dem Landgericht Münster verhandelte Fall, in dem zwei Autobahnbrückenwerfer am 22.6.2015 wegen sechsfachen versuchten Mordes in Tateinheit mit gefährlichem Eingriff in den Straßenverkehr zu langjährigen Gesamtfreiheitsstrafen verurteilt wurden. Nach dem letzten Wurf der aus Langeweile begangenen Tatserie (mit einer Betonplatte) konnte über Funkzellenabfragen an den verschiedenen Tatorten, Abgleich der erhobenen Daten und Handyortung einer der Täter ermittelt werden, der im Rahmen seines alsbald abgelegten Geständnisses auch seinen Mittäter benannte. Siehe hierzu:
http://www.faz.net/aktuell/gesellschaft/kriminalitaet/holzstaemme-auf-die-a1-gericht-bestraft-jungenstreich-als-mordversuch-13662147.html und
http://www.wn.de/Muensterland/2025976-Haftstrafe-fuer-Brueckenwerfer-Kein-Streich-mehr-sondern-versuchter-Mord

[28] Vgl. zusammenfassend und mwN Münch, ZRP 2015, 130: Danach wurden insgesamt Auskunftsersuchen für 5082 Anschlüsse im Zeitraum vom 2.3.2010 bis 26.4.2011 erfasst und ausgewertet; im Bereich der Strafverfolgung konnte in 83 % der Fälle (3521 Anschlüsse) die Straftat nicht mehr aufgeklärt werden. Zutr. merkt Münch, aaO, hierzu an, dieses Ergebnis verdeutliche, dass Verkehrsdaten bei der Strafverfolgung häufig den ersten, sichersten und zugleich effizientesten Ermittlungsansatz darstellen. Wie die hier aufgeführten Beispielsfälle zeigen, gilt dies nicht nur für die nach dem Aufgabenzuschnitt des BKA (§ 4 BKAG) geführten Ermittlungsverfahren. Siehe zu teilweise spektakulären nicht mehr aufklärbaren Fällen auch die Presseinformation des BKA vom 8. Oktober 2010 „Die Bedeutung von Mindestspeicherfristen für Gefahrenabwehr und Strafverfolgung“,
http://www.bka.de/nn_234028/SharedDocs/Downloads/DE/ThemenABisZ/Mindestspeicherfristen/101008PresseinformationMindestspeicherfristen.html

bei unerlaubter Drogeneinfuhr oder Schleuserhandlungen – zulassen oder über die jeweils zu einer Telefonnummer feststellbaren Gesprächsverbindungen die Identität eines Anschlussnutzers nachvollziehbar belegen; dies alles, ohne dass hierbei auf Gesprächsinhalte zugegriffen wird, deren Überwachung erst als weiterer Ermittlungsschritt und nur unter den strengen Voraussetzungen des § 100a StPO richterlich angeordnet werden kann zur Klärung eines hinreichend konkretisierten Tatverdachts hinsichtlich einer der dort genannten schweren Katalogstraftaten.

Ein Rückgriff auf gespeicherte Verkehrsdaten kann auch die Aufklärung von Tatserien erleichtern. So ermöglichen etwa Kreuzvergleiche zwischen verschiedenen Funkzellen und unterschiedlichen Tatorten eine Überprüfung, ob jeweils dasselbe Mobiltelefon bzw. derselbe Mobilanschluss dort eingeloggt war. Oftmals hängt die Durchführung tatzeitnaher Ermittlungen, bei denen ein durch Datenlöschung eintretender Beweismittelverlust vermieden werden kann, allerdings von Zufälligkeiten wie etwa dem Anzeigeverhalten eines Tatopfers oder sonstigen Umständen einer Tatentdeckung ab, in deren Anschluss erst neben einer Sicherung und Auswertung von Tatortspuren eine Verkehrsdatenerhebung erfolgen kann. Zu diesen von den Ermittlungsbehörden schon nicht steuerbaren Umständen kommt bisher die Zufälligkeit hinzu, für welche Zeitdauer der jeweilige Funknetzbetreiber aus geschäftlichen oder betriebstechnischen Gründen die beim ihm anfallenden Verkehrsdaten speichert; die Zeitspanne reicht von mehreren Tagen bis zu mehreren Monaten. Mit der beabsichtigten Neuregelung der Vorratsdatenspeicherung wird dem vorgebeugt, indem die Telekommunikationsanbieter gemäß § 113b Abs. 1 Nr. 2 TGK (RegE) verpflichtet werden, Standortdaten für vier Wochen zu sichern.

Die Verfahrensskizzen zeigen ferner, dass den durch eine Verkehrsdatenauswertung gewonnenen Erkenntnissen eine entscheidend entlastende Wirkung zukommen kann. Gerade bei dem Rückschluss auf den Nutzer eines tatrelevanten Mobiltelefons ist einem Beschuldigten durch die Verkehrsdaten das Vorbringen verdachtsentkräftender Umstände – etwa in Form einer Alibibe-

hauptung (vgl. vorstehend die Fälle zu I.1.b [4], 1.c [6]) – in verschiedener Hinsicht möglich.

3. Bedeutung von Verkehrsdaten auf weiteren Deliktsfeldern

Über die vorstehend anhand von Verfahren aus dem Alltag der Ermittlungsbehörden und Strafgerichte beschriebene Bandbreite von dort bearbeitenden Erscheinungsformen der Schwerkriminalität hinaus gibt es zahlreiche Deliktstypen, in denen Verkehrsdaten wegen spezifischer Tatbegehungsweisen eine besondere Bedeutung als bisweilen einziger Ermittlungsansatz zukommt.[29]

a) Kinderpornographie in Kommunikationsnetzen

Hinzuweisen ist zunächst auf die besondere Bedeutung von Bestandsdaten zu IP-Adressen im Kontext mit der effektiven Verfolgung einer Verbreitung von Kinderpornographie im Internet. Der Austausch von kinderpornografischem Material wurde inzwischen weitgehend ins Internet verlagert. Deutsche Ermittlungsbehörden erfahren hiervon und den damit begangenen Straftaten auf unterschiedliche Weise. Regelmäßig werden durch ausländische und internationale Polizeidienststellen (wie FBI und Europol) beispielsweise zu deutschen Nutzern die sie betreffenden Daten von sichergestellten Servern oder anderweitig ermittelte Informationen übersandt. Polizeiliche Aufgabe ist es dann zu versuchen, die Personen hinter den IP-Adressen zu ermitteln und so aufzuklären, wer sich kinderpornografisches Material bestellt oder dieses verbreitet hat. Allein vom National Center for Missing & Exploited Children (NCMEC) werden aus den USA monatlich mehrere hundert Fälle an das BKA übersandt. Infolge Löschung bzw. Nichtspeicherung der Verkehrsdaten (d. h. der dynamischen IP-Adressen) ist es kaum möglich, den Besteller ausfindig zu machen. Oft fehlt so der einzige Ermittlungsansatz und die Täter bleiben unentdeckt. Dies dürfte zu-

29 Siehe hierzu die Übersichten des BKA, aaO (Fn. 28).

künftig mit Blick auf jüngste Gesetzesänderungen weiter an Bedeutung gewinnen.[30]

Die Konsumenten von Kinderpornographie werden sich naheliegend einer neu geschaffenen Zugriffsmöglichkeit auf Verkehrsdaten auch nicht dadurch entziehen, dass sie den Datenabruf von Internet-Cafés aus betreiben; sie suchen erfahrungsgemäß die Privatheit und werden den eigenen Internet- bzw. Telefonanschluss auch weiterhin nutzen. Die Ausweitung der Speicherung ist naheliegend geeignet, über die bereits bestehenden Ermittlungsinstrumente der §§ 95, 96 TKG, § 15 TMG und § 100j StPO hinaus (Abfrage von Nutzer-, Bestands- und Verkehrsdaten mittels Auskunftsersuchen nach §§ 161, 163 StPO), eine zahlenmäßig breitere Aufklärung – gerade auch in der Pyramide der Täter nach oben hin – zu ermöglichen. Insbesondere ist 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 absehbar.

b) Internetbasierte Kriminalität

Ein hier ebenfalls nur zu streifender, für die Ermittlungsbehörden höchst relevanter Kriminalitätsbereich, in dem Aufklärungsmöglichkeiten bei fehlenden Mindestspeicherfristen kaum bestehen, sind die über das Internet als Tatmittel begangenen Delikte.[31] Schwerwiegendere Kriminalitätserscheinungen in diesem Bereich sind insbesondere gewerbs- und bandenmäßige über das Internet und ergänzend unter Zuhilfenahme von Telekommunikationseinrichtungen begangene (Computer-) Betrugstaten und Cyberangriffe zur Schädigung von Unternehmen, öffentlichen Einrichtungen und Privatleuten insbesondere über sogenannte Botnetze.

[30] Vgl. Neunundvierzigstes Gesetz zur Änderung des Strafgesetzbuches – Umsetzung europäischer Vorgaben zum Sexualstrafrecht v. 21. Januar 2015, BGBl. I, S. 10 ff.
[31] Vgl. den Überblick des BKA in: Cybercrime, Bundeslagebild 2012; instruktiv einführend hierzu auch der Lexikon-Artikel „Internetkriminalität“ bei Wikipedia.

Indem sich Täter beispielsweise mit fremden oder gefälschten Zugangsdaten bei Internet-Providern einloggen, können sie unbefugt so genannte SIM-Locks bei Mobiltelefonen entsperren und erhalten so Zugang zu Telefonanschlüssen, unter deren Verwendung weitere Straftaten begangen werden.[32] Ließe sich hier die verwendete IP-Adresse ermitteln, könnten die bei der Zugangserschleichung zu Telefonanschlüssen anfallenden Logdaten ausgewertet und Täter identifiziert werden. Um Straftaten aufklären zu können, die Cyberkriminelle über „gekaperte" Rechner begangen haben, zu denen sie sich über mittels Trojaner eingeführter Schadsoftware Zugang verschafften, und zugleich die Botnetze zu vernichten, ist es unentbehrlich zu wissen, welche Geräte Teil des Netzes sind. Wenn bekannt ist, wer hinter der IP-Adresse eines Bot steht, wer Inhaber eines zum Zwecke des Identitätsdiebstahls infizierten Geräts ist, können die Opfer kontaktiert werden, die ihre missbrauchten Geräte durch „Reinigen" aus dem Botnetz trennen und ggf. noch verhindern können, dass von den Tätern mit ausgespähten Online-Zugangsdaten zu Bank- und Kreditkartenkonten Abhebungen durchgeführt werden. Andernfalls können selbst bei Überführung eines Täters, der Botnetze über seinen Rechner und angemietete Server steuert, die durch das Ausspähen ihrer Daten (§ 202a StGB) Betroffenen nicht informiert werden, die durch noch nicht ermittelte Komplizen des Täters weiterhin mit Schäden infolge eines Bankdatenmissbrauchs (§ 152b StGB, § 263a StGB) bedroht sind.[33]

c) Terroristische Straftaten

Nicht zuletzt weist das BKA – aus ermittlungsrichterlicher Sicht völlig zu Recht – auch darauf hin, dass (jenseits gefahrenabwehrrechtlicher Aspekte) die Strafverfolgung gerade auch terroristischer Straftaten, etwa solche von Mitgliedern oder Unterstützern des sog. Islamischen Staats, ohne Verkehrsdatenspei-

[32] vgl. zu Beispielsfällen Presseinformation des BKA vom 8. Oktober 2010 „Die Bedeutung von Mindestspeicherfristen für Gefahrenabwehr und Strafverfolgung", aaO.

[33] Dies zeigte sich beispielhaft in einem vom Landgericht Berlin mit Urteil vom 12.2.2014 (Az. 536 KLs 8/13 – 255 Js 750/13) entschiedenen Fall (vgl. BGH, Beschluss vom 29.7.2014 – 5 StR 233/14, bei juris), in dem der Angeklagte, der ua wegen Geldwäsche, Computerbetrugs und gewerbsmäßiger Fälschung von Zahlungskarten zu einer mehrjährigen Gesamtfreiheitsstrafe verurteilt wurde, zur Begehung seiner Straftaten insgesamt vier Botnetze betrieben hatte.

cherung deutlich erschwert oder gar unmöglich sei.[34] Mit Hilfe dieser Daten können die Anrufziele der etwa in den Irak oder nach Syrien ausgereisten Verdächtigen, die zuvor in Deutschland häufig in Kontakt zu anderen Personen der islamistischen Szene gestanden haben, erhellt und hierdurch Erkenntnisse über die Strukturen und Beteiligtenkreise im Bundesgebiet gewonnen werden. Indem Unterstützer ermittelt und strafrechtlich verfolgt werden, lässt sich islamistischer Terrorismus effektiv durch das Strafrecht bekämpfen und generalpräventiv terroristischen Straftaten vorbeugen. Namentlich lassen sich Urheber im Internet hochgeladener, gewaltverherrlichender Videos ermitteln.

Hingegen geht die Erwägung fehl, wonach die Terroranschläge von Paris im Januar 2015 die Ungeeignetheit der Verkehrsdaten zur Abwehr terroristischer Gewalttaten belegen könne. Die in Frankreich mit besonders langer Speicherfrist vorrätig gehaltenen Verkehrsdaten konnten den Anschlag zwar nicht verhindern; dies schaffen andere repressive und eben nicht gefahrenabwehrrechtliche Ermittlungsinstrumente, wie etwa Wohnraumdurchsuchungen, jedoch ebenfalls nicht. Ermöglicht wird aber insbesondere durch die Erhebung von Verbindungsdaten der von den Tätern verwendeten Mobilfunkanschlüsse eine Aufhellung ihres Umfeldes, ihrer Kontaktpersonen und Unterstützer. So konnten die französischen Sicherheitsbehörden anhand gespeicherter Verbindungsdaten Kontakte der Terroristen untereinander und zu anderen Islamisten schnell nachvollziehen, was bei der schnellen Aufklärung und Bewertung einer möglichen weiteren Bedrohung half.

Insofern lässt sich ausmalen, welche wichtigen Hinweise nach Aufdeckung der NSU-Terrorzelle im November 2011 die Verbindungs- und Standortdaten zu den mehreren weitgehend zerstört sichergestellten Handys der Gruppe hätten liefern können, wären diese Daten noch in nennenswertem Umfang gespeichert und durch die seinerzeit von den Ermittlungsrichtern des BGH nach § 100g StPO erlassenen Anordnungen zu erheben gewesen. Die einen Unterstützerkreis der Gruppe betreffenden Fragen aufzuklären, wie es gegenwärtig im

[34] Münch, ZRP 2015, 131 f.

Strafprozess vor dem OLG München mühselig mit teilweise unwilligen Zeugen versucht wird, wäre sicher leichter gefallen.

Ein aktuelles Beispiel aus dem Bereich der Bekämpfung terroristischer Straftaten in Deutschland, bei dem der nicht nur für die Strafverfolgung, sondern vor allem auch für die Gefahrenabwehr wichtige Erfolg offenbar auch durch einen Zugriff auf Verkehrsdaten ermöglicht worden ist, stellt der Fall des in der Nacht zum 30. April 2015 verhafteten Salafisten-Paares dar, das in den Wochen zuvor eine funktionsfähige Rohrbombe gebaut und im Keller seines Hauses zusammen mit Waffenteilen und Munition gelagert hatte. Das Paar wohnte in der Nähe der Strecke eines traditionell zum 1. Mai veranstalteten Frankfurter Radrennens. Der Beschuldigte Halil D., der Kontakt zu mehreren aus dem Kriegsgebiet in Syrien zurückgekehrten Islamisten hielt, hatte in den Tagen vor seiner Festnahme mehrfach auch entferntere, als Beobachtungs- und Anfeuerungsorte für Zuschauer geeignete Plätze entlang der Strecke des Radrennens näher inspiziert, das nach Aufdeckung seines kriminellen Tuns abgesagt werden musste. Der *Spiegel* hob in seinem Bericht[35] über den Lauf des Ermittlungsverfahren auch das erhebliche Glück hervor, das bei dem Aufklärungserfolg der Ermittlungsbehörden und ihrer Verhinderung eines mutmaßlich geplanten Terroranschlags in Deutschland erneut im Spiel war:

> *„Glück, dass eine Baumarktkassiererin so aufmerksam war. Glück, dass es nicht nur ein Überwachungsvideo gab, sondern auch einen Fingerabdruck, und dass die Daten der Funkzelle noch nicht gelöscht waren.“*

Sich auf derartiges Glück nicht mehr im bisherigen Ausmaß verlassen zu müssen, wird naheliegend nach einer Wiedereinführung der Vorratsdatenspeicherung die künftige Ermittlungsarbeit zur Verhinderung drohender und Aufklärung begangener terroristischer Gewaltdelikte erleichtern.

[35] Ausgabe Nr. 20 vom 9.5.2015, S. 34, 36.

II. Gutachten des Max-Planck Instituts aus dem Jahre 2011

1. Fehlende Belastbarkeit des gutachterlichen Ergebnisses

Vor dem Hintergrund der vorstehend geschilderten eigenen praktischen Erfahrungen und der hierdurch begründeten Erwartung betreffend einer Speicherpflicht mit einer Höchstspeicherfrist für Verkehrsdaten kann der *Verf.* die vorsichtige Bewertung der praktischen Bedeutung einer Vorratsdatenspeicherung durch das Max-Plack-Institut für ausländisches und internationales Strafrecht (MPI) in Freiburg aus dem Jahre 2011 nicht teilen.

Nach dessen „Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten“ soll diesem Ermittlungswerkzeug in den vom MPI ausgewählt betrachteten Deliktsbereichen – namentlich mit Blick auf die vor und nach Einführung der Höchstspeicherfrist angeblich gleichgebliebenen Aufklärungsquoten – keine signifikante Bedeutung zukommen. Dem Auftragsgutachten zugrunde liegt u.a. eine Auswertung von etwa 80 Gesprächen mit Strafrechtspraktikern aus Polizei, Staatsanwaltschaft und Strafjustiz sowie etwa 50 vom Bundeskriminalamt geführter Ermittlungsverfahren.

Neben den vom MPI selbst zur Belastbarkeit seiner Erhebungen formulierten Bedenken[36] in Bezug auf eine schmale Datenbasis bestehen solche auch mit Blick auf den gewählten gutachterlichen Ansatz. Der Vergleich von Aufklärungsquoten vor und nach Einführung der Speicherfristen lässt schon nicht erkennen, ob es während der Erhebungszeiträume nicht auch andere Ursachen für eine stabile Aufklärungsquote gegeben hat. Ferner können die ausgewerteten Verfahrensakten des BKA keinen zuverlässigen Überblick über sämtliche Kriminalitätsbereiche vermitteln, in denen Verkehrsdaten einen Ermittlungsansatz bieten; befasst sich das BKA bei seinen Ermittlungen nach dem durch § 4 BKAG vorgegebenen Katalog von Straftaten, bei denen es die polizeilichen

[36] Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Max-Planck-Institut für ausländisches und internationales Strafrecht, Freiburg, 2. Aufl. 2011, S. 7 ff.; vgl. zu den vom MPI getroffenen Schlussfolgerungen trotz schmaler Datenbasis auch 218, 221 f.

Aufgaben auf dem Gebiet der Strafverfolgung wahrnimmt, doch nur mit sehr ausgewählten Deliktsphänomen, etwa dem Terrorismus, der Spionage oder besonders umfangreicher Bandenkriminalität. Zu letzterer hat das MPI lediglich zwölf Verfahren auswerten können.[37]

Auch die vom MPI ausgewählten Deliktsbereiche erweisen sich als unvollständig. Zunächst erfassen sie solche (etwa das Stalking), um die es gegenwärtig in der Diskussion über den Regierungsentwurf nicht mehr geht. Zum anderen behandelt das Gutachten solche Bereiche nicht, die nach Einschätzung des *Verf.* besonders relevant sind. Gerade bei schweren Raub- und Erpressungstaten haben sich die Verkehrsdaten – wie die vorstehenden Skizzen illustrieren – als effizientes Ermittlungsinstrument und die hieraus gewonnenen Erkenntnisse als gewichtiges Beweismittel erwiesen. Die Bundesregierung erfasst diese Delikte mit Recht in § 100g Abs. 2 Nr. 1 Buchst. g StPO (RegE). Gerade bei der Erpressung belässt es das MPI-Gutachten aber bei einem Hinweis auf die polizeiliche Kriminalstatistik und die hiernach „seit Anfang des Jahrtausends stabile Aufklärungsquote“; eine Untersuchung der Effektivität dieses Instruments auch am Einzelfall fehlt.[38]

Überdies erscheint es unverständlich, wenn die Kriminalitätserscheinung des „Enkeltrickbetrugs“, die zwar „nur“ 0,2% der Betrugstaten ausmachen soll, aber doch häufig die Verbrechensqualifikation eines banden- und gewerbsmäßigen Betrugs nach § 263 Abs. 5 StGB erfüllt, als ein „Randphänomen“ beschrieben wird, was – etwa deshalb? – nicht mit dem Aufwand einer Verkehrsdatenspeicherung verfolgt werden sollte. Ebenso wenig weiterführend ist die Überlegung, durch das Absehen von einer Auswertung von Datenträgern zur Verfolgung der Kinderpornographie könnten die dort verausgabten Haushaltsmittel geschont und stattdessen in die Täterprävention investiert werden.[39] Solches erscheint gerade mit Blick auf das Legalitätsprinzip und die erst jüngst vom Gesetzgeber verabschiedete Verschärfung dieses Teilbereichs des Straf-

[37] MPI, a.a.O., S. 114.
[38] MPI, a.a.O., S. 113.
[39] MPI, a.a.O., S. 221.

rechts[40] bemerkenswert. Überdies verstellt der Vorschlag den Blick darauf, dass ältere Verkehrsdaten insbesondere den Ursprung und den Weg, den eine Bilddatei zurückgelegt hat, zu erhellen und damit Aufklärungsquoten zu steigern vermögen.

Vor allem erstaunt allerdings, dass die im Gutachten dokumentierten Ergebnisse der Praktiker-Interviews ganz überwiegend die hier geäußerte Einschätzung teilen, dass gespeicherte Verkehrsdaten ein Ermittlungsinstrument von erheblicher Bedeutung für die Verbrechensaufklärung sind. Eine Stimme wird dem durch das Gutachten indes nicht verliehen.

2. Möglichkeiten empirischer Erhebungen

Abschließend sei zu Möglichkeiten empirischer Erhebungen in diesem Bereich über die vom MPI in seinem Gutachten selbst dargestellten Problemstellungen hinaus auf Folgendes hingewiesen:

Die Bedeutung des Ermittlungsinstruments „Verkehrsdaten“ lässt sich regelmäßig nicht am Verfahrensergebnis, dem rechtskräftigen Strafurteil, erkennen. Denn Verkehrsdaten sind oftmals nur ein erster Hebel, um die Identität der Täter zu ermitteln, Strukturen zwischen ihnen und anderen Tatbeteiligten zu erhellen und sodann gegebenenfalls mit Hilfe anderer, eingriffsintensiverer Maßnahmen (etwa Überwachung der Telekommunikationsinhalte oder Durchsuchungen) nähere Erkenntnisse zu erzielen. Ein solches weiteres Ermittlungsergebnis oder sogar ein – etwa in Ansehung erdrückender Beweislage – abgelegtes Geständnis ist dann schon vielfach Beweisgrundlage für die Annahme eines hinreichenden Tatverdachts bei Anklageerhebung und noch häufiger für die Überzeugungsbildung des Tatgerichts (§ 261 StPO). Dementsprechend wird in Fällen, in denen die erhobenen Verkehrsdaten nur als erster Ermittlungsansatz eine Rolle spielten, der ursprüngliche Einsatz dieses Ermittlungsinstruments in dem das tatgerichtliche Verfahren abschließenden Urteil nicht mehr erwähnt.

[40] Vgl. Neunundvierzigstes Gesetz zur Änderung des Strafgesetzbuches – Umsetzung europäischer Vorgaben zum Sexualstrafrecht v. 21. Januar 2015, BGBl. I, S. 10 ff.

Eine belastbare empirische Untersuchung müsste sich daher in einem repräsentativen Umfang mit Verfahren aus sämtlichen relevanten Deliktsbereichen befassen und hier jeweils den konkreten Ablauf der Ermittlungen untersuchen und den Ablauf der gerichtlichen Beweisaufnahme und Überzeugungsbildung bewerten. Um die Erforderlichkeit einer Verkehrsdatenabfrage und der Effizienz zur Tataufklärung jeweils beurteilen zu können, dürften ermittlungstaktische Kenntnisse und Erfahrungen bei den Gutachtern unabdingbar sein.

III. Fazit

1. Die Möglichkeit einer Verkehrsdatenabfrage ist nach den praktischen Erfahrungen des *Verf*. ein aus der ermittlungstaktischen Arbeit der Strafverfolgungsbehörden nicht wegzudenkendes Ermittlungsinstrument. Die Annahme des BVerfG[41], dass „hierdurch Aufklärungsmöglichkeiten geschaffen (werden), die sonst nicht bestünden und angesichts der zunehmenden Bedeutung der Telekommunikation auch für die Vorbereitung und Begehung von Straftaten in vielen Fällen erfolgversprechend sind“, hat sich auch nach seinem Urteil vom 2. März 2010 – trotz der durch Wegfall der Vorratsdatenspeicherung entstandenen Schutzlücke – in unzähligen Strafverfahren bestätigt.
2. Die geschäftsmäßige Speicherung der Verkehrsdaten durch die betreffenden Telekommunikationsunternehmen (§ 96 TKG) bietet keine ausreichende Grundlage für eine rechtsstaatliche Aufklärung schwerer Straftaten. Die vom Regierungsentwurf vorgesehene Wiedereinführung einer Speicherpflicht von Telekommunikationsunternehmen ist notwendig, um zu vermeiden, dass die Ergebnisse von Strafverfahren zufallsbedingt von

[41] BVerfG, Urteil vom 2.3.2010 – 1 BvR 256/08, u.a., BVerfGE 125, 260, Rn. 207; ähnlich der EuGH, in seinem Urteil vom 8.4.2014 – C-293/12, NJW 2014, 2169, 2171:
„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.“

dem Zeitpunkt eines Ermittlungsbeginns und von der unterschiedlichen Praxis der Telekommunikationsunternehmen hinsichtlich Umfang und Dauer von Speicherungen abhängen; diese Praxis ist nach Maßgabe ihrer eigenen geschäftlichen Bedürfnisse willkürlich und – wie die weite Verbreitung von Flatrates und ein damit einhergehendes Entfallen von Verbindungs-Einzelabrechnungen zeigt – einem rasanten Wandel unterworfen. Zufallsbedingte Verfahrensergebnisse sind mit den – auch verfassungsrechtlichen – Anforderungen an eine gleichmäßige funktionstüchtige Strafrechtspflege unvereinbar.

3. Die mit dem Gesetzentwurf beabsichtigte Speicherung von Verkehrsdaten bei privaten Telekommunikationsprovidern unterscheidet sich in der praktischen Ausgestaltung nicht von der geschäftsmäßigen Speicherung von Verkehrsdaten durch diese Unternehmen aufgrund der vertraglichen Beziehungen mit ihren Kunden. Eine staatliche „Überwachung“ aller Nutzer mobiler Telekommunikation ist mit dem geplanten Gesetz nicht verbunden.

4. Der Gesetzentwurf will sicherstellen, dass kurzfristig gespeicherte Verkehrsdaten von den Strafverfolgungsbehörden nur zur Aufklärung schwerwiegender Straftaten und nur mit richterlicher Genehmigung abgerufen und verwendet werden dürfen. Dass die Hürden für diese Maßnahme mit dem Straftatenkatalog nach § 100g Abs. 2 StPO (RegE) allerdings ebenso hoch sein sollen wie bei der – freilich ungleich tiefer in die Grundrechte eingreifenden – Anordnung einer Wohnraumüberwachung nach § 100c StPO und damit sogar strenger als bei einer Überwachung von Inhalten einer Telekommunikation nach § 100a StPO, ist schwerlich nachzuvollziehen. Der Gesetzentwurf lässt eine Begründung für diese Beschränkung einer Erhebungsbefugnis nach § 100g StPO (RegE) vermissen, die dem Gesetzeszweck effektiver Verfolgung schwerer Straftaten zuwider läuft, innerhalb des Gefüges telekommunikationsbezogener Ermittlungsmaßnahmen systemwidrig erscheint und die auch nicht durch eine vom BVerfG vorgegebene Anforderung an ein verfassungsgemäßes

Gesetz geboten ist. In spezifischen Deliktsbereichen sind nach der geplanten Regelung Schutzlücken zu erwarten. So kommt Verkehrsdaten gerade bei der Aufklärung von nicht im Katalog enthaltenen Raubstraftaten (§ 249 Abs. 1 StGB) eine hohe Bedeutung zu (vgl. beispielhaft oben Fall I. 1 a) [1]). Deshalb erscheint hier und etwa auch hinsichtlich des Qualifikationstatbestands eines Verbrechens des bandenmäßigen und gewerbsmäßigen Betrugs (§ 263 Abs. 5 StGB) eine Anlehnung an den für die Überwachung von Telekommunikationsinhalten geltenden (weitergehenden) Straftatenkatalog nach § 100a Abs. 2 StPO sinnvoller.

5. Die sehr knapp bemessenen Speicherfristen insbesondere von nur vier Wochen für Standortdaten (§ 113b Abs. 1 Ziff.2 TKG RegE) dürften sich in der Rechtsanwendungspraxis als zu kurz erweisen, um dem Gesetzeszweck noch gerecht zu werden.

6. Zur Verbesserung des Schutzes der Persönlichkeitsrechte von Beschuldigten wäre es im Übrigen zu begrüßen, wenn das Gesetz bei der richterlichen Anordnung der Herausgabe von Verkehrsdaten – ebenso wie auch bei sämtlichen weiteren an die Provider gerichteten Anordnungen – die Übersendung von Kurzausfertigungen der richterlichen Beschlüsse für eine wirksame Abfrage der gespeicherten Verkehrsdaten ausreichen ließe. Hierdurch würden in der Rechtspraxis immer wieder – in Anmaßung eines scheinbaren Prüfungsrechts – artikulierte Zweifel der Provider an der Wirksamkeit einer richterlichen Anordnung einerseits vermieden[42] und andererseits – nicht zuletzt mit Blick auf die Unschuldsvermutung – dem Provider keine Kenntnis von der Art und Schwere der gegen den Beschuldigten erhobenen Tatvorwürfe gegeben.

[42] Vgl. MPI, aaO, S. 154.

DEUTSCHER RICHTERBUND
Bund der Richterinnen und Richter,
Staatsanwältinnen und Staatsanwälte

Stellungnahme

Nr. 12/15
Mai 2015

Stellungnahme des Deutschen Richterbundes zum Referentenentwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

Deutscher Richterbund
Kronenstraße 73
10117 Berlin

T +49 30 206 125-0
F +49 30 206 125-25

info@drb.de
www.drb.de

Verfasserin der Stellungnahme:
Sigrid Hegmann, Bundesanwältin beim BGH,
Mitglied des Präsidiums

A. Tenor der Stellungnahme

Die geplante Neuregelung der Verkehrsdatenerhebung durch § 100g Abs. 2 StPO-E in Verbindung mit § 113 b TGK-E bleibt noch hinter der bisherigen Rechtslage zurück und entspricht damit nicht den Bedürfnissen einer effektiven Strafverfolgung.

Die kurze Speicherfrist von zehn Wochen für Verkehrsdaten und vier Wochen für Standortdaten ist weder verfassungsrechtlich geboten noch ermittlungstechnisch ausreichend.

Auch der Katalog möglicher Straftaten, die einen Eingriff nach § 100g Abs. 2 StPO-E rechtfertigen, greift zu kurz. Als tauglicher Anknüpfungspunkt für die besondere Schwere einer Straftat bietet sich der Katalog des § 100a Abs. 2 StPO an.

Zudem ist es verfassungsrechtlich nicht geboten, die Verkehrsdaten von E-Mails sowie von Daten über aufgerufene Internetseiten bei der Verkehrsdatenerhebung wie vorgesehen auszuklammern.

B. Bewertung im Einzelnen

Der Deutsche Richterbund hat den Referentenentwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten zur Kenntnis genommen. Vor dem Hintergrund des Hinweises des Bundesministeriums der Justiz und für Verbraucherschutz auf die „große Eilbedürftigkeit", der in diesem Zusammenhang nicht erfolgten Verbändeanhörung – das Gesetz soll offenbar noch vor der Sommerpause verabschiedet werden (vgl. Sensburg/Ulrich DRiZ 2015, 172) – und der Komplexität der zu regelnden Materie wird im Folgenden nur auf einige wenige, besonders praxisrelevante Probleme und Kritikpunkte hinsichtlich der geplanten Neuregelung hingewiesen.

Nicht nachvollziehbar ist für den Deutschen Richterbund, warum trotz des vom Gesetzgeber festgestellten erheblichen Eingriffs in die Grundrechte der Betroffenen bei der Verkehrsdatenspeicherung das finanzielle Interesse der Dienstanbieter zur Abrechnung ihrer Leistungen eine Speicherung von Verkehrsdaten über eine Frist von 6 Monaten rechtfertigt (§ 97 Abs. 3 TKG), während die Verfolgung von erheblichen Straftaten, auch Verbrechen, einen generellen Zugriff auf solche Daten verbietet und eine Höchstspeicherfrist von nur 10 Wochen erzwingt. Die hier vorgenommene Abwägung zwischen Strafverfolgung im Allgemeininteresse und dem Abrechnungsinteresse der Dienstanbieter überzeugt nicht. Dies trifft auch auf die Vorgaben zur Speicherung zu. Während jene Daten, die für Strafverfolgungszwecke vorgehalten werden, dem strengen Regime des § 113b TKG n.F. unterworfen werden, gelten für die Speicherung von Verkehrsdaten zur Abrechnung weiterhin die allgemeinen datenschutzrechtlichen Vorgaben.

1. Straftatenkatalog des § 100g Abs. 2 StPO-E

Die Aufzählung der Straftaten, zu deren Ermittlung eine Erhebung von nach § 113b TKG-E verpflichtend gespeicherten Verkehrsdaten zulässig ist, erscheint einer strafrechtsdogmatischen Systematik nicht ohne Weiteres zugänglich. Im Gesetzentwurf selbst ist von einer „Teilmenge der im Katalog des § 100a Abs. 2 StPO enthaltenen Straftaten" die Rede. Tatsächlich fehlen aber die in § 100g Abs. 2 StPO-E aufgenommenen Straftatbestände der §§ 125a und § 184c Abs. 2 StGB in dem Katalog des § 100a Abs. 2 StPO. Aus nicht genannten Gründen wurden hingegen beispielsweise schwere Straftaten nach dem Außenwirtschaftsgesetz nicht in den neuen Katalog aufgenommen. Umgekehrt dürfte der Umstand, dass Verbrechen in aller Regel besonders schwere Straftaten darstellen, bei der Erstellung des Katalogs keine (ausschlaggebende) Rolle gespielt haben, denn einige der aufgenommenen Tatbestände, wie §§ 89a, 184b Abs. 2, 184c Abs. 2 StGB, stel-

len keine Verbrechenstatbestände dar. Es drängt sich der Eindruck auf, dass sich der Katalog mehr an gefühlten, in der veröffentlichten Meinung als schwer empfundenen Straftaten orientiert als an strafrechtssystematisch nachvollziehbaren Kriterien.
Aus Sicht der Praxis ist insbesondere auf folgenden Umstand hinzuweisen: Verkehrsdaten sind als Ermittlungsansatz vor allem zu Beginn eines Ermittlungsverfahrens von großer Bedeutung. Zu diesem Zeitpunkt beziehen sich Verdachtslagen allerdings in der Regel auf die grundsätzlich nicht im Katalog des § 100g Abs. 2 StPO-E aufgeführten Grundtatbestände. Erfahrungsgemäß stellt sich erst im Laufe des Ermittlungsverfahrens und nach umfassender Würdigung von Tat und Täter heraus, dass auch ein besonders schwerer Fall in Betracht kommen kann. In vielen Fällen schwerer und schwerster Kriminalität wird daher auch künftig die Speicherung von Verkehrsdaten nicht zulässig sein, wenn man nicht von den Ermittlungsbehörden bereits zu Beginn des Verfahrens hellseherische Fähigkeiten hinsichtlich der Bejahung eines besonders schweren Falls verlangen will.

Auffallend ist, dass im Katalog des § 100g Abs. 2 StPO-E „Computerstraftaten“, vom § 263a über §§ 202a, b, 303a, b sowie auch der neue § 202d StGB-E, aber auch § 17 UWG, konsequent ausgenommen werden. Gerade für die Ermittlung dieser Straftaten ist die Zuordnung von Verkehrsdaten als einer der ersten Ermittlungsschritte von erheblicher Bedeutung. Mit dem nun vorgelegten Gesetzentwurf macht der Gesetzgeber deutlich, dass eine erfolgreiche Strafverfolgung von Computerstraftaten und Betriebsspionage nicht angestrebt wird.

Als geeigneter und verfassungsrechtlich unbedenklicher Anknüpfungspunkt für die einen Eingriff nach § 100g StPO rechtfertigende Schwere der Straftat bietet sich der Katalog des § 100a Abs. 2 StPO an. Dieser ist verfassungsgemäß (BVerfG Beschl. v. 12.10.2011 (2 BvR 236/08, Rn. 200 ff. - juris) und hat sich bewährt. Auch soweit die dort enthaltenen Straftaten eine Höchstfreiheitsstrafe von (nur) fünf Jahren vorsehen, sind sie in Anbetracht der jeweils geschützten Rechtsgüter – Schutz der Funktionsfähigkeit des Staates oder seiner Einrichtungen besonders schützenswerte Rechtsgüter Privater – als schwer zu klassifizieren. Das Bundesverfassungsgericht hat in der Entscheidung vom 02.03.2010 nicht gefordert, an die Erhebung von Verkehrsdaten höhere Anforderungen zu stellen als an die Erhebung von Inhaltsdaten, die im Hinblick auf Umfang und Intensität des Eingriffs in das Fernmeldegeheimnis erheblich schwerer wiegt.

2. Art der zu erhebenden Daten

Die besondere Bedeutung der Telekommunikation in der heutigen Welt bringt ein erhebliches spezifisches Gefahrenpotenzial mit sich. Die neuen Telekommunikationsmittel überwinden Zeit und Raum in einer früher nicht gekannten Weise und mit vielen Möglichkeiten der Verschleierung und Tarnung. Darauf hat das Bundesverfassungsgericht zu Recht eindringlich hingewiesen (BVerfG Urt. v. 02.03.2010 – 1 BvR 256/08 Rn. 216 – juris): „Durch die praktisch widerstandsfreie Kommunikation wird eine Bündelung von Wissen, Handlungsbereitschaft und krimineller Energie möglich, die die Gefahrenabwehr und Strafverfolgung vor neuartige Aufgaben stellt. Manche Straftaten erfolgen unmittelbar mit Hilfe der neuen Technik. Eingebunden in ein Konglomerat von nurmehr technisch miteinander kommunizierenden Rechnern und Rechnernetzen entziehen sich solche Aktivitäten weithin der Beobachtung. Zugleich können sie – etwa durch Angriffe auf die Telekommunikation Dritter – auch neuartige Gefahren begründen. Eine Rekonstruktion gerade der Telekommunikationsverbindungen ist daher für eine effektive Strafverfolgung und Gefahrenabwehr von besonderer Bedeutung."

Dies gilt für die Daten von Diensten der elektronischen Post in gleicher Weise wie für die in § 113b Abs. 1 bis 3 TKG-E genannten Daten. Die Nichtaufnahme von Verkehrsdaten von E-Mails sowie von Daten über aufgerufene Internetseiten in die Liste der zu speichernden Daten (§ 113b Abs. 5 TKG-E) erscheint damit auch angesichts des Verschwimmens der Grenzen zwischen den jeweiligen Kommunikationsformen im Internet – soziale Medien, Messenger-Dienste, Chatforen, Weblogs, Online-Rollenspiele – anachronistisch und ist vor diesem Hintergrund jedenfalls nicht mit der Erklärung nachvollziehbar, den Anforderungen des Bundesverfassungsgerichts im Urteil vom 02.03.2010 (1 BvR 256/08 u.a.) entsprechen zu wollen. Denn dort wird nicht zwischen Verkehrsdaten von Diensten der elektronischen Post und anderen Verkehrsdaten der Telekommunikation unterschieden. Die Verkehrsdaten von E-Mails oder Daten von aufgerufenen Internetseiten sind nicht höherrangig oder schützenswerter als die weiteren in § 113b TKG-E genannten Daten und können ebenfalls wichtige Ermittlungsansätze bieten.

3. Speicherfristen

Die kurze Speicherfrist von zehn Wochen für Verkehrs- und vier Wochen für Standortdaten ist weder verfassungsrechtlich geboten noch ermittlungstechnisch ausreichend. Möglicherweise entspringt sie vielmehr reinen rechtspolitischen Ängsten. Die Differenzierung zwischen Verkehrs- und Standortdaten ist nicht nachvollziehbar, zumal angesichts der Vielzahl von beliebten und erfolgreichen Applikationen auf Mobiltelefonen, die auf

Standortdaten zugreifen und diese zu geschäftlichen Zwecken speichern, nicht von einer erhöhten Sensibilität oder gar einem Gefühl des Bedrohtseins seitens der Nutzer auszugehen ist. Auch das Bundesverfassungsgericht hat eine längere – sechsmonatige – anlasslose Speicherung von Telekommunikationsdaten für qualifizierte Verwendungen im Rahmen der Strafverfolgung wie auch der Gefahrenabwehr nicht für mit Art. 10 GG schlechthin unvereinbar gehalten (BVerfG Urt. v. 02.03.2010 – 1 BvR 256/08, Rn. 205 ff. – juris). Der Gerichtshof der Europäischen Union hat in seinem Urteil vom 08.04.2014 (C-293/12 u.a.) die Richtlinie 2006/24/EG aus anderen Gründen, nicht wegen der dort vorgesehenen Mindestspeicherfrist von sechs Monaten für ungültig erklärt.

4. Richtervorbehalt

Der strenge Richtervorbehalt des § 101a Abs. 1 S. 2 StPO-E für die Fälle des § 100g Abs. 2 StPO-E ohne Möglichkeit einer staatsanwaltschaftlichen Eilkompetenz nach § 100b Abs. 1 S. 2 StPO wird voraussichtlich die Ermittlungen eher erschweren als erleichtern, da die Sicherung von Verkehrsdaten in der Regel am Anfang eines Ermittlungsverfahrens steht, in dem erfahrungsgemäß Eile geboten ist. Die Staatsanwaltschaft ist Teil der Rechtspflege und unterliegt als Anordnungsbehörde in gleicher Weise wie die Gerichte strenger Gesetzesbindung, sodass ein nachvollziehbarer Grund für die Nichteinräumung einer staatsanwaltschaftlichen Eilkompetenz mit nachfolgender richterlicher Bestätigungspflicht nicht erkennbar ist.

Die erhöhten Begründungsanforderungen in § 101a Abs. 2 StPO-E sind der Vorschrift des § 100d Abs. 3 StPO zur Begründung der (einen ungleich schwereren Eingriff darstellenden) Wohnraumüberwachung entlehnt. Die der qualifizierten Begründungspflicht zugrundeliegende Vorstellung des Referentenentwurfs, damit „überflüssige Bewegungsprofile“ zu vermeiden (S. 38 RefE), offenbart ein unbegründetes Misstrauen gegenüber den Gerichten und unterstellt ohne jede Tatsachengrundlage für die Vergangenheit zu Unrecht überflüssige und damit unverhältnismäßige Anordnungen durch Gerichte.
Jede richterliche Entscheidung im Ermittlungsverfahren ist zu begründen, § 34 StPO. Eine Erklärung für die Forderung nach einer vertieften Begründungspflicht, wie sie sonst nur für den schweren, an Intensität mit den hier in Rede stehenden Maßnahmen nicht zu vergleichenden Eingriff nach § 100c StPO (§ 100d Abs. 3 StPO) gilt, bleibt der Referentenentwurf schuldig.

5. Benachrichtigungspflichten

Die Ausgestaltung der Verkehrsdatenerhebung als grundsätzlich offene Maßnahme gegenüber dem Betroffenen ist praxisfremd, entspricht indes den Transparenzanforderungen des Bundesverfassungsgerichts (Urt. v. 02.03.2010 – 1 BvR 256/08 Rn. 243ff. – juris). Von der vorherigen Anhörung kann nach Maßgabe des § 33 Abs. 4 StPO abgesehen werden. Der Gesetzentwurf sieht in § 101a Abs. 4 StPO-E eine (weitere) Benachrichtigung nach Erlass, aber vor der Umsetzung der Maßnahme vor, die nur ausnahmsweise unterbleiben darf (§ 101a Abs. 4 S. 2 StPO-E). Würde dieser Entwurf Gesetz, wären also grundsätzlich Betroffene zu Beginn eines Ermittlungsverfahrens darüber zu informieren, dass und wegen welcher Straftat nunmehr gegen sie ermittelt wird. Weiteren erfolgreichen nichtoffenen Ermittlungsmaßnahmen, die sich regelmäßig an die Auswertung der Telekommunikationsdaten anschließen, wäre damit jeglicher Boden entzogen.
Soll eine Benachrichtigung bei entgegenstehenden schutzwürdigen Belangen einer betroffenen Person unterbleiben, bedarf dies nach dem Entwurf einer richterlichen Anordnung; gleiches gilt im Fall der erstmaligen Zurückstellung einer Benachrichtigung bei Gefährdung des Untersuchungszwecks, des Lebens, der körperlichen Unversehrtheit und der persönlichen Freiheit einer Person und von bedeutenden Vermögenswerten (§ 101 Abs. 5 StPO). Die Benachrichtigungspflichten gehen damit weiter als die Regelungen über Zurückstellung und Unterbleiben der Benachrichtigung, die für die verdeckten Ermittlungsmaßnahmen nach §§ 98a, 99, 100a ff. StPO gelten und in § 101 Abs. 4 bis 7 StPO geregelt sind. Zu begrüßen ist die Empfehlung des Entwurfs, bereits mit dem Antrag auf Anordnung einer Verkehrsdatenerhebung zugleich die gerichtliche Zustimmung zur Zurückstellung der Benachrichtigung zu beantragen (S. 39 RefE). Ein Bedürfnis für diese strenge Benachrichtigungsregelung besteht indessen nicht.

6. Kennzeichnungspflichten

Die Pflicht zur Aufrechterhaltung der Kennzeichnung in § 101a Abs. 3 S. 3 StPO-E entspricht § 101 Abs. 3 S. 2 StPO. Vor dem Hintergrund, dass die Erhebung von Verkehrsdaten in aller Regel am Anfang eines Ermittlungsverfahrens steht und Verkehrsdaten häufig den einzigen Ermittlungsansatz darstellen, ist aus praktischer Sicht der weitere Umgang mit den so gekennzeichneten Daten zu bedenken. Werden Erkenntnisse aus verdeckt erhobenen Maßnahmen in denselben Ermittlungsakten inhaltlich wiedergegeben oder auf sie Bezug genommen, etwa in Auswertungsvermerken, Zwischen- und Schlussberichten, in der Anklageschrift oder im Urteil, ist eine erneute Kennzeichnung nicht erforderlich. Denn der Verwendungsbeschränkung des

§ 477 Abs. 2 StPO wird dadurch genügt, dass nur Primärschriftstücke zu Beweiszwecken verwendet werden können.

7. Datenhehlerei, § 202d StGB-E

Der Deutsche Richterbund begrüßt die Einführung eines neuen Straftatbestandes der Datenhehlerei, der bestehende Lücken beim Schutz von informationstechnischen Systemen und der in ihnen gespeicherten Daten schließen soll. Das formelle Datengeheimnis kann auf diese Weise wirksamer vor weiteren Verletzungen bei rechtswidrigen Vortaten geschützt werden.

Allerdings führt die nunmehr vorgelegte Fassung im Regelfall weiterhin zur Straffreiheit. Es wird üblicherweise kaum nachzuweisen sein, dass die Daten, die angeboten werden, aus einer Straftat herrühren. Ausspähen von Daten setzt z.B. in Deutschland das Überwinden einer Zugangssicherung, § 202a StGB, voraus. Dies ist z.B. beim Skimming nicht der Fall. Die ausgelesenen Kontendaten befinden sich auf einem ungesicherten Magnetstreifen der EC-Karte, die durch die Täter über ein handelsübliches Kartenlesegerät ohne Überwindung einer Zugangssicherung ausgelesen werden. Hinzu kommt die optische Erfassung der PIN, die über eine Videokamera erfolgt. Auch hier liegt kein Ausspähen von Daten vor. Die Weitergabe dieser Daten an Dritte, die von diesen zusammengeführt zur unberechtigten Abhebung genutzt werden können, wäre daher auch weiterhin nicht als Datenhehlerei strafbar. Auch das Ausspähen von Kreditkartendaten kann, weltweit begangen, unter Voraussetzungen erfolgen, welche keinen deutschen Straftatbestand verletzen.

Der Deutsche Richterbund ist mit rund 15.500 Mitgliedern in 25 Landes- und Fachverbänden (bei bundesweit 25.000 Richtern und Staatsanwälten insgesamt) der mit Abstand größte Berufsverband der Richterinnen und Richter, Staatsanwältinnen und Staatsanwälte in Deutschland.

Rainer Franosch
Oberstaatsanwalt

Marburg, den 15. September 2015

Hessische Zentralstelle zur Bekämpfung der Internetkriminalität
(z. Zt. abgeordnet an das Hessische Ministerium der Justiz)

Betr.: Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages

Anhörung zu dem
a) Gesetzentwurf der Fraktionen der CDU/CSU und SPD
Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten
BT-Drucksache 18/5088

b) Gesetzentwurf der Bundesregierung
Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten
BT-Drucksache 18/5171

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

Zur Vorbereitung der Anhörung gebe ich die nachfolgende Stellungnahme ab, die sich vor allem auf den Phänomenbereich Cybercrime bezieht.

1) Notwendigkeit der Vorratsdatenspeicherung (VDS) für die effektive Bekämpfung von Cybercrime (zu BT-Drucksache 18/4971)

a) Die Bedrohung

Als „Cybercrime" (früher „Informations- und Kommunikationskriminalität" oder auch verkürzend „Internetkriminalität") bezeichnet man alle kriminellen Handlungen, die

- gegen elektronische Kommunikationsnetze und Informationssysteme (Cybercrime im engeren Sinn, englisch: „cyber-dependent crimes", z.B. Datenveränderung, § 303a StGB, Ausspähen von Daten, § 202a StGB etc.) oder
- mittels derartiger Netze und Systeme verübt werden (Cybercrime im weiteren Sinn, englisch: „cyber-enabled crimes", also Taten, bei denen das Internet als virtuelles Tatwerkzeug für die Begehung von Straftaten genutzt wird, z.B. Verbreitung von Kinderpornografie, Volksverhetzung, Verbreitung extremistischer

Propaganda, öffentliche Aufforderung zu Straftaten, betrügerisches Anbieten von Waren und Dienstleistungen oder Geldanlagen, verbotenes Glücksspiel, unlautere Werbung, Urheberrechtsverletzungen, Verkauf von Waffen, Betäubungsmitteln oder verbotenen Medikamenten)[1]

Auch wenn die meisten Internet-Straftaten Betrugsdelikte sind (Anteil in der PKS 2014: 74,2 Prozent[2]), darf die gesamtgesellschaftliche Bedrohungslage durch Cybercrime aus mehreren Gründen nicht unterschätzt werden.

Zunächst ist festzuhalten, dass jeder – nicht nur die Internetnutzer – Opfer von Cybercrime werden kann, sei es der einzelne Bürger, Unternehmen oder auch staatliche Stellen.
Mit der Zunahme der Bedeutung der IT als Bestandteil des Alltags der Bürger steigen die Manipulations- und Angriffsmöglichkeiten auf Seiten der Cyberkriminellen. Cyberkriminelle handeln global, nationale Grenzen spielen keine Rolle, wobei Handlungs-, Taterfolgs- und Aufenthaltsorte von Tätern und Opfern irrelevant sind.

Das Internet bringt alles und alle zusammen. Bucht ein Bürger in Frankfurt am Main eine Urlaubsreise über Internet, hat der am anderen Ende der Welt wartende Straftäter in Echtzeit potentiellen Zugriff auf den für die Buchung genutzten Computer. Aber auch diejenigen, die ihre Urlaubsreise nicht selbst über Internet buchen, können Opfer von Cybercrime werden, z.B. dadurch, dass die Täter sich Zugriff auf die persönlichen Daten durch einen Angriff auf die Server des Reisevermittlers verschaffen.

Das bedeutet kurz gefasst, dass durch das Internet erstmals in der Geschichte der Kriminalität Straftaten

- weltweit und
- unter Überwindung jeder räumlichen Distanz zwischen Täter und Opfer in Echtzeit

begangen werden können.

Der im Januar 2014 bekannt gewordene Diebstahl von 16 Millionen E-Mail-Adressen belegt beispielhaft die Schadensdimensionen im Phänomenbereich Cybercrime. Der Diebstahl digitaler Identitäten, also der Diebstahl von Daten, ist ein Massenphänomen.

Die digitale Identität ist die Summe aller Möglichkeiten und Rechte des einzelnen Nutzers sowie seiner Aktivitäten innerhalb der Gesamtstruktur des Internets. Konkret handelt es sich um alle Arten von Nutzer-Accounts, also zum Beispiel Zugangsdaten in den Bereichen Kommunikation (E-Mail- und Messengerdienste), E-Commerce (Onlinebanking, internetgestützte Vertriebsportale aller Art), berufsspezifische Informationen (z. B. Nutzung eines Homeoffice für den Zugriff auf firmeninterne technische Ressourcen) und E-Government (z.B. elektronische Steuererklärung oder elektronische Bußgeldakte).

---

[1] vgl BKA, Bundeslagebild Cybercrime 2013, S. 5; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:DE:PDF

[2] Es ist allgemein bekannt, dass die Dunkelfeldproblematik bei Cybercrime besonders ausgeprägt ist, vgl. z.B. http://www.heise.de/newsticker/meldung/Cybercrime-Das-Dunkelfeld-wird-groesser-2303524.html; BKA, Bundeslagebild Cybercrime 2013, S. 10 m.w.N.

Darüber hinaus sind auch alle anderen zahlungsrelevanten Informationen (insbesondere Kreditkartendaten einschließlich der Zahlungsadressen sowie weiterer Informationen) Bestandteil der digitalen Identität. Die Täter nutzen Schadprogramme, um Eingaben des Computernutzers auszuspähen sowie Anmeldedaten zu erlangen und Transaktionen durchführen zu können; sie gehen dabei häufig arbeitsteilig und unter Nutzung professioneller Strukturen vor. Anschließend werden die Daten entweder von den Tätern selbst eingesetzt oder aber an Dritte weiterveräußert, welche die Daten dann kriminell einsetzen.

Legt man die Ergebnisse einer Online-Umfage aus dem Jahr 2013 zugrunde, wurde schon rund ein Fünftel der Deutschen (21 Prozent) Opfer von Identitätsdiebstahl oder -missbrauch, weitere 27 Prozent können nicht ausschließen, dass ihre personenbezogenen Daten schon missbraucht wurden[3]. Diese Zahlen gehen weit über die polizeilich registrierten Fälle des Ausspähens/Abfangens von Daten hinaus und sind ein Beleg für das hohe Dunkelfeld im Bereich Cybercrime.

Aber das Internet bietet für die Täter noch weit mehr: Immer mehr verlagert sich der Handel mit illegalen Waren und Dienstleistungen in das Internet.
Unter Nutzung der Informationstechnologie und digitaler Währungen gebrauchen Cyberkriminelle das sogenannte „Darknet", jenen Teil des Internets, der nicht über normale Suchmaschinen auffindbar ist und der als versteckter Dienst z.B. im TOR-Netzwerk die Anonymität der Nutzer durch Verschleierung der Verkehrsdaten wahrt oder ein „anonymes" Hosting ermöglicht. Über solche Online-Plattformen werden hier beispielsweise der illegale Handel mit Drogen, Waffen und Kreditkartendaten betrieben oder illegale Dienstleistungen, wie z.B. die Durchführung von DDoS-Attacken, angeboten.

Diese arbeitsteilige Cyberunterwelt wird zu Recht als „Underground Economy" bezeichnet. Täter kaufen und verkaufen illegale Waren und Dienstleistungen, finden sich zu international agierenden Banden zusammen, ohne sich ein einziges Mal im wahren Leben getroffen zu haben. Es existiert ein funktionierender globaler Markt, auf dem Angriffswerkzeuge, Erkenntnisse über Schwachstellen in Betriebssystemen oder Schadsoftware eingekauft oder als Dienstleistung in Auftrag gegeben werden können („Crime-as-a-Service").

Die nahezu unbegrenzten Möglichkeiten von Cybercrime führen dazu, dass sich auch die organisierte Kriminalität zunehmend dieses Bereiches annimmt.[4]

Naturgemäß sind derartige, allgemeine Beschreibungen von Kriminalitätsphänomenen blass und wenig eindrücklich.

Daher nachfolgend einige Beispiele:

---

[3] Online-Umfrage der SCHUFA Holding AG und des Marktforschungsinstituts Innofact AG, http://www.presseportal.de/pm/25316/2556036
[4] Europol, Internet Organised Crime Threat Assessment (iOCTA) 2014, S. 9

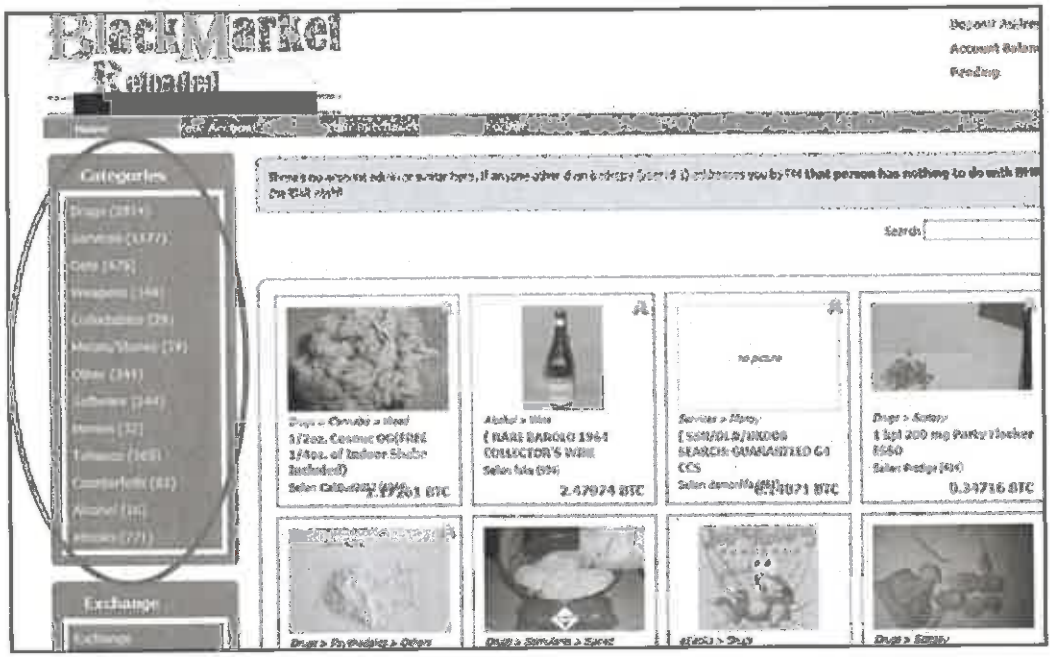


Abb. 1

Abbildung 1 zeigt die Startseite eines Marktplatzes im Darknet. Angeboten werden u.a:

- Drogen (Abb. 2 und 3)
- Dienstleistungen (illegaler Art)
- Daten (ausgespähte)
- Waffen (Abb. 4 und 5)
- Kinderpornographie
- gefälschte Dokumente und Falschgeld

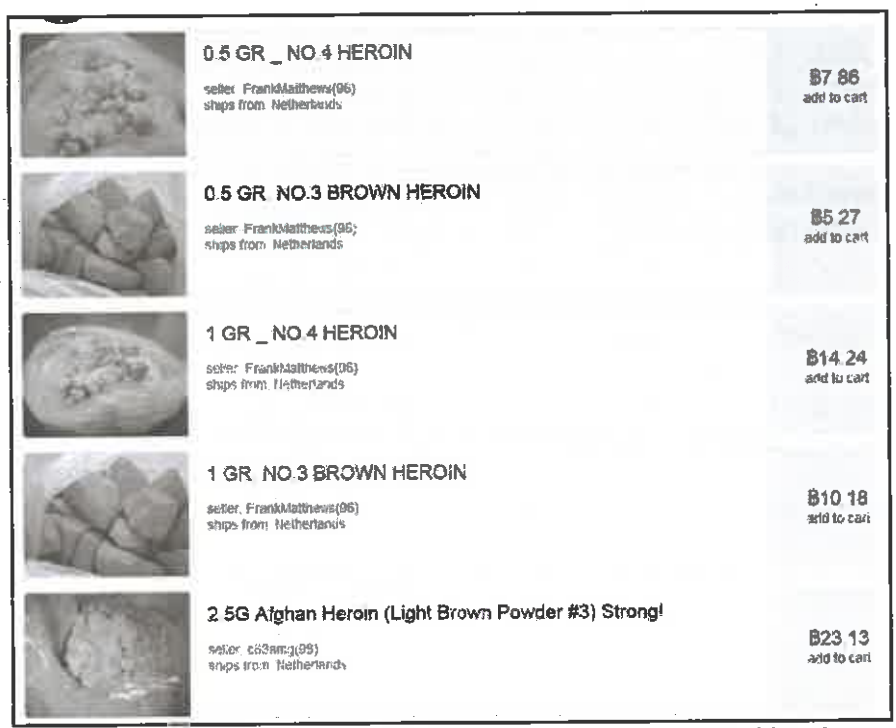


Abb. 2: Im Internet sind alle Drogen erhältlich, auch Heroin.

Abb. 3: Ware eines Online-Dealers von nur einem Tag (rd. 4,5 kg Cannabis und 0,5 kg Haschisch), beschlagnahmt in einer Packstation, adressiert an verschiedene Abnehmer aus ganz Deutschland.

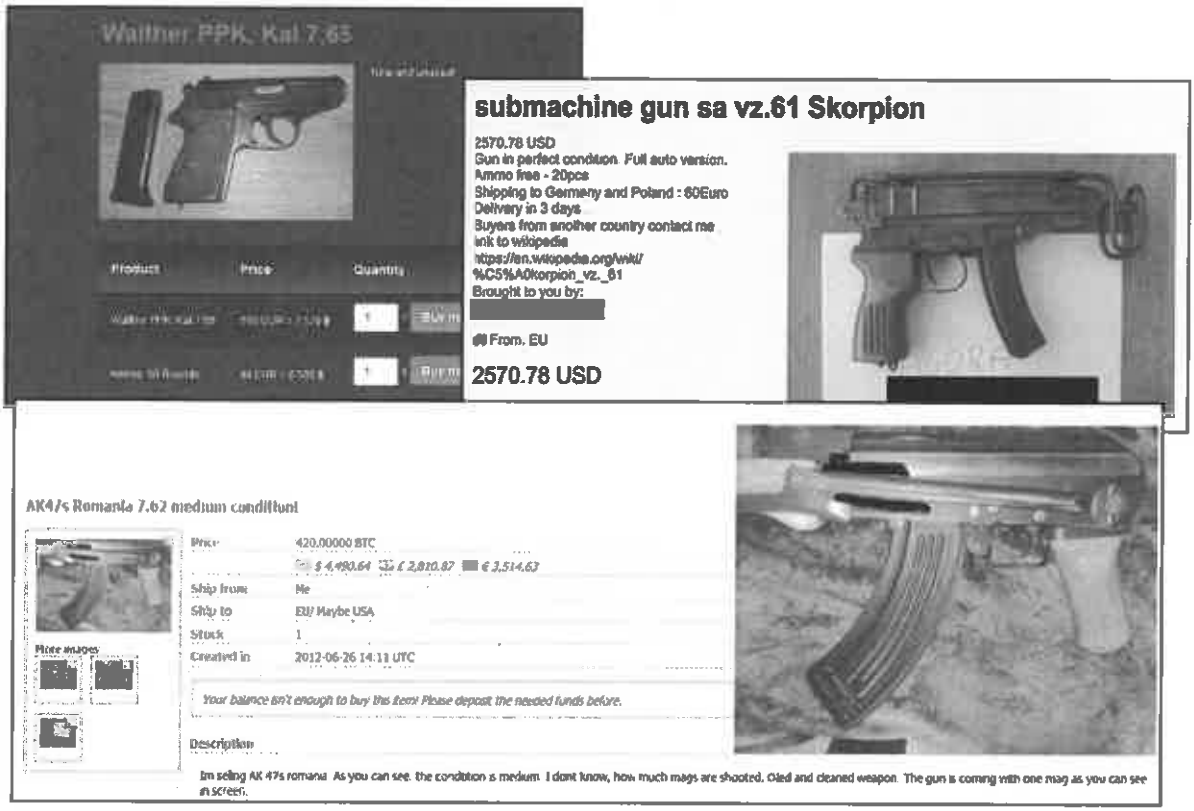


Abb. 4: Das Angebot an Waffen im Darknet ist unbegrenzt, einschließlich Kriegswaffen.

Abb. 5: Diese Pistole mit Schalldämpfer wurde in einem hessischen Ermittlungsverfahren bei einem Darknet-Verkäufer beschlagnahmt.

Neben Waren werden auch Dienstleistungen angeboten, darunter auch die Begehung von Tötungsdelikten gegen Entgelt:

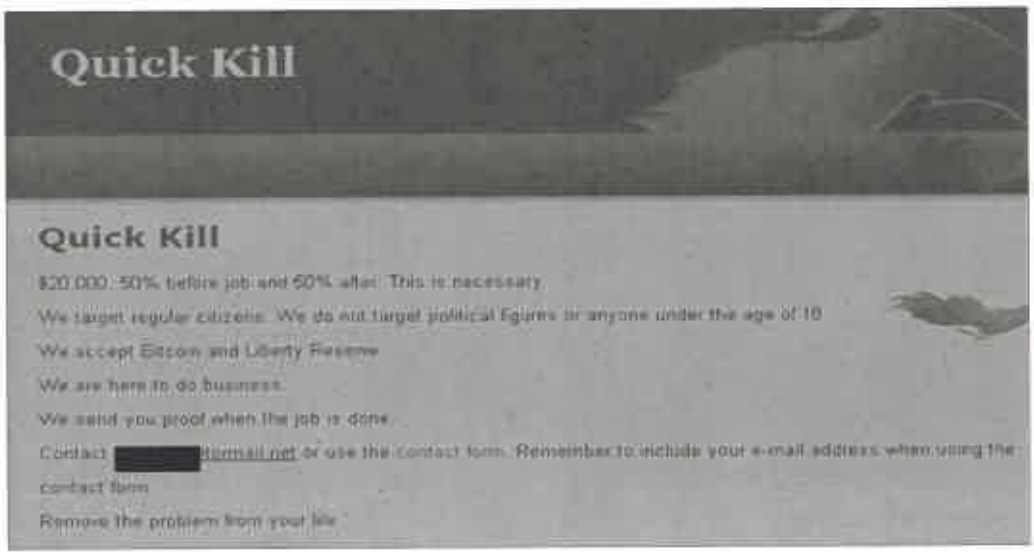


Abb.6

Dass Auftragsmorde über das Internet verabredet werden, ist aus US-amerikanischen Ermittlungsverfahren bereits bekannt[5].

Auch in Hessen hat es bereits einen derartigen Fall gegeben:

Im Frühjahr 2014 kam der Angeschuldigte A via Internet über das „Darknet" in Kontakt mit dem Mitangeschuldigten B. B. war im Forum http://germanyXXX.onion schon seit längerem auf der Suche nach Arbeit und bot gegen lukrative Bezahlung die Erledigung von Diensten aller Art an:

[5] z.B. http://www.bloomberg.com/news/articles/2014-12-09/us-says-silk-roads-ulbricht-solicited-six-murders-for-hire

„Fast egal was! Transporter, Mafia, Hitman"

Der Angeschuldigte A beauftragte B über Internet, gegen Entgelt für ihn den C zu töten, da dieser seit Mitte März 2014 der neue Lebensgefährte seines Ex-Freundes D war. Die Trennung von D hatte der von massiver Eifersucht sowie Missgunst geplagte A nicht verwunden. Für den geplanten Mord erhielt B eine Anzahlung in Höhe von 3.000,00 €, zusätzliche 10.000.- € waren als „Erfolgshonorar" vereinbart worden. B suchte sodann das Opfer C auf und versuchte, ihm mit einem Messer mit 20 cm langer Klinge die Kehle durchzuschneiden. C konnte mit Hilfe von Zeugen den Angriff abwehren und überlebte mit erheblichen Schnittverletzungen im Hals-, Gesichts- und Schulterbereich sowie an den Händen.

Auszug aus einer E-Mail des Auftragsmörders B an den Auftraggeber A:

> Du willst wissen wie Skrupellos ich bin, ich kann z.b. mit einem Grinsen im Gesicht jemandem ein Messer in den Hals stecken. Wie gesagt ich habe mit meinem Leben abgeschlossen, schon vor Jahren.
>
> Und ich weise nochmals darauf hin das ich kein abgefuckter Gesetzesdiener bin, zu gern würde ich sie jagen und auslöschen.

Abb. 7

Ohne die Möglichkeit, anonym über das Darknet nach einem Auftragsmörder zu suchen, wäre es dem in kriminellen Dingen völlig unerfahrenen A nicht gelungen, die Verbindung zu einer tatgeneigten Person aufzunehmen.

- Kinderpornographie

Der sexuelle Missbrauch von Kindern wird durch das Internet ebenfalls massiv gefördert. Dies betrifft nicht nur die Kinderpornographie, die nahezu ausschließlich netzbasiert unentgeltlich im Tausch, aber auch entgeltlich über professionelle Webseiten vertrieben wird, sondern auch die internetgestützte Verabredung von Tätern zu Treffen, um gemeinsam Kinder zu missbrauchen. Auch der Missbrauch von Kindern durch Erwachsene vor der Webcam ist ein zunehmendes Phänomen.

Es ist festzustellen, dass sich im Internet organisierte pädokriminelle Strukturen neuer Qualität herausgebildet haben. In umfangreichen Ermittlungen in diesem Phänomenbereich seit 2009 konnte nicht nur festgestellt werden, dass es festgefügte, abgeschottete und hierarchisch aufgebaute geschlossene Benutzerkreise zum Austausch von Kinderpornographie gibt, sondern auch exklusive Bereiche, in denen der reale sexuelle Missbrauch von Kindern und die Weitergabe des so selbst produzierten Materials als Zugangsvoraussetzung dienen. Das Motto eines Bereiches in einem Pädophilen-Forum lautete:

„Don't ask for membership if you haven't got your own daughter to share".

In dem Umfangsverfahren „Geisterwald" konnten weltweit insgesamt über 160 Personen als Mitglieder solcher geschlossener Strukturen identifiziert werden. Rund 30% dieser Personen haben nicht lediglich Kinderpornographie konsumiert und weiterverbreitet, sondern selbst Kinder missbraucht. Das Verfahren war ein Erfolg, weil

zum Zeitpunkt des Beginns der Ermittlungen im Jahr 2009 die Regelung zur Vorratsdatenspeicherung noch in Kraft war.

Schließlich ist noch das sog. „Cybergrooming" zu nennen, also die internetbasierte Kontaktaufnahme von pädophilen Erwachsenen zu Kindern, um diese zu sexuellen Handlungen entweder an sich selbst vor einer Webcam oder zu Realtreffen zum Zwecke des Missbrauch zu bringen. In einem hessischen Ermittlungsverfahren mit dem Einsatz nicht offen ermittelnder Polizeibeamter, die als vermeintliche Kinder auftraten, nahmen innerhalb von nur acht Tagen 395 Personen mit den als Kindern auftretenden Polizeibeamten Kontakt auf und wirkten im Sinne von § 176 Abs. 4 Nr. 3 StGB auf diese ein.

Im Zusammenhang mit sexueller Gewalt gegen Kinder dient das Internet indes nicht nur als Transportmedium für die inkriminierten Bilder und Filme. In einschlägigen Foren und Chatrooms finden Pädophile darüber hinaus Gleichgesinnte, mit denen sie sich austauschen können. Es ist zu beobachten, dass im Rahmen derartiger Kommunikationsgruppen eine Radikalisierung stattfindet. Teilnehmer, die noch Skrupel haben, Kinder zu missbrauchen, werden ermuntert, diese fallen zu lassen (siehe Bildunterschrift unter Abb. 8).
Die wechselseitige Stimulierung und Befeuerung der sexuellen Fantasien in Internetforen ist eine der Ursachen für die zunehmende Brutalisierung des durch Kindesmissbrauch entstehenden Bild- und Filmmaterials. Abbildungen des Missbrauchs von Säuglingen und Kleinkindern oder sadistischer Gewalthandlungen an Kindern waren noch vor 10 Jahren selten, heute findet man sie auf sehr vielen der sichergestellten Täterrechner (Abb. 8, 9):

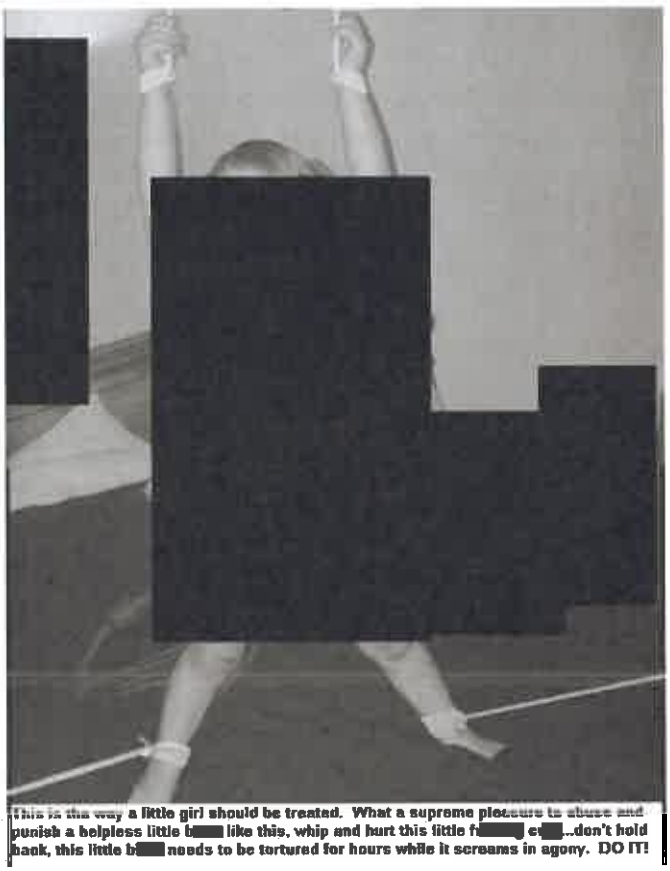


Abb. 8

Abb. 9

- Terrorismus

Auch für den politisch oder religiös motivierten Terrorismus ist das Internet von unschätzbarer Bedeutung. Es dient wie kein anderes Medium der weltweiten Kommunikation und Planung von Anschlägen, aber vor allem auch der Rekrutierung des Nachwuchses. Die Verbreitung von Propaganda über das Internet ist ein wesentliches Mittel zur Nachwuchsgewinnung und zur Einschüchterung des Gegners.

Ferner machen sich Terroristen die Verwundbarkeit kritischer Infrastrukturen infolge ihrer Anbindung an das Internet zunutze. Dies belegt beispielsweise die Attacke auf den französischen Sender TV5. Bei dem Angriff auf TV5 hatten Cyber-Dschihadisten Anfang April den Fernsehsender lahmgelegt. Auch die Social-Media-Auftritte des Senders brachten sie unter ihre Kontrolle und verbreiteten Propaganda. Die Terroristen begründeten ihren Angriff mit der Beteiligung Frankreichs an Luftschlägen gegen den Islamischen Staat (IS) im Irak[6].

Erfolgreiche Cyber-Angriffe auf Unternehmen, Verwaltungen und Privatnutzer bedürfen jedoch keineswegs der nahezu unbegrenzten Ressourcen fremder Nachrichtendienste oder großer Terrornetzwerke. Dies spiegelt sich in der Masse der heutigen Cyber-Angriffe wider. Für erfolgreiche Cyberattacken braucht man derzeit vielfach nicht mehr als einen PC und einen Internetanschluss, da in der Underground Economy sog. Botnetze, also der Zugriff auf tausende infizierte Opferrechner, angekauft oder angemietet werden kann.

Zusammenfassend ist festzuhalten, dass Cybercrime rasant zunimmt, die Schwere der Taten eine erhebliche Steigerung erfährt und somit den einzelnen Bürger und die Gesellschaft nicht nur virtuell oder finanziell, sondern auch an Leib und Leben bedroht.

b) Bedeutung der Vorratsdatenspeicherung für die Verfolgung von Cybercrime

Bei Straftaten, die mittels Internet begangen werden, stellt die IP-Adresse des Täters regelmäßig den einzigen, immer aber den ersten, effizientesten und schnellsten Ermittlungsansatz dar.

Ohne die Zuordnung der IP-Adresse zu einem Anschlussinhaber laufen die Ermittlungen weitgehend ins Leere, weil keine anderen Spuren vorhanden sind.

Dabei dient die Zuordnung der IP-Adresse zu einem Anschlussinhaber in der überwiegenden Mehrzahl der Fälle von Cybercrime letztendlich nicht der Beweisführung in der Hauptverhandlung, wie z.B. die Standortdaten eines Mobiltelefons im gerichtlichen Verfahren die Anwesenheit eines Täter am Tatort beweisen können, sondern – viel elementarer – zunächst der Identifizierung des Anschlussinhabers und der Ermöglichung weiterer Ermittlungen wie z.B. Durchsuchungsmaßnahmen zur Feststellung des eigentlichen Täters.

[6] Inzwischen gibt es Medienberichte, die mutmaßen, dass der Angriff andere Urheber hatte.

Die Erhebung eines IP-Adressinhabers steht mithin grundsätzlich am Anfang der Ermittlungen. Solange eine IP-Adresse nicht zugeordnet werden kann, werden Verfahren entweder zunächst meist gegen Unbekannt geführt oder gar nicht erst eingeleitet.
Schlägt schon der erste Ermittlungsschritt - die Zuordnung einer dynamischen IP-Adresse zum Anschlussinhaber – fehl, müssen die Verfahren regelmäßig eingestellt werden.

Beispiele:

aa) Operation „Hünstein"
Dieses Verfahren ist ein klassisches Kinderpornographieverfahren von verhältnismäßig kleinem Umfang. Die Ermittlungen richteten sich zunächst gegen einen 30-jährigen Kinderpornographiekonsumenten aus Hessen wegen des Verdachts der Verbreitung und des Besitzes von kinderpornographischen Bildern und Videos. Nach der Durchsuchung wurde der Computer des Beschuldigten ausgewertet und dabei eine E-Mail-Datenbank mit über 200 Tauschkontakten aufgefunden. Die Bestandsdaten der Täter bei den E-Mail-Anbietern waren durchweg fiktiv. Aufgrund fehlender Vorratsdatenspeicherung konnten lediglich neun Täter ermittelt werden, da außer den IP-Adressen der letzten E-Mail-Nutzung keine weiteren Spuren vorhanden waren.

bb) Operation „Downfall"
Dieses internationale Ermittlungsverfahren richtete sich u.a. gegen die Nutzer des kinderpornographischen Internetboards „Hurt to the Core". Die Seite war im Darknet gehostet, also vermeintlich anonym, und hatte zum Feststellungszeitpunkt 7.331 registrierte Mitglieder/Nutzer und 18.674 einzelne, allesamt noch abrufbare Postings zu 1.932 einzelnen Themen. Thematisch ausgerichtet war das Board vollständig auf das sexuelle Missbrauchen in Verbindung mit dem sexualisierten Verletzen, Foltern, Töten bis hin zum Verzehren von Menschen, hauptsächlich Kindern. Die Abbildungen 8 und 9 stammen aus diesem Board.
Es gab einen separaten Teil „Deutsch", in dem zuletzt über 100 registrierte Mitglieder in deutscher Sprache kommunizieren und Dateien veröffentlichen konnten.

Es war den US-Ermittlungsbehörden gelungen, durch Ausnutzen einer Schwachstelle der Anonymisierungssoftware TOR (The Onion Router) die Verschleierung der IP-Adressen der Nutzer zu brechen, das Board zu überwachen und nahezu in Echtzeit Real-IP-Adressen an die internationalen Partner auszuleiten. Obwohl die Abfrage der IP-Adressen also zeitnah (binnen Stunden) erfolgte, konnten rund 20% der Täter nicht ermittelt werden.

cc) Operation „Blackshades"
Das Verfahren, in dem es um den Verdacht des Ausspähens von Daten und des Computerbetruges ging, richtete sich gegen die mutmaßlichen Verkäufer und Erwerber der Schadsoftware „Blackshades".
Dieser Trojaner, der zum Preis von lediglich rund 80 Dollar erhältlich war, ermöglicht unter anderem, die Kontrolle über das infizierte Computersystem zu übernehmen, dieses aus der Ferne zu steuern und alle Daten, die darauf gespeichert sind, auszuspähen – ein ideales Tatmittel, um an sensible Unternehmensdaten zu gelangen, Computerbetrugstaten oder Erpressungen durchzuführen. Dazu stellte das Schadprogramm diverse Funktionen zur Verfügung, u.a. die Einrichtung eines sog. Keylog-

gers zum Mitschnitt und zur Ausleitung aller Tastatureingaben des Opfers, eine Funktion zur unbemerkten Steuerung der Webcam des Opfersystems, die Anfertigung von Screenshots (Momentaufnahmen) des aktuell sichtbaren Bereiches auf dem Bildschirm des Opfersystems, die Ausführung von DDoS-Angriffen, eine „Ransomware"-Funktion, die dazu dient, alle Dateien auf dem Opfersystem zu verschlüsseln und das Opfer gegen Geldzahlung zur Freigabe der Daten zu erpressen sowie die Möglichkeit zum gezielten Ausspähen digitaler Identitäten (sog. ID-Theft-Funktionalität.
Das Verfahren gegen die Programmierer und Verkäufer der Software hatte in den Vereinigten Staaten seinen Ursprung. Die US-Ermittlungsbehörden übermittelten die im Rahmen der dortigen Ermittlungen gewonnenen Daten über die weltweiten Abnehmer des Programms an ihre internationalen Partner, darunter Deutschland.
Da die Vertreiber der Schadsoftware nicht in Deutschland aufenthältig waren, richteten sich die hiesigen Ermittlungen ausschließlich gegen die deutschen Abnehmer. Die aus den USA übermittelten rund 400 Datensätze ermöglichten schließlich die Identifizierung von rund 150 Tatverdächtigen aus Deutschland. Haupthindernis für die Identifizierung war dabei die fehlende Vorratsdatenspeicherung. Der Datensatz eines Abnehmers enthielt neben Namen, Anschrift und E-Mailadresse auch die Bestell-IP-Adresse. Letztere war als Ermittlungsansatz in Deutschland unbrauchbar.

Diese Aufzählung von Rechtstatsachen ließe sich beliebig fortsetzen.

Fazit:
Ohne Vorratsdaten ist eine effektive Verfolgung von Cybercrime nicht möglich. Der Ermittlungsansatz „IP-Adresse" kann hier durch keinen alternativen Spurenansatz ersetzt werden. Daher kann auf die Vorratsdatenspeicherung nicht verzichtet werden.

Auch das BVerfG und der EuGH haben die VDS als geeignetes Ermittlungsinstrument angesehen.

Das BVerfG stellte in seiner Entscheidung vom 02.03.2010 fest:

> *„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, 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. […]*
> *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 Vorbe-*

reitung und Begehung von Straftaten in vielen Fällen erfolgversprechend sind. [...]
Eine Speicherung der Telekommunikationsverkehrsdaten [...] knüpft vielmehr in noch begrenzt bleibender Weise an die besondere Bedeutung der Telekommunikation in der modernen Welt an und reagiert auf das spezifische Gefahrenpotential, das sich mit dieser verbindet. Die neuen Telekommunikationsmittel überwinden Zeit und Raum in einer mit anderen Kommunikationsformen unvergleichbaren Weise und grundsätzlich unter Ausschluss öffentlicher Wahrnehmung. Sie erleichtern damit zugleich die verdeckte Kommunikation und Aktion von Straftätern und ermöglichen es auch verstreuten Gruppen von wenigen Personen, sich zusammenzufinden und effektiv zusammenzuarbeiten. Durch die praktisch widerstandsfreie Kommunikation wird eine Bündelung von Wissen, Handlungsbereitschaft und krimineller Energie möglich, die die Gefahrenabwehr und Strafverfolgung vor neuartige Aufgaben stellt. Manche Straftaten erfolgen unmittelbar mit Hilfe der neuen Technik. Eingebunden in ein Konglomerat von nurmehr technisch miteinander kommunizierenden Rechnern und Rechnernetzen entziehen sich solche Aktivitäten weithin der Beobachtung. Zugleich können sie - etwa durch Angriffe auf die Telekommunikation Dritter - auch neuartige Gefahren begründen. Eine Rekonstruktion gerade der Telekommunikationsverbindungen ist daher für eine effektive Strafverfolgung und Gefahrenabwehr von besonderer Bedeutung." (BVerfG NJW 2010, 833)

Der EuGH führte aus[7]:

„Nach der Rechtsprechung des Gerichtshofs stellt die Bekämpfung des internationalen Terrorismus zur Wahrung des Weltfriedens und der internationalen Sicherheit eine dem Gemeinwohl dienende Zielsetzung der Union dar. Das Gleiche gilt für die Bekämpfung schwerer Kriminalität zur Gewährleistung der öffentlichen Sicherheit.
Im Übrigen ist insoweit festzustellen, dass nach Art. 6 der Charta jeder Mensch nicht nur das Recht auf Freiheit, sondern auch auf Sicherheit hat.
[...]
Somit ist festzustellen, dass die durch die Richtlinie 2006/24 vorgeschriebene Vorratsspeicherung von Daten zu dem Zweck, sie gegebenenfalls den zuständigen nationalen Behörden zugänglich machen zu können, eine dem Gemeinwohl dienende Zielsetzung darstellt."

2) Bewertung einzelner Argumente gegen die Vorratsdatenspeicherung

a) <u>VDS und Aufklärungsquoten</u>
Es wird vorgebracht, dass sich der Wegfall der VDS 2010 nicht negativ auf die Aufklärungsquote in der PKS ausgewirkt habe. Diese belege, dass die VDS zur Bekämpfung von Cybercrime nicht nötig sei.

Zunächst ist nochmals darauf hinzuweisen, dass die PKS u.a. wegen der Dunkelfeldproblematik nur eine beschränkte Aussagekraft hat. Viele Betroffene einer Da-

[7] EuGH, Urteil vom 08.04.2014, C-293/12, Celex-Nr. 62012CJ0293, zit. nach Juris

tenausspähung z.B. bemerken zunächst nicht, dass sie Opfer einer Straftat geworden sind. Im Falle der 18 Millionen Datensätze mussten die Opfer über eine Homepage abfragen, ob sie betroffen sind. Nur wenige der Betroffenen haben anschließend Anzeige erstattet. Das bedeutet: eine enorme Menge von Cybercrime-Straftaten ohne statistische Erfassung.

Zudem werden Auslandstaten in der PKS nicht erfasst. Befindet sich das Opfer in Deutschland, handelt der Täter aber – wie es bei Cybercrime häufig der Fall ist – aus dem Ausland oder ist es unklar, ob der Täter aus dem Ausland handelte, fließen diese Fälle in die PKS nicht ein.

Auch werden Ermittlungsverfahren bei von vorneherein erkennbarer Aussichtslosigkeit mangels noch abfragbarer IP-Adressen von den Strafverfolgungsbehörden regelmäßig gar nicht erst eingeleitet und tauchen somit nicht als „ungeklärt" in der Statistik auf. So wurden z.B. im Fallbeispiel der OP Hünstein (oben 1.b.aa) nur diejenigen Verfahren eingeleitet, bei denen noch Ermittlungsansätze bestanden. Das bedeutet, dass allein in dieser kleinen Operation 191 wegen fehlender Vorratsdatenspeicherung ungeklärter Fälle nicht in die PKS Eingang fanden.

Darüber hinaus muss man bedenken, dass in der Praxis der Erfassungsmarker „Tatmittel Internet" durch die jeweiligen polizeilichen Datenerfasser – welche nicht immer mit dem Sachbearbeiter des Verfahrens identisch sein müssen – gesetzt wird, wenn das Internet im Verfahren in beliebiger Weise relevant wurde, also auch dann, wenn lediglich über das Internet kommuniziert wurde. Dies erklärt, warum beispielsweise in der Statistik für das Jahr 2010 auch 31 Fälle des „Diebstahls von Fahrrädern unter erschwerenden Umständen" als Internetkriminalität erfasst wurden. Das heißt, in der PKS werden zahlreiche Fälle als Internetkriminalität erfasst, in denen Daten nicht der einzige Ermittlungsansatz sind.

Bedeutsam ist noch ein weiterer Umstand:
Bei der Beurteilung der Auswirkungen des Wegfalls der VDS auf die Aufklärungsquoten ist zu berücksichtigen, dass die VDS-Pflicht für den Bereich der Internet-Zugangsprovider zu keinem Zeitpunkt in dem gesetzlich vorgesehenen Umfang zum Tragen gekommen ist, weil die erste einstweilige Anordnung des BVerfG vom 11.03.2008 (NStZ 2008, 290) bereits vor Geltung der VDS für die Internetprovider ab dem 01.01.2009 die Verwendung der Daten eingeschränkt hatte. Nach dem genannten Beschluss des BVerfG war die Übermittlung der allein nach § 113a TKG auf Vorrat gespeicherten Verkehrsdaten an die Strafverfolgungsbehörden bis zur Entscheidung in der Hauptsache auf die Fälle des § 100g Abs. 1 S. 1 Nr. 1 StPO, also auf die Fälle der „Straftat von erheblicher Bedeutung", beschränkt.
Das bedeutet: Für das Feld der Internetkriminalität hat sich die VDS nie in vollem Umfang positiv auswirken können. Dies bedingt zwangsläufig, dass ihr Wegfall auch nicht wesentlich negativ bei den Aufklärungsquoten zu Buche schlagen konnte.

Soweit als Beleg für die behauptete Unwirksamkeit der VDS die Studie des Max-Planck-Instituts für ausländisches und internationales Strafrecht aus dem Jahre 2011 herangezogen wird, ist darauf hinzuweisen, dass diese Studie erheblicher, auch wissenschaftlicher, Kritik ausgesetzt ist[8]. In der Ausgabe 11/2012 vom 12.03.2012 be-

[8] https://www.bka.de/nn_196810/sid_5351C45DBA5A6EE13D40CF99BC574DDF/SharedDocs/Downloads/DE/ThemenABisZ/Mindestspeicherfristen/120330StellungnahmeMPIStudie.html?__n

richtete das Magazin „DER SPIEGEL" über eine erste Version des Gutachtens wie folgt:

> *„[...] Es handelt sich dabei um die erste Fassung des Albrecht-Gutachtens. Leutheusser-Schnarrenberger hat sie bislang unter Verschluss gehalten. Das Papier kommt zu anderen Ergebnissen als die spätere Version.*
> *In der 200 Seiten umfassenden Ursprungsexpertise aus dem August 2010 ist Kritik an der Vorratsdatenspeicherung nicht zu finden. Im Gegenteil: Damals drängten Albrecht und seine Co-Autoren geradezu auf eine Neuregelung der Speicherpflicht: ‚In Anbetracht der vielfältigen Einschränkungen, die sich in Deutschland derzeit bei dem Zugriff auf Verkehrsdaten ergeben, erscheint der Handlungsbedarf dringend.' Auf dieses Instrument zu verzichten sei eine ‚politische Abwägung zu Lasten der Strafverfolgung'.*
> *Das Freiburger Max-Planck-Institut hatte für die Originalstudie Interviews mit Experten aus der Praxis im In- und Ausland geführt, mit Staatsanwälten, Polizisten, Richtern. Diese berichteten von gravierenden Folgen, nachdem das Bundesverfassungsgericht die Speicherpflicht im März 2010 kassiert hatte. Die Suche nach IP-Adressen und Telefondaten von Verdächtigen scheitere nun regelmäßig. Viele Fälle vor allem bei der Kinderpornografie blieben ‚derzeit offensichtlich unaufklärbar', schrieben die Wissenschaftler.*
> *Doch als Kriminologe Albrecht diese Ergebnisse im Sommer 2010 dem Hause Leutheusser-Schnarrenberger präsentierte, fiel er glatt durch. Er habe sich in der Studie zu sehr auf die Wünsche der Ermittler konzentriert, vertraglich vereinbarte Leistungen seien nicht erbracht worden, hieß es aus dem Ministerium. Das Max-Planck-Institut musste nachbessern. Neben zusätzlichen Daten aus dem Jahr 2009, die in die Studie einflossen, sollte auf Wunsch des Hauses Leutheusser-Schnarrenberger ein neuer Schwerpunkt aufgenommen werden. Das Thema: ‚Ermittlungseffizienz und Aufklärungsquoten' - und dort werden jetzt jene Fakten betont, die dem Ministerium später als Argumente gegen die Vorratsdatenspeicherung dienen sollten.*
> *Das Freiburger Institut lieferte im vergangenen Juli die um 92 Seiten erweiterte Fassung mit deutlich modifizierten ‚Schlussfolgerungen'. Frühere Bewertungen der Wissenschaftler standen im Konjunktiv oder wurden in der Neufassung den befragten Ermittlern zugeschrieben. Das Justizministerium war zufrieden. [...]"*[9].

Das MPI hat den SPIEGEL-Bericht in einer Presseerklärung als „verkürzend" und „fehlinterpretierend" bezeichnet[10]. Eine Veröffentlichung der ersten Fassung des Gutachtens zum Zwecke der Überprüfung des Widerspruchs ist jedoch, soweit ersichtlich, nicht erfolgt.

---

nn=true; http://www.spiegel.de/spiegel/print/d-84339472.html;
www.sueddeutsche.de/digital/gutachten-zur-vorratsdatenspeicherung-ein-institut-zwei-meinungen-1.1307175

[9] http://www.spiegel.de/spiegel/print/d-84339472.html

[10] https://www.mpicc.de/shared/data/pdf/pm_02_12_vorratsdatenspeicherung.pdf

In der SPIEGEL-Ausgabe 12/2012 wurde über ein Gespräch mit dem Leiter des Freiburger Max-Planck-Instituts für ausländisches und internationales Strafrecht, Prof. Albrecht, wie folgt berichtet:

> *„[...] In der Debatte hätten Kritiker und Befürworter einer Wiedereinführung des umstrittenen Schnüffelinstruments die Ergebnisse seines Gutachtens ‚jeweils in ihrem Sinne interpretiert'. Die Vorratsdatenspeicherung sei keine Wunderwaffe, ‚aber sie bietet in bestimmten Fällen wichtige Ermittlungsansätze', so Albrecht. [...]"*[11]

Eine mangelnde Sorgfalt bei der Erstellung der zweiten Fassung des MPI-Gutachtens dürfte sich jedenfalls dadurch belegen lassen, dass die oben dargestellte Rechtslage zur eingeschränkten Nutzung der vorratsgespeicherten Daten aufgrund der einstweiligen Anordnungen des BVerfG und damit die beschränkte Aussagekraft der Aufklärungsquoten in dem Gutachten nicht ausführlich diskutiert, sondern lediglich knapp abgehandelt wird. Damit vermitteln die Ergebnisse der Studie in der zweiten Fassung den Eindruck, die VDS hätte ihre Wirksamkeit bei der Bekämpfung von Cybercrime entfalten können, was aber nicht den Tatsachen entspricht. Auch erfährt die Aussagekraft von Aufklärungsquoten in der Studie insgesamt eine unangemessene Überbewertung (s.o., überproportionales Dunkelfeld).

Hinzu kommt, dass die in dem Gutachten getroffenen Aussagen zum Nutzen von Vorratsdaten für die Verfolgung von Kinderpornographie mehr als fragwürdig sind. Sie beruhen überwiegend auf Erkenntnissen einer Studie der Universität Hannover, für die lediglich 81 Verfahren ausgewertet wurden. Allein in der OP „Geisterwald" wurden über 160 Verfahren gegen Konsumenten von Kinderpornographie geführt und dabei rund 50 Kindesmissbraucher überführt. Die im MPI-Gutachten getroffene Feststellung, wonach nur eine verschwindend geringe Zahl an Konsumenten von Kinderpornographie tatsächlich auch Kinder sexuell missbrauchen würden, ist aus Sicht der Hessischen Zentralstelle zur Bekämpfung der Internetkriminalität, die sich dabei auf die Erfahrung von über 3.000 Ermittlungsverfahren berufen kann, unzutreffend[12].

b) <u>Einsatz von Anonymisierungsdiensten (z.B. TOR) oder Nutzung von Internetcafés</u>
Das Argument, dass die VDS durch die Benutzung von Anonymisierungsdiensten oder Internetcafés ausgehebelt werden könne und daher für zahlreiche Verfahren ohnehin ohne Bedeutung sei, greift zu kurz. Der Umstand, dass die meisten Wohnungseinbrecher Handschuhe tragen, hat bisher noch niemanden veranlasst, den Einsatz von Daktyloskopie als für die Strafverfolgung ungeeignet zu betrachten und deren Abschaffung zu fordern.
Allein die Tatsache, dass geschickt agierende Täter trotz Vorratsdatenspeicherung nicht zu ermitteln sein werden, spricht nicht gegen dieses Ermittlungsinstrument, denn dies gilt für viele andere Kriminalitätsfelder in gleicher Weise. Überdies hat eine Vielzahl von Verfahren gezeigt, dass in einigen Kriminalitätsfeldern – wie der Verbreitung von Kinderpornographie – Verschleierungsmaßnahmen nicht durchgehend vorgenommen werden. Dies liegt u.a. daran, dass z.B. Kinderpornographie als visuelle Masturbationsvorlage von den Tätern nicht im Internetcafé oder einer Telefonzelle konsumiert wird, sondern zu Hause. Zudem sind technische Verschleierungsmaß-

[11] http://www.spiegel.de/spiegel/print/d-84430173.html
[12] vgl. dazu und zu KiPo allgemein auch S. 22 ff. der Stellungnahme des BKA zum MPI-Gutachten (oben Fn. 8)

nahmen häufig umständlich einzurichten und verlangsamen den Datenverkehr, so dass viele Täter aus Bequemlichkeit keine solchen Maßnahmen ergreifen.

Schließlich zeigt das Beispiel der OP „Downfall", dass es den Ermittlungsbehörden durchaus (wenn auch immer noch zu selten) gelingt, Anonymisierungsmaßnahmen der Täter zu brechen (s.o. 1.b.bb). Auf diese Weise erlangen die Behörden Real-IP-Adressen und benötigen die VDS.

Auch die Ermittlung eines vom Täter genutzten Internetcafés durch die VDS kann weiterhelfen, da sich daran weitere Maßnahmen - wie z. B. eine Observation - anschließen können.

c) Das Argument, durch Vermeidungsmaßnahmen der Täter könne der Erfolg sonstiger verdachtsabhängiger TKÜ-Maßnahmen im Internet vereitelt werden, ist nicht stichhaltig. Um eine verdachtsabhängige TKÜ-Maßnahme im Bereich von Internetermittlungen vornehmen zu können, sind regelmäßig Anknüpfungstatsachen erforderlich, die ohne vorratsgespeicherte Daten gar nicht erst erlangt werden können. Wie soll eine verdachtsabhängige TKÜ-Maßnahme gegen einen Täter eingeleitet werden, der wechselnde IP-Adressen verwendet, wenn man mangels Vorratsdatenspeicherung nicht ermitteln kann, an wen die IP-Adressen vergeben waren?

d) Kosten der Vorratsdatenspeicherung
Ebenso wird ins Feld geführt, die VDS sei für die TK-Unternehmen unverhältnismäßig teuer.
Es trifft zu, dass die VDS nicht unerhebliche Kosten verursacht. Andererseits ist die Anzahl der Insolvenzen von TK-Unternehmen in Ländern, die die VDS gesetzlich vorgeschrieben haben, nicht spürbar gestiegen.
Zudem darf nicht vergessen werden, dass die TK-Unternehmen seit dem Jahr 2009 für die Kosten der alten Regelung zur VDS dadurch entschädigt wurden, dass die Vergütung für Auskünfte im JVEG massiv erhöht wurde[13]. Seit dem 01.07.2009 erhielten die TK-Unternehmen z.B. für die Auskunft zu einer einzigen IP-Adresse 30,-Euro (geändert ab dem 01.08.2013, jetzt 30,-Euro pro zehn IP-Adressen in einem Abfragevorgang, immer noch ein sehr erheblicher Betrag). Als die VDS im März 2010 in Wegfall geriet, wurde das JVEG nicht geändert, so dass die TK-Unternehmen seit März 2010 für etwas entschädigt werden, das es nicht mehr gibt.

Schließlich sieht der Gesetzentwurf in § 113a TKG-E eine Entschädigung für die Umsetzung der VDS für solche Unternehmen vor, die eine unbillige Härte nachweisen können.

e) Die VDS sei ein unverhältnismäßiger Grundrechtseingriff und ermögliche die Erstellung von Bewegungsprofilen im Internet
Die Intensität des Eingriffs der Speicherung der Zuordnung einer IP-Adresse zu einem Anschlussinhaber wird überbewertet.
Es ist nicht möglich, durch eine verkehrsdatengestützte Bestandsdatenauskunft, also durch die Auskunft zu einer dynamisch vergebenen IP-Adresse, den Nutzer eines Computers oder Smartphones festzustellen. Festgestellt wird lediglich der Vertragspartner des TK-Unternehmens, der Anschlussinhaber. Es ist mithin auch nicht möglich, mithilfe von Vorratsdaten Kommunikationsvorgänge unmittelbar einer Person

[13] BT-Drs. 16/7103, siehe auch becklink 271926

zuzuordnen. Die Ermittlung eines Täters erfolgt in der Praxis mittels einer Durchsuchung und anschließender Rechnerauswertung, zumal sich häufig mehrere Personen einen Internetanschluss teilen. Am ehesten kann man die VDS im Internetbereich – etwas anderes gilt sicherlich für die Geodaten – mit der Funktion einer KFZ-Zulassungsstelle und die dynamische IP-Adresse mit einem KFZ-Kennzeichen vergleichen. Die Ermittlung des Halters eines KFZ lässt noch keinen endgültigen Schluss auf den Fahrer zu. Genauso ist es bei der VDS: Vertragspartner und Nutzer des Anschlusses zu Tatzeit sind oft verschieden. Mithin kann man aus vorratsgespeicherten Daten nicht die Kommunikationsgewohnheiten einer einzelnen Person zweifelsfrei belegen.

Die Behauptung, durch die Regelung über die VDS sei die Nutzung des Internets weithin nachvollziehbar („Bewegungsprofile" im Internet), entspricht nicht den Tatsachen. Da im Rahmen der Vorratsdatenspeicherung keine Inhaltsdaten aufgezeichnet werden, können rückwirkend nur Verkehrsdaten erhoben werden, d.h. es können durch die Strafverfolgungsbehörden lediglich die näheren Umstände der Telekommunikation, nicht aber ihr Inhalt, ermittelt werden.
Für den Bereich der Internetnutzung werden die Provider verpflichtet, die Zuordnung einer dynamisch vergebenen IP-Adresse zu den Daten des Kunden zu speichern. Nur wenn den Strafverfolgungsbehörden der eigentliche Telekommunikationsvorgang bereits genau bekannt ist (Bsp.: Der Nutzer mit der IP-Adresse 88.196.249.49 hat am 10.11.2014 um 14:38 Uhr die Internetseite www.ebay.de aufgerufen und betrügerisch eine Ware verkauft), kann ermittelt werden, welcher Kunde Teilnehmer an dem betreffenden TK-Vorgang ist (Bsp.: Die IP-Adresse 88.196.249.49 wurde am 10.11.2014 um 14:38 Uhr durch den Kunden X genutzt).
Es ist jedoch bei geltender Verpflichtung zur Vorratsdatenspeicherung - selbst unter Heranziehung von Daten nach dem TMG – nicht möglich, die komplette Internetnutzung einer Person nachzuvollziehen, weil die Provider nicht speichern müssen, welche Internetseiten ein Kunde aufgerufen hatte (Bsp.: Die Anfrage „Welche Internetseiten hat der Kunde X zwischen dem 01.11. und dem 30.11.2014 besucht?" kann der Provider auch zukünftig unter Geltung der Vorratsdatenspeicherung nicht beantworten).

f) Die VDS trage nicht zur Verhinderung von Straftaten bei.
Die Anschläge in Frankreich hätten bewiesen, dass trotz der dort vorhandenen VDS keine Straftaten verhindert werden können.
Diese Sichtweise verkennt, dass die VDS im Rahmen der Kriminalitätsbekämpfung nur ein Baustein ist. Zudem trägt die Auswertung der gespeicherten TK-Daten der Täter dazu bei, die Tat- und die Täterstrukturen aufzuklären und dadurch zukünftige Anschläge durch dieselbe Tätergruppierung zu verhindern.

Es wäre im Übrigen in Bezug auf die Aufklärung der NSU-Strukturen überaus hilfreich gewesen, auf Vorratsdaten zurückgreifen zu können. Unterstützerstrukturen hätte leichter ausgemacht werden können, wenn die TK-Verkehrsdaten rückwirkend für z.B. 6 Monate hätten erhoben werden können.

3) Zu einzelnen Regelungen des Gesetzentwurfes über die VDS

Die Vorratsdatenspeicherung ist, wie dargelegt, für eine effektive Strafverfolgung notwendig. Der Gesetzentwurf bedarf indes erheblicher Korrekturen, um für die Strafverfolgungspraxis von Nutzen zu sein.

a) Zu kurze Speicherfristen

Die in § 113b TKG-E bestimmten Speicherfristen von zehn (Verkehrsdaten) bzw. vier Wochen (Standortdaten) sind zu kurz. Für den Bereich Cybercrime gilt, dass IP-Adressen als Spuren für weiterführende Ermittlungen häufig das Ergebnis von Auswertungen von Servern und anderen Computern oder Smartphones sind. Diese Auswertungen nehmen erfahrungsgemäß eine gewisse Zeit in Anspruch und sind selten in zehn Wochen abgeschlossen.

Wie das in der breiten Öffentlichkeit bekannte Beispiel der OP „Selm" zeigt, werden ermittlungsrelevante IP-Adressen nicht selten als Ergebnis ausländischer Ermittlungen nach Deutschland übersandt. Auch insoweit muss damit gerechnet werden, dass zehn Wochen Speicherfrist den Anforderungen der Praxis nicht genügen.

Ich vermag weder der Entscheidung des BVerfG, noch derjenigen des EuGH das Gebot derartig kurzer Speicherfristen zu entnehmen.

In dem BKA-Abschlussbericht „Stand der statistischen Datenerhebung im BKA zu den Auswirkungen des Urteils des Bundesverfassungsgerichts zu ‚Mindestspeicherfristen' " finden sich folgende, empirisch begründete Aussagen[14]:

> *Darüber hinaus belegen die Angaben zur idealen Speicherdauer bezogen auf die zugrundeliegenden Sachverhalte die polizeifachliche Erforderlichkeit der Verkehrsdatenspeicherung für 6 Monate. Die Ergebnisse zeigen aber auch, dass die polizeiliche Reaktionszeit nur geringen Einfluss auf diesen polizeilich für erforderlich erachteten Mindestspeicherzeitraum hat. Zwischen dem Zeitpunkt der Kenntniserlangung des BKA über das Vorliegen ermittlungsrelevanter Verkehrsdaten und dem Moment der Stellung des Auskunftsersuchens lagen in der Regel (86 % der Fälle) maximal 7 Tage. Dies bedeutet im Umkehrschluss, dass nicht die polizeiliche Reaktionszeit, sondern das „Alter" der Verkehrsdaten den erforderlichen Speicherzeitraum bestimmt. Das tatsächliche „Alter" der relevanten Verkehrsdaten bei Auskunftsersuchenstellung muss daher zumeist annähernd 6 Monate betragen haben. Polizei bzw. Staatsanwaltschaft haben jedoch zumeist keinen Einfluss darauf, wie schnell sie durch Anzeige o. ä. überhaupt von dem Fall und somit dem Vorliegen möglicherweise ermittlungsrelevanter Verkehrsdaten erfahren.*
>
> *Nach wie vor wird eine hohe Bedeutung des „Ermittlungsansatzes Verkehrsdaten" festgestellt, auch wenn diese deliktsabhängig nicht in allen*

---

14 http://www.bka.de/nn_234042/SharedDocs/Downloads/DE/ThemenABisZ/Mindestspeicherfristen/120130StatistischeDatenerhebungMindestspeicherungsfristenAbschlussbericht.html

Fällen (so aber insbesondere in den Phänomenbereichen Kinderpornographie und IuK-Kriminalität) den einzigen Ermittlungsansatz bilden.

Aus meiner eigenen Erfahrung im Phänomenbereich Cybercrime (seit 1999) kann ich die Aussagen des BKA bestätigen.

b) Straftatenkatalog unvollständig

Der Straftatenkatalog des § 100g Abs. 2 StPO-E greift deutlich zu kurz. Es fehlen z.B. die im Cybercrimebereich besonders relevanten Straftaten der §§ 263, 263a StGB (s.o., 74,2 Prozent).

Es ist nicht verständlich und nicht geboten, dass durch den Gesetzentwurf der Zugriff auf Verkehrsdaten nunmehr höheren Schranken unterliegen soll als der Zugriff auf Inhaltsdaten. Dies führte zu dem absurden Ergebnis, dass bei einem Fall des gewerbsmäßigen Computerbetruges eine Inhaltsüberwachung der Telekommunikation möglich wäre, nicht aber ein Zugriff auf Vorratsdaten. Dies widerspricht der vom BVerfG in ständiger Rechtsprechung zugrunde gelegten Wertung, dass der Zugriff auf Verkehrsdaten weniger intensiv ist als der Zugriff auf Inhaltsdaten.

Aus Sicht der Strafverfolgungspraxis sollte der Katalog erweitert und derjenige des § 100a Abs. 2 StPO herangezogen werden. Verfassungsrechtliche oder europarechtliche Bedenken gegen die Anwendung dieses Straftatenkatalogs sind nicht ersichtlich.

c) Fehlende Abfragemöglichkeit für in der Vergangenheit liegende Standortdaten

Der Gesetzentwurf bleibt eine hinreichende Begründung dafür schuldig, aus welchem Grund der Zugriff auf in der Vergangenheit liegende Standortdaten zukünftig auf die Fälle von Katalogtaten nach § 100g Abs. 2 StPO-E eingeschränkt wird. Die zwingende Notwendigkeit hierfür ist weder dem Urteil des BVerfG zu entnehmen, noch folgt dies aus der Entscheidung des EuGH. Daher ist diese Einschränkung zu streichen, denn sie bedeutet eine Verschlechterung der Rechtslage gegenüber dem jetzigen Zustand.

d) Fehlende Erfassung der E-Mail-Verkehrsdaten

Obwohl das BVerfG dies in seiner Entscheidung als Anforderung für eine künftige Regelung der VDS nicht gefordert hat, werden Verkehrsdaten bei E-Mail-Providern zukünftig nicht zu speichern sein (§113b Abs. 5 TKG-E). Nach wie vor besitzt der E-Mail-Verkehr im Bereich Cybercrime indes eine erhebliche Bedeutung. Werden E-Mail-Verkehrsdaten von der VDS ausgenommen, schränkt dies die Aufklärungsmöglichkeiten für die Strafverfolgungsbehörden ohne sachlichen Grund erheblich ein.

E-Mai-Verkehrsdaten (Message-ID, Zeitstempel, IP-Adresse des Absenders) sind daher in den § 113b TKG-E aufzunehmen.

e) Richtervorbehalt ohne Eilanordnungskompetenz für die Staatsanwaltschaft

Auch dieser Unterschied zu Telekommunikationsinhaltsüberwachung ist sachlich und verfassungsrechtlich nicht geboten. Vorratsdaten sind in ihrer Sensibilität mit Inhaltsdaten nicht zu vergleichen, denn sie erlauben keinen unmittelbaren Rückschluss auf den konkret Kommunizierenden und bergen auch nicht die Gefahr von Kernbereichsrelevanz. Es ist mithin angezeigt, ebenso wie im § 100b StPO eine Eilanordnungskompetenz der Staatsanwaltschaft vorzusehen und § 101a Abs. 1 S. 2 StPO-E ersatzlos zu streichen.

f) Fehlende Speicherverpflichtung für Telemediendienste, die TK-Leistungen erbringen

Der Gesetzentwurf sieht in § 113a Abs. 1 TKG-E eine Pflicht zur Speicherung nur für die Erbringer von öffentlich zugänglichen Telekommunikationsdiensten, also für Telefon- und Internetzugangsdienste, vor. Vielfach werden heute aber Telekommunikationsdienste auch von Telemediendiensten erbracht. Telemediendienste sind gemäß § 1 Telemediengesetz (TMG) alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 des Telekommunikationsgesetzes oder Rundfunk nach § 2 des Rundfunkstaatsvertrages sind (Beispiel: Facebook ist ein Telemediendienst). Die über Telemedien geführte Kommunikation besitzt eine erhebliche Bedeutung für die Strafverfolgungsbehörden.

Es sollten daher auch die Telemediendienste, die öffentlich zugängliche Telekommunikationsdienste erbringen, verpflichtet werden, folgende Daten zu speichern:

- die Daten, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind (Bestandsdaten, vgl. § 14 Abs. 1 TMG) und
- die Daten, die bei der Inanspruchnahme von über Telemedien öffentlich erreichbare Telekommunikationsdienste anfallen, soweit es sich nicht um Angaben über die vom Nutzer in Anspruch genommenen Telemedien handelt. (reduzierte Nutzungsdaten, vgl. § 15 Abs. 1 Nr. 1 und 2, aber nicht nach Nr. 3 TMG, also Merkmale zur Identifikation des Nutzers und Angaben über Beginn und Ende der jeweiligen Nutzung eines über Telemedien öffentlich erreichbare Telekommunikationsdienste, aber keine Inhaltsdaten).

g) Fehlende Regelung zur Umsetzung von Art. 16, 17 des Übereinkommens über Computerkriminalität

Die Grenzenlosigkeit des Internets verursacht eine steigende Notwendigkeit grenzüberschreitender Ermittlungen. Die damit verbundenen Probleme – erforderliche Strafverfolgungsmaßnahmen berühren die Hoheitsrechte anderer Staaten und bedingen Rechtshilfemaßnahmen – sind den Tätern wohlbekannt und werden gezielt ausgenutzt (siehe oben). Das Übereinkommen über Computerkriminalität (Convention on Cybercrime, ETS No.185, auch „Budapester Konvention gegen Datennetzkri-

minalität" genannt) vom 23.11.2001 ist das weltweit erste multilaterale Übereinkommen über Datennetz- und Computerkriminalität. Die Vertragsstaaten haben sich zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Computersystemen verpflichtet, bestimmte materielle Straftatbestände im Bereich der Computerkriminalität sowie bestimmte Befugnisse für Ermittlungsverfahren einzuführen. Deutschland hat die Cybercrime Convention (nachfolgend: CC) am 09.03.2009 ratifiziert und am 01.07.2009 in Kraft gesetzt. Das Vertragswerk enthält in Kapitel III (Art. 23 bis 35) Vorschriften zur internationalen Zusammenarbeit und Rechtshilfe, insbesondere, sofern Beweise in elektronischer Form erhoben werden sollen. Geregelt werden die Behandlung von Rechtshilfeersuchen bei Vorliegen von anwendbaren völkerrechtlichen Übereinkünften sowie solche ohne. Darüber hinaus sind Vorschriften enthalten zum grenzüberschreitenden Zugriff auf gespeicherte Daten ohne Rechtshilfeersuchen und zur Errichtung eines 24 (Stunden) /7 (Tage) Netzwerkes für eine schnelle wechselseitige Hilfeleistung.

Besonders hervorzuheben ist dabei die Möglichkeit einer beschleunigten zwischenstaatlichen Rechtshilfe zur umgehenden Sicherung von beweiserheblichen Computerdaten nach Art. 29 CC i.V.m. Art. 16 und 17 CC. Hierfür soll ein formloses Ersuchen an den ausländischen Vertragsstaat zur Vorabsicherung der beweisrelevanten Daten, das inhaltlich den Anforderungen des Art. 29 Abs. 2 CC entsprechen muss, genügen. Durch die Verpflichtung zur Sicherung der Daten, insbesondere gegen die automatische Löschung, begründet die Maßnahme im Unterschied zur klassischen Durchsuchung und Beschlagnahme, die nur mit einer Duldungspflicht einhergehen, eine aktive Mitwirkungspflicht der betroffenen Provider. Nach Eingang des Ersuchens hat der Vertragsstaat gem. Art. 29 Abs. 3 S. 1 CC geeignete Maßnahmen zur umgehenden Sicherung der Daten zu treffen, wobei die beiderseitige Strafbarkeit keine Voraussetzung für die Vornahme der Sicherung ist (Art. 29 Abs. 3 S. 2 CC). Durch diese vorläufige Maßnahme lässt sich damit eine Aufbewahrung der beweisrelevanten Daten erreichen, die viel schneller und effektiver als traditionelle Rechtshilfehandlungen ist. Art. 29 Abs. 7 CC sieht vor, dass die gesicherten Daten für mindestens 60 Tage aufbewahrt werden sollen, um der ersuchenden Vertragspartei ein förmliches Rechtshilfeersuchen um Durchsuchung oder ähnlichen Zugriff bzw. Beschlagnahme oder ähnliche Sicherstellung oder Weitergabe der Daten zu ermöglichen.

Art. 35 CC verpflichtet die Vertragsparteien zur Einrichtung einer Kontaktstelle, die an sieben Wochentagen 24 Stunden täglich zur Verfügung steht, um für eilige Ermittlungshandlungen oder für die Erhebung von Beweismaterial in elektronischer Form unverzüglich für Unterstützung zu sorgen. Diese Unterstützung umfasst unter anderem die jederzeitige transnationale Übermittlung der Vorabsicherungsersuchen nach Art. 29 CC. Die Aufgabe des Art. 35 CC übernimmt das auf polizeilicher Ebene eingerichtete G7 24/7 High Tech Crime Network (HTCN). Die deutschte Kontaktstelle ist das Bundeskriminalamt.

Derzeit kann Deutschland ausländischen Ersuchen gemäß Art. 29 nicht in der Weise nachkomme, wie es die Konvention eigentlich vorsieht. Die in Art. 17 i. V. m. Art. 16 Abs. 1 des Übereinkommens geforderte beschleunigte Sicherung von Verkehrsdaten ist bislang nicht ausdrücklich in nationales Recht umgesetzt worden. Zum Zweck der Umsetzung war zunächst erwogen worden, in § 100g StPO die zur Beauskunftung Verpflichteten auch zu verpflichten, die von ihnen erhobenen Verkehrsdaten aufgrund einer polizeilichen oder staatsanwaltschaftlichen Anordnung für die Dauer von einer Woche bereitzuhalten, wenn die Strafverfolgungsbehörden die Beantragung

einer gerichtlichen Anordnung zur Erhebung der Daten ankündigen. Man ging jedoch dann davon aus, dass die Umsetzung der Richtlinie 2006/24/ EG über die Vorratsspeicherung von Verkehrsdaten dies entbehrlich machen würde (BR-Drucksache 16/5846, S. 27). Durch den Wegfall der Vorratsdatenspeicherung besteht insoweit ein für die Strafverfolgungsbehörden spürbares Umsetzungsdefizit, das sich immer dann bemerkbar macht, wenn andere Vertragsstaaten entsprechende Ersuchen auf beschleunigte Vorabsicherung von Daten an die zuständige deutsche Kontaktstelle richten und diese oft nicht in erforderlicher Weise erledigt werden können. Mangels einer Verpflichtung der Provider (in der Praxis sind zumeist Hostserviceprovider, also Telemediendienste, betroffen), auf polizeiliche oder staatsanwaltschaftliche Anordnung beschleunigt Daten vor einer Löschung zu bewahren („Quick-Freeze"), kann hier derzeit regelmäßig nur der herkömmliche und deutlich langsamere Weg über §§ 94 Abs. 1 Nr. 1 i.V.m. 67 Abs. 1, Abs. 2 und 66 Abs. 1 Nr. 1, Abs. 2 Nr. 1 IRG beschritten werden.

In den GesetzE sollte die überfällige Regelung zur vollständigen Umsetzung des Übereinkommens aufgenommen werden. Das TKG und das TMD sind um Quick-Freeze Vorschriften zu ergänzen, wonach TK- und TM-Dienste verpflichtet werden, beweiserhebliche Daten für die Dauer von 60 Tagen (mit Verlängerungsmöglichkeit) zu sichern. Herauszugeben sind die Daten erst, wenn das ausländische Rechtshilfeersuchen eingetroffen und bewilligt ist.

4) Zur Datenhehlerei

Der Straftatbestand der Datenhehlerei schließt eine Schutzlücke, indem Daten im Kernstrafrecht nunmehr ähnlich wie Sachen geschützt werden. Die Einführung der Datenhehlerei ist trotz der Strafbarkeit nach § 44 BDSG notwendig, da sich der Schutz des BDSG nur auf personenbezogene Daten erstreckt, also nicht z.B. auf Unternehmensdaten, und dieser als absolutes Antragsdelikt für eine effektive Strafverfolgung im Bereich des Datenhandels untauglich ist.

Es ist allerdings zu kritisieren, dass der ursprüngliche Gesetzentwurf (BT-Drs. 17/14362) nicht unverändert übernommen wurde, sondern erhebliche Einschränkungen erfahren hat. So ist die Strafandrohung mit bis zu drei Jahren zu niedrig, d.h. Daten sind noch immer weniger geschützt als Sachen. Auch die Tatsache, dass die schweren Fälle nicht übernommen wurden, ist zu kritisieren.

Der ursprüngliche Gesetzentwurf der Datenhehlerei (BT-Drs. 17/14362) ist dem nunmehr vorgelegten vorzuziehen.

5) Zusammenfassung

Der Gesetzentwurf zur VDS vermag nicht zu überzeugen und bringt in einigen Bereich sogar eine Verschlechterung der Rechtslage für die Strafverfolgungsbehörden mit sich.
Vor allem die kurzen Speicherfristen und der zu sehr eingeschränkte Straftatenkatalog sind praxisuntauglich.

Sollte das Gesetz unverändert verabschiedet werden, wird es im Phänomenbereich Cybercrime weitgehend ohne Wirkung bleiben. Zudem besteht dann die Gefahr, dass die zahlenmäßig geringen Anwendungsfälle den nicht unerheblichen Grundrechtseingriff der Vorratsdatenspeicherung als solchen nicht mehr zu rechtfertigen vermögen und das Gesetz damit wegen fehlender Eignung zur Zweckerreichung insgesamt verfassungswidrig sein könnte.

Demgegenüber ist der Straftatbestand der Datenhehlerei eine notwendige Ergänzung des strafrechtlichen Schutzes für Daten. Allerdings ist der erste Gesetzentwurf zur Datenhehlerei aus der vergangenen Legislaturperiode praxisgerechter als der aktuelle.

gez.
Franosch
Oberstaatsanwalt

DeutscherAnwaltVerein

Stellungnahme

des Deutschen Anwaltvereins durch die Ausschüsse Gefahrenabwehrrecht, Informationsrecht und Strafrecht

zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz für ein Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (Stand: 15.05.2015)

Stellungnahme Nr.: 25/2015 Berlin, im Mai 2015

Mitglieder des Ausschusses Gefahrenabwehrrecht

- Rechtsanwältin Dr. Heide Sandkuhl, Potsdam (Vorsitzende und Berichterstatterin)
- Rechtsanwalt Wilhelm Achelpöhler, Münster
- Rechtsanwalt Prof. Dr. Björn Gercke, Köln (Berichterstatter)
- Rechtsanwältin Andrea Groß-Bölting, Wuppertal
- Rechtsanwalt Dr. Stefan König, Berlin
- Rechtsanwältin Dr. Regina Michalke, Frankfurt / Main (Berichterstatterin)
- Rechtsanwältin Kerstin Oetjen, Freiburg

Zuständig in der DAV-Geschäftsführung

- Rechtsanwalt Thomas Marx

Mitglieder des Ausschusses Informationsrecht

- Rechtsanwalt Dr. Helmut Redeker, Bonn (Vorsitzender)
- Rechtsanwältin Dr. Christiane Bierekoven, Nürnberg
- Rechtsanwältin Isabell Conrad, München
- Rechtsanwalt Dr. Malte Grützmacher, LL.M., Hamburg
- Rechtsanwalt Prof. Niko Härting, Berlin (Berichterstatter)
- Rechtsanwalt Peter Huppertz, LL.M., Düsseldorf
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München (Berichterstatter)
- Rechtsanwalt Prof. Dr. Holger Zuck, Stuttgart

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
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Zuständig in der DAV-Geschäftsführung

- Rechtsanwalt Thomas Marx

Mitglieder des Ausschusses Strafrecht

- RA Prof. Dr. Stefan König, Berlin (Vorsitzender und Berichterstatter)
- RA Dr. h.c. Rüdiger Deckers, Düsseldorf
- RAin Dr. Margarete Gräfin von Galen, Berlin
- RAin Dr. Gina Greeve, Frankfurt am Main
- RA Prof. Dr. Rainer Hamm, Frankfurt am Main
- RA Eberhard Kempf, Frankfurt am Main
- RA Dr. Ali B. Norouzi, Berlin
- RAin Gül Pinar, Hamburg
- RA Michael Rosenthal, Karlsruhe
- RA Martin Rubbert, Berlin
- RAin Dr. Heide Sandkuhl, Potsdam (Berichterstatterin)
- RA Dr. Rainer Spatscheck, München
- RA PD Dr. Gerson Trüg, Freiburg im Breisgau

Zuständig in der DAV-Geschäftsführung

- RAin Tanja Brexl, DAV-Berlin

Verteiler

Bundesministerium der Justiz und für Verbraucherschutz
Bundesministerium für Wirtschaft und Energie
Bundesministerium des Inneren

Ausschuss für Recht und Verbraucherschutz im Deutschen Bundestag
Ausschuss für Wirtschaft und Energie im Deutschen Bundestag
Ausschuss Digitale Agenda im Deutschen Bundestag
Innenausschuss im Deutschen Bundestag
Vorsitzende des Ausschusses für Recht und Verbraucherschutz im Deutschen Bundestag, Renate Künast
Vorsitzender des Innenausschusses im Deutschen Bundestag, Wolfgang Bosbach

Bundesgerichtshof
Bundesanwaltschaft

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Die Datenschutzbeauftragten der Bundesländer

Arbeitsgruppen Recht der Bundestagsfraktionen
Arbeitsgruppen Inneres der Bundestagsfraktionen
Justizministerien und Justizsenatoren der Länder
Landesministerien und Senatsverwaltungen des Inneren
Wirtschaftsministerien der Länder
Innenausschüsse der Landtage

Europäische Kommission - Vertretung in Deutschland
Bundesrechtsanwaltskammer
Bundesnotarkammer
Bundesverband der Freien Berufe
Deutscher Richterbund
Deutscher Notarverein e.V.
Deutscher Steuerberaterverband
Bundesverband der Deutschen Industrie (BDI)
GRUR
BITKOM
DGRI
Gewerkschaft der Polizei (Bundesvorstand)
Deutsche Polizeigewerkschaft im DBB
Ver.di, Recht und Politik
Deutscher Strafverteidiger e.V., Mirko Roßkamp
Regionale Strafverteidigervereinigungen
Organisationsbüro der Strafverteidigervereinigungen und – initiativen
Bund Deutscher Kriminalbeamter
Strafrechtsausschuss der BRAK
Vorsitzende des Strafrechtsausschusses des KAV, BAV

DAV-Vorstand und Geschäftsführung
Vorsitzende der DAV-Gesetzgebungsausschüsse

Vorsitzende der DAV-Landesverbände
Vorsitzende des FORUMs Junge Anwaltschaft
Gefahrenabwehrrechtsausschuss des Deutschen Anwaltvereins
Informationsrechtsausschuss des Deutschen Anwaltvereins
Strafrechtsausschuss des Deutschen Anwaltvereins
Geschäftsführender Ausschuss der Arbeitsgemeinschaft Strafrecht des Deutschen Anwaltvereins

Frankfurter Allgemeine Zeitung
Süddeutsche Zeitung GmbH
Berliner Verlag GmbH
Redaktion NJW
Juve-Verlag
Redaktion Anwaltsblatt
Juris
Redaktion MultiMedia und Recht (MMR)
Redaktion Zeitschrift für Datenschutz ZD
Redaktion heise online
Strafverteidiger-Forum (StraFo)
Neue Zeitschrift für Strafrecht, NStZ
Strafverteidiger

Prof. Dr. Jürgen Wolter, Universität Mannheim
Deutscher Juristentag (Präsident und Generalsekretär)
Prof. Dr. Schöch, LMU München

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit derzeit ca. 66.000 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

Zusammenfassung und Vorbemerkung

Nach Auffassung des DAV ist der Referentenentwurf weit davon entfernt, den mit einer Vorratsdatenspeicherung verbundenen schweren Eingriff in das Fernmeldegeheimnis zu rechtfertigen. Das Rechtfertigungsdefizit wiegt umso schwerer, als keine gesicherten empirischen Erkenntnisse darüber vorliegen, ob mit der flächendeckenden Vorratsdatenspeicherung das Ziel der Gefahrenabwehr und der Strafverfolgung überhaupt erreicht werden kann.

Der Schutz des anwaltlichen Berufsgeheimnisses erfordert einen gesteigerten Schutz jedweder beruflichen Kommunikation des Anwalts. Berufsgeheimnisträger sind durch die Vorratsdatenspeicherung besonders betroffen, ihre Arbeit ist auf Vertraulichkeit angelegt. Diesem besonderen Schutz wird der Referentenentwurf nicht gerecht.

Aus datenschutzrechtlicher Hinsicht werden mit dem vorgeschlagenen Entwurf in vielerlei Hinsicht die Vorgaben des EuGH nicht eingehalten. Dies betrifft unter anderem die Datensicherheit bei Speicherung der Daten und die Bezeichnung derjenigen Kommunikationsformen, die vom Gesetz erfasst sein sollen.

Neu im Vergleich zu den Leitlinien vom 15. April 2015 ist die geplante Einführung eines Straftatbestandes der Datenhehlerei. Damit unternimmt es die Bundesregierung – an verborgener Stelle eines Gesetzentwurfes, dessen Überschrift insinuiert, es gehe um Datenspeicherfristen – staatlichen Stellen die Früchte illegaler Datenerhebungen zu sichern. Dies wäre angesichts des bekannt gewordenen Verdachts systematischer Ausspähung von Bürgern, Unternehmen und Amtsträgern durch (ausländische) staatliche Stellen ein

fatales Signal. Zu dem vorgeblichen Zweck des neuen Straftatbestandes, das formelle Datengeheimnis vor einer Fortsetzung und Vertiefung seiner durch eine vorausgegangene Straftat erfolgten Verletzung zu schützen, steht dies in einem grotesken Widerspruch (dazu unter IV.).

Schließlich sollten auch die Erfahrungen in der Europäischen Union mit nationaler Gesetzgebung zur Vorratsdatenspeicherung berücksichtigt werden. In den Niederlanden, Bulgarien und der Slowakei wurden die Gesetze zur Speicherung von Vorratsdaten im Jahr 2015 für nichtig erklärt, in Österreich, Rumänien und Slowenien bereits im Jahr 2014. In mehreren Mitgliedstaaten der Europäischen Union sind derzeit verfassungsrechtliche Verfahren zur nationalen Gesetzgebung zur Speicherung von Vorratsdaten anhängig.

I.

Kein Anlass für eine anlasslose Vorratsdatenspeicherung

Während der Bundesminister der Justiz und für Verbraucherschutz seit 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[1], hat er nun eine Kehrtwende vollzogen. Nachdem das Ministerium sein Vorhaben zunächst in „Leitlinien zur Einführung einer Speicherfrist und Höchstspeicherfrist für Verkehrsdaten“ am 15. April 2015 vorgestellt hatte, legte es jetzt am15. Mai 2015 einen Referentenentwurf für ein Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vor. Weder in den Leitlinien noch im Referentenentwurf findet sich eine Begründung, weshalb jetzt eine Vorratsdatenspeicherung für erforderlich und angemessen erachtet wird. Der Referentenentwurf rekurriert lediglich auf Lücken bei der Strafverfolgung und bei der Gefahrenabwehr. Wenn – so argumentieren die Entwurfsverfasser – es nach geltender Rechtslage vom Zufall abhängt, ob Verkehrsdaten zum Zeitpunkt der

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

Anfrage noch vorhanden sind oder nicht, „kann (es) im Einzelfall dazu führen, dass strafrechtliche Ermittlungen ohne Erfolg bleiben, weil weitere Ermittlungsansätze nicht vorhanden sind."

1.

Inhalt des Referentenentwurfes

Der Referentenentwurf sieht im Wesentlichen folgendes vor:

- Speicherung von Verkehrsdaten, die bei der Telekommunikation anfallen,
- Speicherfrist: Standortdaten: vier Wochen, im Übrigen: zehn Wochen,
- Abruf der Daten:
  - zur Gefahrenabwehr durch Polizeibehörden, wenn tatsächliche Anhaltspunkte für bestimmte konkrete schwerste Gefahren vorliegen,
  - zu Strafverfolgungszwecken durch die Strafverfolgungsbehörden (umfassender Richtervorbehalt, keine Eilkompetenz der Staatsanwaltschaft, Straftatenkatalog),
- vor dem Abruf der Daten sind die Betroffenen grundsätzlich zu benachrichtigen,
- Telekommunikationsdiensteanbieter müssen die Daten gegen unbefugte Kenntnisnahme und Verwendung schützen; tun sie dies nicht, sollen sie mit „Sanktionen belegt" werden,
- bei unverhältnismäßiger Kostenlast Entschädigung der Telekommunikationsdiensteanbieter für die Umsetzung der Speicherverpflichtung,
- Löschung der Daten nach Ablauf der Höchstspeicherfrist,
- Androhung von Ordnungsgeld für den Fall, dass die Löschverpflichtung verletzt wird,
- Einführung eines Straftatbestandes der Datenhehlerei (§ 202d StGB-E)

2.

Verfassungsrechtlicher Rahmen

Mit Urteil vom 2. März 2010 hat das Bundesverfassungsgericht klargestellt, dass eine vorsorgliche anlasslose Speicherung der Telekommunikationsverkehrsdaten die **Ausnahme** bleiben müsse, da es sich um einen besonders schweren Eingriff mit einer Streubreite handele, wie sie die Rechtsordnung bisher nicht kenne und der geeignet sei, ein „diffus bedrohliches Gefühl des Beobachtetseins“ hervorzurufen[2]. Insoweit korrespondiert hiermit die Entscheidung des Europäischen Gerichtshofs vom 8. April 2014, nach der der Schutz des Grundrechts auf Achtung des Privatlebens verlangt, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkung auf das absolut Notwendige beschränken müssten[3]. Geht es aber mit der anlasslosen Vorratsdatenspeicherung um eine absolute Ausnahme vom geltenden Recht, die auf das absolut Notwendige beschränkt werden muss, bedeutet dies für den rechtspolitischen Handlungsrahmen Folgendes:

Bereits aus der Beachtung des rechtsstaatlich kaum zu überschätzenden Verhältnismäßigkeitsprinzips ergibt sich, dass den Gesetzgeber von vornherein eine Darlegungslast trifft. Darzulegen ist, dass die Vorratsdatenspeicherung „erforderlich“ und – wenn man die Erforderlichkeit unterstellt – zur Erreichung der sicherheitspolitischen Ziele „geeignet“ ist. Die damit einhergehende Darlegungslast bedeutet der Sache nach, dass der Gesetzgeber zur Rechtfertigung des beabsichtigten Eingriffs der Notwendigkeit unterfällt, darzutun, dass und inwieweit es überhaupt zur Gefahrenabwehr eines derartigen Eingriffs bedarf. Nichts anderes gilt im verfassungsrechtlichen Ergebnis, wenn man an den den Gesetzgeber überantworteten Gestaltungsspielraum verfahrensbezogene Anforderungen knüpft. Immerhin ist nach der Rechtsprechung des BVerfG davon auszugehen, dass Gesetze, die auf einer Prognose beruhen, stets aus sich

[2] *BVerfG* NJW 2010, 833.
[3] *EuGH* U. v. 08.04.2014, I-25; verbundene Rechtssachen C-293/12 und C-594/12.

selbst heraus eine spätere und überprüfbare Begründung zu den Annahmen über ihre voraussichtliche Wirkung erkennen lassen[4]. Diese Darlegungslast ist die Kehrseite des dem Gesetzgeber eingeräumten Entscheidungs- und Beurteilungsspielraums, denn nur hierdurch wird der Bürger in die Lage versetzt, die Gründe für den Eingriff in seine Grundrechte zu erfahren und erforderlichenfalls Rechtsschutz in Anspruch zu nehmen.

Der Referentenentwurf ist weit davon entfernt, den mit einer Vorratsdatenspeicherung verbundenen schweren Eingriff in das Fernmeldegeheimnis zu rechtfertigen.

a.

Gefahrenabwehrrecht

Dass mit einer Vorratsdatenspeicherung Gefahren nicht abgewehrt werden können, zeigen die Pariser Attentate. Obwohl Frankreich die Vorratsdatenspeicherung längst eingeführt hatte, half sie nicht, den Anschlag zu verhindern.

b.

Strafverfolgung

Ob mit einer Speicherung der Telekommunikationsdaten von 80 Millionen Bundesbürgerinnen und Bundebürgern tatsächlich Kriminalität, insbesondere der internationale Terrorismus, wirksam bekämpft werden kann, steht überhaupt nicht fest. Im Gegenteil:

- Der wissenschaftliche Dienst des Deutschen Bundestages hat festgestellt, dass die Vorratsdatenspeicherung auf die Aufklärungsquoten in den EU-

[4] Zur Darlegung bereits in der Begründung des Gesetzes, siehe *BVerfG*E 79, 311 ff., 343.

Mitgliedsstaaten „*praktisch keine Auswirkungen*“ hat[5]. Nach einem Rechtsgutachten des wissenschaftlichen Dienstes des Deutschen Bundestages, das sich auf Zahlen des Bundeskriminalamtes beruft, steigt die Aufklärungsquote mit Vorratsdatenspeicherung nur marginal um 0,006 %[6].

- Geht man nach dem vom Bundesamt für Justiz in Auftrag gegebenen Gutachten der kriminologischen Abteilung des Max-Planck-Instituts für ausländisches und internationales Strafrecht „zu möglichen Schutzlücken durch den Wegfall der Vorratsdatenspeicherung“ von Juli 2011 aus, erfolgt der Zugriff auf Vorratsdaten der Telekommunikation lediglich „*in einer sehr kleinen Zahl von Verfahren*“[7]. Das Gutachten gelangt unter anderem zu folgenden Ergebnissen:

> „*Gegenwärtig können die Auswirkungen des BVerfG-Urteils vom 2.3.2010 noch nicht mit belastbaren Zahlen quantifiziert werden. (…) Die Untersuchung von Schutzlücken bei Wegfall der Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten kann auch im Hinblick auf die Auswirkungen auf Aufklärungsquoten nur eingeschränkt erfolgen. Dieses bedingt durch das Fehlen von spezifischen empirischen Untersuchungen, die Nichterfassung von verfahrensbezogenen Daten zur Abfrage von Verkehrsdaten sowie Vorratsdaten oder IP-Adressen und die im Zusammenhang mit besonderen Deliktsphänomenen nur bruchstückhaft vorliegenden (und erfassten) Informationen zur Aufklärungsquote. Der Diskussion zu Nutzen und Konsequenzen der Vorratsdatenspeicherung kann entnommen werden, dass geeignete Daten, die zu einer quantitativen Überprüfung der Auswirkungen der Vorratsdatenspeicherung auf die Aufklärungsquote führen könnten, bislang nicht erfasst werden,* ***und im Übrigen auch nicht systematisch erfasst werden sollen****. Die Resultate der bis heute vorliegenden Antworten auf Anfragen zu dem Nutzen der Vorratsdatenspeicherung in Landtagen lassen ferner davon ausgehen, dass entsprechende statistische Erfassungen deshalb nicht vorgenommen worden sind und nicht vorgenommen werden,* ***weil sie als zu kostenträchtig angesehen werden***.“[8]

Mit anderen Worten heißt dies:

[5] Vgl. wissenschaftlicher Dienst des Deutschen Bundestages, Sachstandsbericht v. 18.03.2011, WD 7-3000-036/11.
[6] Vgl. wissenschaftlicher Dienst des Deutschen Bundestages, Rechtsgutachten v. 25.02.2011, WD 11-3000-18/11.
[7] Vgl. Gutachten Max-Planck-Institut (zweite erweiterte Fassung) Juli 2011, S. 120.
[8] Vgl. Gutachten Max-Planck-Institut (zweite erweiterte Fassung) Juli 2011, S. 218.

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

Nach der Rechtsprechung des Bundesverfassungsgerichts und des Europäischen Gerichtshofs muss die vorsorglich anlasslose Speicherung aller Telekommunikationsverkehrsdaten eine absolute Ausnahme bleiben, da sie – um es mit den Worten des Bundesverfassungsgerichts zu sagen – „*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*“[9]. Wiegt ein Eingriff derart schwer, ist es die vornehmliche Pflicht des Gesetzgebers, den Bürgerinnen und Bürgern die sachlichen Gründe darzutun, die es aus seiner Sicht rechtfertigen sollen, Grundrechte des Einzelnen auszuhöhlen. Sieht der Gesetzgeber hiervon ab – etwa weil ihm die dafür erforderlichen statistischen Erfassungen zu kostenträchtig sind und/oder die damit einhergehende Transparenz nicht willkommen ist –, haben schwerwiegende Eingriffe in die Grundrechte der Bürgerinnen und Bürger zu unterbleiben. Sie sind unverhältnismäßig, zumal folgendes noch hinzukommt:

Für diejenigen, die sich der Datenüberwachung entziehen wollen, gibt es zahlreiche Möglichkeiten, eine Überwachung durch Vorratsdatenspeicherung zu umgehen – sei es durch gestohlene Prepaid- oder SIM-Karten oder durch Nutzung offener W-LAN-Netze oder öffentlicher Netzzugänge, bei denen die

[9] *BVerfG* NJW 2010, 833.

IP-Adresse nicht einer einzelnen Person zugeordnet werden kann. Auf der anderen Seite verfügen Strafverfolgungsbehörden über neue Ermittlungsansätze – etwa das Auslesen von Datenträgern, die der Kommunikation zwischen Mensch und Maschine dienen, beispielsweise SIM-Karten, die in einer Vielzahl von technischen Geräten vorzufinden sind (z. B. in Navigationsgeräten, Geräten zum Aufspielen von Programmen zur Fehlersuche oder für Updates in Kraftfahrzeugen). Werden Computer zu Zahlungszwecken eingesetzt, können über die so gespeicherten Daten retrograde Bewegungsbilder erstellt werden. Wissenschaftler untersuchen zudem, ob über den Akku-Status des Mobiltelefons dessen Standort ermittelt werden kann. Mit anderen Worten: Zur Erreichung des hier in Rede stehenden Zwecks kann es mildere Mittel als die Vorratsdatenspeicherung geben. Jedenfalls muss dies aufgeklärt werden, bevor von der Regel abgewichen und eine Ausnahme statuiert wird, mit der höchstpersönliche Daten von Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte[10], gespeichert und dadurch die Möglichkeit geschaffen wird, sehr genaue Schlüsse auf das Privatleben unbescholtener Bürgerinnen und Bürger, mithin auf Gewohnheiten des täglichen Lebens, Aufenthaltsorte, ausgeübte Tätigkeiten und soziale Beziehungen zu ziehen.

II.

Unzureichender Schutz der Berufsgeheimnisträger

Berufsgeheimnisträger sind durch die Vorratsdatenspeicherung besonders betroffen, ihre Arbeit ist auf Vertraulichkeit angelegt. Die „Vorratsdatenspeicherung“ schafft aber gerade das Gegenteil von Vertrauen: Kontrolle. Kontrolle der Datenströme, die die technischen Endgeräte mannigfaltig produzieren sowie Kontrolle der Personen – und damit auch der Berufsgeheimnisträger – die die Datenströme verursachen.

[10] Vgl. *EuGH* U. v. 08.04.2014, 1-25; verbundene Rechtssache C-293/12 und C-594/12.

Der Referentenentwurf wirft gerade in Bezug auf Berufsgeheimnisträger besondere Probleme auf:

Ein effektiver Schutz eines engen Kreises von auf besondere Vertraulichkeit angewiesenen Berufsgeheimnisträgern bereits auf Datenerhebungsebene wie bei anderen Überwachungsmaßnahmen ist bei der Vorratsdatenspeicherung schwierig, da sie eben schon begrifflich anlasslos ist und damit kraft Natur keine vorherige Befassung im Einzelfall ermöglicht. Für – die praktisch ganz überwiegend verwandten – dynamischen IP-Adressen soll dies schon in technischer Hinsicht gelten; Simitis und Spiecker haben deutliche Zweifel daran geäußert, ob dieses Argument wirklich hieb- und stichfest ist (Simitis/Spiecker, A Never-Ending Story, Beitrag vom 5.5.2015, http://www.verfassungsblog.de/a-never-ending-story-die-vorratsdatenspeicherung/).

Dem Schutz des Berufsgeheimnisses soll lediglich dadurch Rechnung getragen werden, dass die Verkehrsdaten von Berufsgeheimnisträgern nicht *abgerufen* werden dürfen, mithin einem Schutz erst auf Verwertungsebene. Dies steht nicht im Einklang mit dem Schutz von Berufsgeheimnisträgern, wie er in den § 97 StPO und § 160a StPO normiert ist, welche einen Schutz von Berufsgeheimnisträgern bereits auf der Erhebungsebene vorsehen. Ausweislich der Gesetzgebungsmaterialien gerade zu § 160a StPO ist ein solcher absoluter Schutz im Hinblick auf die Anwaltschaft geboten, um die Gewährleistung ausreichender Verteidigungsrechte, welchen von Verfassung wegen besondere Bedeutung zu kommt, zu garantieren. Die Verfasser des Referentenentwurfes ziehen mithin den falschen Schluss: Weil es technisch – angeblich – im Regelfall nicht anders geht, will es Berufsgeheimnisträger erst auf der Verwertungsebene schützen. Dabei kann letztlich nur durch den Verzicht auf die Vorratsdatenspeicherung effektiv gewährleistet werden, dass die Verteidigungsrechte nicht beeinträchtigt werden.

Alternativ muss der Schutz des Berufsgeheimnisses bereits bei einem Datenabgleich erfolgen, also auf Erhebungsebene. Hier sind Vorkehrungen zu treffen, die „Treffer" in geschützter Kommunikation vermeiden. Auf diese Weise lässt sich eine „Identifizierung" geschützter Kommunikation im Vorfeld eines Grundrechtseingriffs erreichen. Konkret bedeutet dies, dass bei der Programmierung des Datenabgleichs Negativmerkmale zu verwenden sind (Telefonnummern, Mailadressen, Suchbegriffe), die es in größtmöglichem Umfang ausschließen, dass anwaltliche Kommunikation in „Trefferlisten" aufscheint. Gegen ein derartiges „Identifizierungsgebot" lässt sich nicht einwenden, dass dies eine gezielte Suche nach geschützter Kommunikation bedingt und somit Grundrechtseingriffe fördert bzw. intensiviert. Die „Identifizierung" ist typischerweise möglich, ohne Kenntnis vom Inhalt der Kommunikation zu nehmen. Bei der Briefpost lässt sich die „Identifizierung" regelmäßig anhand der Absender- und Empfängerangaben vornehmen, die sich auf dem Briefumschlag befinden. Beim Abhören lässt sich die „Identifikation" zumeist anhand der beteiligten Rufnummern erreichen. Die „Identifizierung" erfordert somit keinen intensiven Grundrechtseingriffs und kann im „Vorfeld" eines Grundrechtseingriffs erfolgen.

Die Bedeutung von Beweiserhebungsverboten im Vorfeld bloßer Verwertungsverbote kann aber nicht hoch genug geschätzt werden: Was gespeichert ist, wird auch wahrgenommen, kann in den Akten erfasst werden und letztlich auch inhaltlich Eingang in Verfahren finden; auch wenn diese Informationen im Ergebnis nicht verwertet werden dürfen, erhöht allein dieser Umstand jenseits aller juristischen Dogmatik und ggf. unter Begründungsakrobatik die Gefahr, dass jene auf die ein oder andere Art ihren Eingang ins Verfahren finden. Genau vor diesem Hintergrund hat der Gesetzgeber in der jüngeren Gesetzgebung, insbesondere im Telekommunikationsneuregelungsgesetz vom 21.12.2007 (TKÜN-RegG, BGBl. I, 3198) etwa in § 100a Abs. 4 S. 1 StPO und § 160a Abs. 1 S. 1 StPO wie schon zuvor in § 100c Abs. 4 S. 1 StPO den Grundrechtsschutz durch ein Beweis*erhebungs*verbot sichergestellt.

Gerade das Urteil des EuGH zur Richtlinie über die Vorratsdatenspeicherung zeigt überdies auf, dass den Berufsgeheimnisträgern besonderer Schutz zu kommen muss. Der EuGH geht nämlich davon aus, dass eine europarechtskonforme Richtlinie Berufsgeheimnisträger von der Vorratsdatenspeicherung ausnimmt und letztere für Berufsgeheimnisträger gar nicht gelten soll. Insbesondere wenn man diese Äußerung in den Kontext der sehr hohen datenschutzrechtlichen Anforderungen durch den EuGH (wie auch durch das BVerfG) setzt, genügt die „neue“ Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten gerade nicht den Vorgaben der Rechtsprechung. Denn wenn man die Daten dem EuGH zufolge gar nicht erst speichern soll, bedeutet dies begrifflich notwendig, sie gar nicht erst zu erheben. Ein Schutz auf Verwertungsebene dürfte daher jedenfalls nach der Rechtsprechung des EuGH unzureichend sein.

Hinzu kommt, dass ein Abrufverbot immer nur auf der Seite des Berufsgeheimnisträgers greift: Ein Abruf der Einzelverbindungsdaten der Anwaltskanzlei lässt sich gesetzlich verbieten.

Ins Leere geht dagegen ein Abrufverbot, wenn der Abruf beim Mandanten erfolgt. Durch einen solchen Abruf beim Mandanten/Normalbürger können staatliche Stellen trotz eines Abrufverbots ohne weiteres herausfinden, wann, wie oft und wie lange der Bürger mit seinem Anwalt (und mit seinem Arzt, Seelsorger, Steuerberater und Journalisten) telefoniert hat.

III.

Datenschutzrechtliche Probleme

1. IP-Adressen

Mit Urteil vom 8. April 2014 hat die Große Kammer des Europäischen Gerichtshofs die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rats vom 15. März 2006 über die Vorratsspeicherung von Daten für ungültig erklärt. Maßgeblich hat sich das Gericht dabei auf die Unvereinbarkeit der Richtlinie mit Art. 7, 8, 52 Abs. 1 EU-Grundrechtecharta (GRCh) gestützt. Weiter gehend als das Bundesverfassungsgericht hat der EuGH der anlasslosen Speicherung von Daten eine Absage erteilt.

Das Urteil des EuGH ist in zweifacher Hinsicht von Bedeutung für das Thema Vorratsdatenspeicherung. Zum einen klärt es erstmals das Verhältnis der Art. 7 und 8 der GRCh zueinander. Nach Auffassung des EuGH wurde durch die Richtlinie gleichrangig in beide Grundrechte auf Datenschutz und Privatsphäre in schwerwiegender Weise eingegriffen. Zum anderen verbindet es die Rechtsordnung der EU und des Europarates dadurch, dass es eine parallele Auslegung der Rechte auf Datenschutz und Privatsphäre in Europa vornimmt und in diesem Zusammenhang (erstmals) im Hinblick auf die Vorratsdatenspeicherung mehrfach auf Entscheidung des EGMR zu Datenschutz und Datensammlungen Bezug nimmt.[11]

Der Klageweg gegen bestehende mitgliedstaatliche Vorratsdatenspeicherungsgesetze ist somit in verschiedenen Konstellationen eröffnet. Als Anrufungsgrund der nationalen Verfassungsgerichte kommt Art. 15 der ePrivacy-RL in Betracht, der bestimmt, dass die nationalen Vorratsdatenspeichergesetze dem EU-Recht unterliegen und damit auch im Hinblick auf die Art. 7, 8 und 52 (1) der Charta überprüfbar sind. Die Auslegung der GRCh durch den EuGH wird durch die vorliegende Entscheidung auch zum Maßstab generell für die Rechtmäßigkeit des nationalen Rechts im Hinblick auf jedwede staatlichen

[11] Urteil EuGH Rn. 47, 54 und 55.

Überwachungssysteme. Klagen von Privatpersonen gegen ihre Provider oder den Staat wären möglich. Auch der Provider könnte ein Interesse an der Abschaffung der ihm auferlegten Speicherpflicht haben. Als Individualbeschwerde wäre der Weg zum EGMR nach Straßburg möglich.[12]

Auch der Bundesgerichtshof sieht Klärungsbedarf in europarechtlicher Hinsicht: Der BGH hat dem EuGH unter dem 28. Oktober 2014 die Frage vorgelegt, ob die – nicht zuletzt für die Vorratsdatenspeicherung elementar bedeutsame – Speicherung der IP-Adressen durch Telekommunikationsdiensteanbieter über den jeweiligen Nutzungsvorgang hinaus mit der EG-Datenschutz-Richtlinie zu vereinbaren ist. In der Konsequenz bedeutet dies, dass der EuGH nunmehr auch über die grundsätzliche Frage zu entscheiden haben wird, ob es sich bei der IP-Adresse um ein vom Datenschutzrecht geschütztes personenbezogenes Datum handelte. Das aber wiederum hat Auswirkungen auf die Zulässigkeit der Vorratsdatenspeicherung, insbesondere bezüglich der IP-Adressen. Jedenfalls hat der EuGH in seiner Entscheidung vom 8. April 2014 die IP-Adressen zu den schützenswerten Daten gezählt.

Hinzukommt folgende Problematik:

Im Kontext der Vorratsdatenspeicherung dürften IP-Adressen allerdings immer personenbezogene Daten sein: Denn die Pflicht zur Speicherung dieser Daten trifft den Provider, also denjenigen, der die Internetverbindung für den User herstellt, mit diesem also in einem entsprechenden Vertragsverhältnis steht und dem damit zwingend dessen Identität bekannt ist. Stellt man auf den Provider als verantwortliche Stelle nach § 3 Abs. 7 BDSG ab, handelt es sich also stets um personenbezogene Daten, die er – im Falle einer anlasslosen Erhebung und Speicherung – zwecklos erhebt und speichert.

[12] Das Straßburger Gericht hat sich mit Fragen der Überwachung bereits mehrfach befasst: S and Marper v. United Kingdom [GC], nos 30562/04 und 30566/04, ECHR 2008-V; Liberty and Others v. United Kingdom, no 58243/00, s. LIBE-lang, Fn. 41.

Dies widerspricht nicht nur den oben dargestellten verfassungsrechtlichen Vorgaben, insbesondere dem Verhältnismäßigkeitsgrundsatz, sondern auch dem das Datenschutzrecht beherrschenden Zweckbindungsgrundsatz. Dieser wird auch in der Entscheidung des EuGH zur Vorratsdatenspeicherung in Rn. 59 ausdrücklich aufgegriffen. Dort heißt es:

> *„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.“*

Der EuGH fordert also einen spezifischen Zusammenhang zwischen den erhobenen Daten und der Zweckverfolgung zur Bekämpfung schwerer Kriminalität, insbesondere eine Beschränkung der Daten 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.“*

Eine solche Beschränkung, die aber Grundvoraussetzung für einen rechtmäßigen und verhältnismäßigen Grundrechtseingriff ist, sehen weder die Leitlinien noch der Referentenentwurf vor. Hier bestehen also erhebliche (schwer behebbare) Mängel.

Ferner ist folgendes zu beachten:

IP-Adressen sind dem Anschlussinhaber zugeordnet. Derjenige User, der über den Anschluss das Internet verwendet, muss aber nicht notwendigerweise der Anschlussinhaber sein. Bei den wohl in Deutschland

am häufigsten anzufindenden privaten DSL-Anschlüssen ist Anschlussinhaber vielmehr oft eine andere Person (etwa ein Elternteil, der Hauptmieter, etc.), Nutzer also andere und zum Teil viele weitere Personen, etwa bei offenen WLAN-Zugängen, Internetcafes, etc.

Eine Zuordnung zu bestimmten Nutzerrechnern (etwa eines Hotelgasts, der über das Hotel-WLAN das Internet verwendet) erfolgt dabei allenfalls intern.

Erfasst werden in solchen Fällen also regelmäßig die Daten der „falschen“ Personen, nämlich nicht derjenigen, die kommunizieren, sondern der, die „nur“ die Technik dazu zur Verfügung stellen. Es erscheint zunächst zweifelhaft, ob diese „falschen“ Daten polizeilich überhaupt sinnvoll verwendet werden können.

Darüber hinaus widerspricht auch dies den Anforderungen des EuGH, wonach ein Bezug zu Personen gefordert wird, die Anlass zur Strafverfolgung geben, siehe Rn. 58:

> „*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.“*

Zu beachten ist ferner, dass man im Zeitpunkt der Erhebung und Speicherung einer IP-Adresse dieser nicht ansieht, zu welchen Zwecken der betroffene Internet-User die Internetverbindung hergestellt hat: Dies kann etwa zum „Surfen“ sein, für die Internettelefonie, aber auch zum Versand von Emails oder zur Nutzung von Messenger-Diensten.

§ 113b-E sieht in Absatz 5 folgendes vor:

„Der Inhalt der Kommunikation, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post dürfen auf Grund dieser Vorschrift nicht gespeichert werden.“

Zu Daten der elektronischen Post gehört aber auch und gerade die IP-Adresse des Absenders (und Empfängers). Diese findet sich auch in aller Regel in einer versandten Email selbst (im sog. Header).

Wenn aber bei Aufbau und auch Nutzung einer Internetverbindung nicht klar ist, wozu diese verwendet wird, zugleich keine Daten, die die Nutzung elektronischer Post betreffen dürfen, verwendet werden sollen, heißt das, dass überhaupt keine Daten auf Vorrat erfasst werden dürfen, denn es könnte sich um Daten der Nutzung von elektronischer Post handeln.

2. Ins Leere laufende Ausnahme der elektronischen Post

Die vorgenannte Ausnahme im Referentenentwurf, Daten der Dienste der elektronischen Post auszunehmen, liefe zudem faktisch ins Leere und würde den Eingriff nicht weniger intensiv oder gar verhältnismäßig machen:

Zwar sollen die Daten der Dienste von elektronischer Post nicht erfasst werden, sehr wohl aber alle andere Formen der Kommunikation, also auch – und dies sogar ausdrücklich, siehe Anlage 1 der Leitlinie, dort bei den Telefondiensten am Ende – SMS, MMS und „ähnliche Nachrichten“.

Damit ist unklar, ob die aktuellen Kommunikationsformen wie die Nutzung von Messengers auf Mobilgeräten, Skype, Chats, Foren, IRC, etc. erfasst sind oder nicht.

Die Herausnahme (zumindest) der Email-Kommunikation minimiert zwar für sich genommen die Eingriffsintensität, ist bei weitem aber nicht ausreichend, wenn in Form von „ähnlichen Nachrichten“ vergleichbare Kommunikation doch beinhaltet sein soll. Dies gilt besonders deshalb, weil zumindest im Bereich der Privatkommunikation Messengerdienste E-Mails zunehmend ersetzen und funktional Dienste der elektronischen Post darstellen (dazu ausführlich: Stellungnahme 55/13 des DAV durch den Ausschuss

Informationsrecht zur Anwendung des TKG auf neue Kommunikationsplattformen (bspw. Whats App) v. 13.12.2013).

Ähnliches gilt für die vorgesehene Ausnahme hinsichtlich des Speicherns von Internetseiten, die aufgerufen werden: Denn der Aufruf selbst soll zwar nicht gespeichert werden, kann aber – sofern anderweitig erfasst – über die http-Anfrage zugeordnet werden. Ohne die Vorratsdatenspeicherung wäre genau dies nicht möglich.

3. Metadaten – aussagekräftiger als Inhaltsdaten

Der offenbar verfolgten Argumentationslinie, dass über die Ausnahme der Nichtspeicherung von Inhaltsdaten die Eingriffsintensität reduziert werde, ist falsch.

Denn diese Argumentation übersieht, dass Verkehrsdaten und vor allem deren Kombination oftmals aufschlussreicher als die Inhalte selbst sind, da Verkehrsdaten einerseits – anders als Inhaltsdaten – von Anfang an als strukturierte Daten (also in einem bestimmten und definierten Format vorliegend) sehr viel leichter automatisiert auswertbar sind und andererseits über die Kombination der Verkehrsdaten sehr einfach Strukturen und Zusammenhänge erfasst werden können und sich durch einfache Algorithmen eine um ein Vielfaches effektivere Auswertung und damit auch Verwertungsmöglichkeit ergibt.

Mit den schon heute vorhandenen Methoden des Data Mining und der im Rahmen der technischen Disziplin der „Business Intelligence“ entwickelten Methoden zum Entdecken von Mustern in Datenbeständen ist es ein Leichtes, aus den Verkehrsdaten und deren Kombination zukünftiges Verhalten vorauszuberechnen (sog. „predictive analytics“).[13]

Die Erhebung „nur“ von Verkehrsdaten stellt also kein „weniger“ als die Erhebung von Inhaltsdaten dar, sondern einen genauso intensiven, wenn nicht sogar noch intensiveren Grundrechtseingriff.

[13] Siehe mit einem guten Überblick, http://en.wikipedia.org/wiki/Predictive_analytics).

4. Standortdaten

Bei Blick auf die Standortdaten kann auch der Argumentation dazu nicht gefolgt werden, wonach nur einzelne Standortdaten abgerufen werden dürfen. Denn nach dem Referentenentwurf soll § 113b-Ein Absatz 4 folgende Regelung enthalten:

> *„Bezeichnung der Funkzelle, die durch den anrufenden und angerufenen Anschluss bei Beginn der Verbindung genutzt werden.“*

Was aber ist mit „Verbindung“ gemeint? Da es aus dem Kontext der Leitlinien heraus ausdrücklich auch um Verbindungen in das Internet geht, kann dies also heißen, dass bei jeder Verbindungsaufnahme eines mobilen Geräts der Standort erfasst und gespeichert wird, was alle paar Sekunden der Fall sein kann. Insofern würden sehr exakte Bewegungsprofile im Rahmen der Vorratsdatenspeicherung erstellt.

Aber selbst wenn man nur den Beginn eines Telefongesprächs erfassen würde (mit der Schwierigkeit, ein solches überhaupt von einer Internetverbindung abgrenzen zu können), ergäbe sich bei einer Speicherdauer von 4 Wochen ein sehr umfassendes Bewegungsprofil.

Die Regelung, die auf die erste Aktivierung von Diensten abstellt, ebenso die Bezeichnung der Funkzelle, wenn Dienste im Voraus bezahlt werden, ist zudem unklar. Wie soll festgestellt werden, was eine „erste“ Aktivierung ist? Dazu müsste auch dieses Datum erhoben und gespeichert werden, was aktuell aber gemäß der Liste in Anlage 1 nicht vorgesehen ist.

Auch aus diesen genannten Gründen ist eine Erhebung und Speicherung schon nicht verhältnismäßig.

5. Datenspeicherung nur in der EU

Der Kritik des EuGH an der EU-Richtlinie, wonach nicht festgelegt war, dass die Daten innerhalb der EU gespeichert werden müssen, um eine unabhängige Kontrolle zu garantieren, ist vollständig zu folgen.

Diese Vorgabe greifen Leitlinien und Referentenentwurf zwar auf und betonen diesen Umstand. Es ist jedoch zu bezweifeln, dass dies viel nützt. Denn die Tendenz der US-Gerichte scheint dahin zu gehen, US-Anbieter (in einem konkreten Fall: Microsoft) zu verurteilen, auch Auskunft gegenüber den US-Behörden für in der EU gespeicherte Daten erteilen zu müssen (Urteil vom 5. April 2014, United States District Court des Southern District of New York).

Zumindest für Provider, die – auch – US-Bezug haben, dürfte ähnliches zu erwarten sein. Die vom EuGH und den europäischen Datenschutzregelungen ganz essenziell geforderte unabhängige Kontrolle wäre damit nicht nur unterlaufen, sondern ausgehebelt.

Dies ist zwar ein generelles Problem, das aber die Vorratsdatenspeicherung noch deutlich verstärken würde: Denn Daten, die nicht gespeichert sind, kann auch ein US-Provider einer US-Behörde nicht herausgeben.

6. Datensicherheit

Eine weitere Kritik des EuGH war, dass kein spezieller Schutz aus technischer und organisatorischer Sicht für die gespeicherten Daten in der EU-RL vorgesehen war.

Auch diesen Gedanken greifen die Richtlinien auf und sehen vor, dass „*die nach dem Stand der Technik höchstmögliche Sicherheit der Daten“* zu gewährleisten ist.

Was soll dieser Stand aber sein?

Die Speicherung von Daten in einem Hochsicherheitsrechenzentrum in einem Bergwerk mit 365/24/7 Bewachung durch schwer bewaffnetes Wachpersonal? Der Serverraum in einem normalen Rechenzentrum?

Der Referentenentwurf und die Leitlinien nennen zwar einige grundsätzlich erforderliche Maßnahmen, bleiben aber viel zu vage.

Der Ansatz der Leitlinien, auch den physikalischen Schutz der Daten vorzuschreiben, ist zwar richtig, die insofern genannten Punkte zur Datensicherheit sind aber schon heute für ganz „normale“ Daten Standard.

Dem Umstand, die über die Erhebung der Verkehrsdaten von 80 Millionen Deutschen über 10 Wochen (und über 4 Wochen bei Standortdaten) anfallende beispielslose Datenmasse in besonderer Weise zu schützen, werden diese Maßnahmen keineswegs gerecht.

Zu einer Minimierung des schon *durch die Erhebung* (!) erfolgenden Grundrechtseingriffs können Maßnahmen, die die *spätere Speicherung* betreffen, ohnehin nicht beitragen.

Selbst bei der Speicherung verringern sie die Eingriffsintensität nicht: Denn sie dienen dem Schutz vor Missbrauch, der selbstverständlich wichtig ist. Der unzulässige Grundrechtseingriff liegt aber nicht (erst) im Missbrauch, sondern schon im rechtmäßigen Zugriff.

Eine gute technische Absicherung minimiert diesen Eingriff nicht und kann ihn auch nie legitimieren.

Aus demselben Grund ist zwar begrüßenswert, bei Verstößen gegen die Vorgaben zur Datensicherheit Sanktionen zu verhängen. Dann aber wäre es aber einerseits dem verfassungsrechtlichen Bestimmtheitsgebot nach nötig, die Datensicherheitsmaßnahmen sehr konkret vorzugeben, die aktuelle Auflistung von nur generischen Vorgaben reicht nicht aus.

Andererseits kann aber auch hier eine *spätere* Sanktion bei Nichtbeachtung von Vorgaben nie einen *zuvor* erfolgenden Grundrechtsverstoß legitimieren.

Auffallend ist ferner, dass auch bei einer längeren Speicherung als die festgelegte Speicherfrist die TK-Anbieter zwar sanktioniert werden sollen, allerdings keine Regelung insoweit besteht, dass nach dem Überschreiten der Höchstfrist länger vorgehaltene Daten nicht mehr abgerufen werden dürfen und – wenn doch – ein Beweiserhebungs- und Beweisverwertungsverbot bestehen muss.

Verstoßen die TK-Anbieter damit gegen die geplante Regelung, geschieht das damit sogar regelmäßig im Sinne der Strafverfolgungsbehörden.

Alles in allem kann aus datenschutzrechtlicher Sicht der Referentenentwurf nicht überzeugen, ganz im Gegenteil: Er hält in vielerlei Hinsicht die Vorgaben des EuGH nicht ein.

IV.

Einführung eines Tatbestandes der „Datenhehlerei“ (§ 202d-E)

Die mit dem Entwurf vorgeschlagene Einführung eines Tatbestandes der „Datenhehlerei“ (§ 202d-E) geht auf einen Bundesratsentwurf zurück (BT-Drs. 17/14362 vom 10.07.2013), der jedoch nie zur Abstimmung gelangte. Der jetzige Vorschlag weist in der tatbestandlichen Ausgestaltung erhebliche Abweichungen auf.

Die Notwendigkeit einer neuen Regelung wird 2013 wie heute mit dem Bestehen einer Strafbarkeitslücke begründet. Gegen die Existenz einer solchen Strafbarkeitslücke spricht, dass die Zahl der in der polizeilichen Kriminalstatistik registrierten Verfahren wegen eines Verstoßes gegen §§ 44, 43 BDSG extrem gering und auf diesem geringen Niveau zusätzlich seit Jahren rückläufig ist (erfasst werden „Straftaten gegen das Bundesdatenschutzgesetz“. 2010 wurden 748 Fälle registriert, 2011 noch 571 Fälle und 2012 nur noch 479 Fälle). Es wird also von der bisher bestehenden Strafnorm kaum Gebrauch gemacht. Soweit der Entwurf sich auf statistische Erhebungen stützt, handelt es sich nur um Daten über das

Begehungsaufkommen der *Vortaten (*§§ 202a und b StGB*).* Hier ist tatsächlich ein starker Anstieg zu verzeichnen. Dies mag Veranlassung dafür geben, diese Tatbestände zu ergänzen und die Strafdrohungen zu erhöhen. Für die Notwendigkeit der Pönalisierung von „Datenhehlerei“ lässt sich daraus wenig ableiten.

§ 202 Abs. 3 StGB-E sieht vor, dass *Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher und beruflicher Pflichten dienen* nicht von dem Tatbestand erfasst werden. Dazu gehörten *insbesondere solche Handlungen von Amtsträgern oder deren Beauftragten, mit denen Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zugeführt werden sollen.*

Damit unternimmt es die Bundesregierung – an verborgener Stelle eines Gesetzentwurfes, dessen Überschrift insinuiert, es gehe um Datenspeicherfristen – staatlichen Stellen die Früchte illegaler Datenerhebungen zu sichern. Dies wäre angesichts des bekannt gewordenen Verdachts systematischer Ausspähung von Bürgern, Unternehmen und Amtsträgern durch (ausländische) staatliche Stellen ein fatales Signal. Zu dem vorgeblichen Zweck des neuen Straftatbestandes, das formelle Datengeheimnis vor einer Fortsetzung und Vertiefung seiner durch eine vorausgegangene Straftat erfolgten Verletzung zu schützen, steht dies in einem grotesken Widerspruch.

Die Entwurfsbegründung gibt vor, mit der Regelung, wonach Handlungen von der Strafbarkeit ausgenommen sind, die „ausschließlich der Erfüllung rechtmäßiger dienstlicher und *beruflicher* Pflichten dienen“ sollten nicht nur Amtsträger, sondern u. a. auch Journalisten vor Strafverfolgung geschützt werden (vgl. S. 54 d. Entwurfsbegründung). Ob von dieser sprachlichen Wendung aber auch tatsächlich ein Schutz für Angehörige dieser

Berufsgruppe ausgeht, darf bezweifelt werden. Auch bei der wortgleichen Regelung des § 184b Abs.5 StGB (Ausnahmen von der Strafbarkeit des Besitzes kinderpornographischer Materialen) ist es umstritten, ob Journalisten tatsächlich aus dem Anwendungsbereich ausgenommen sind. Es stellt sich schon die Frage, was „berufliche *Pflichten*“ eines Journalisten seien sollen. Besonders problematisch erscheint aber, dass nach der Entwurfsbegründung nur die journalistische Tätigkeiten *in Vorbereitung einer konkreten Veröffentlichung* von der Strafbarkeit ausgenommen sein soll. Dies dürfte mit den im Medienbetrieb üblichen Arbeitsweisen nicht in Einklang zu bringen sein. Ein Journalist, der Daten zugespielt bekommt, kann naturgemäß erst nach der Sichtung des Datenbestandes beurteilen, ob daraus eine Veröffentlichung werden kann bzw. soll. Strafbar hätte er sich dann aber womöglich schon gemacht. Hier ist eine Klarstellung unbedingt notwendig um die Arbeit kritischer Medien zu schützen.

V.

Kosten

Das Bundesverfassungsgericht hat in seiner Entscheidung vom 2.3.2010 die derzeitige Regelung, dass nur die Abrufkosten und nicht die Investitionskosten den Telekommunikationsunternehmen erstattet werden, nicht beanstandet.[14] Hierdurch steht allerdings zu befürchten, dass die Auswahl der Sicherheitstechnologie anhand der jeweiligen Kosten bestimmt wird. Aufgrund der hohen sicherheitstechnischen Anforderungen ist mit deutlich höheren Investitions- und Betriebskosten zu rechnen, als dies die in den Jahren 2008 bis 2010 bestehende Datenspeicherungspflicht ausgelöst habe.[15]

Im Einzelnen:

- Anspruchsvolleres Verschlüsselungsverfahren bedeutet für viele Anbieter die Anschaffung neuer Software

[14] BVerfG v. 2.3.2010 – 1 BvR 256/08, 263/08/, 586/08 (Rn. 302).
[15] *Moser-Knierim*, Vorratsdatenspeicherung: Zwischen Überwachungsstaat und Terrorabwehr, S. 351.

- Gesonderte „Speichereinrichtungen“, d.h. neue Hardware bzw. Speichermedien in exorbitantem Umfang
- „revisionssichere Protokollierung“, d.h. mehr Personalaufwand und ggf. neue Software zur Protokollierung
- „Vier-Augen-Prinzip“, d.h. ein deutlich erhöhter (besonders kostenintensiver) Personalaufwand.

Hierdurch werden erhebliche – einmalige wie auch dauerhaft wiederkehrende – Kosten entstehen.

Der Referentenentwurf sieht eine Entschädigung für die „Umsetzung der Speicherpflichten“, also der Investitionskosten vor, allerdings nur, wenn diese „erdrosselnde Wirkung“ haben; näher konkretisiert wird dies nicht. Unabhängig hiervon trägt letztlich der Bürger diese Kosten: Entweder als Nutzer des jeweiligen Providers, der die Kosten auf seine Kunden umlegen wird (so auch der Entwurfsverfasser, S. 31 d. Entwurfsbegründung), oder schlicht als Steuerzahler, sollte der Staat tatsächlich „einspringen“.

VI.

Erfahrungen in der Europäischen Union

Schließlich – und abschließend – sollten auch die Erfahrungen in der Europäischen Union mit nationaler Gesetzgebung zur Vorratsdatenspeicherung berücksichtigt werden. In den Niederlanden, Bulgarien und der Slowakei wurden die Gesetze zur Speicherung von Vorratsdaten im Jahr 2015 für nichtig erklärt, in Österreich, Rumänien und Slowenien bereits im Jahr 2014. In mehreren Mitgliedstaaten der Europäischen Union sind derzeit verfassungsrechtliche Verfahren zur nationalen Gesetzgebung zur Speicherung von Vorratsdaten anhängig.

Stellungnahme zum Gesetzentwurf der Fraktionen der CDU/CSU und SPD für ein Gesetz "zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

Mit der vorliegenden Stellungnahme soll auf verfassungsrechtliche Bedenken gegen die Regelungen des Gesetzentwurfes in der Drucksache 18/5088 eingegangen werden, ohne in umfassender Weise alle Kritikpunkte an Einzelfragen des Gesetzes aufzugreifen. Dazu haben insbesondere die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und einzelne Verbände detailliert Stellung bezogen.

1. Die verfassungsrechtlichen Prüfungsmaßstäbe

1.1. Bundesrecht

Als Prüfungsmaßstab kommen das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 iVm 1 Abs. 1 GG) und das Telekommunikationsgeheimnis aus Art. 10 Abs. 1 GG in Betracht. [1]

Hierbei ist in der Rechtsprechung des Bundesverfassungsgerichts geklärt, dass Verkehrsdaten in den Schutzbereich des Art. 10 Abs. 1 GG fallen, während Bestandsdaten vom Grundrecht auf informationelle Selbstbestimmung geschützt sind.

Eine Besonderheit gilt für die dynamischen IP-Adressen, da diese Auskunft über die Identität eines Nutzers geben, also mit anderen Bestandsdaten wie der Telefonnummer vergleichbar sind, aber nur vorübergehend vergeben werden, so dass ihr Rückbezug auf den Inhaber nur unter Verwendung von Verkehrsdaten ermittelt werden kann. Wegen dieses Rückbezuges ordnet das Bundesverfassungsgericht auch die dynamischen IP-Adressen dem Schutzbereich des Art. 10 Abs. 1 GG zu. [2]

Das zu beurteilende Gesetz betrifft ausschließlich die Speicherung und Beauskunftung von Verkehrsdaten und ist daher am Prüfungsmaßstab des Art. 10 Abs. 1 GG zu messen.

1.1.2 Schutzbereich des Art. 10 Abs. 1 GG

Art. 10 Abs. 1 GG schützt die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs vor einer Kenntnisnahme durch die öffentliche Gewalt. Hiervon sind nicht nur der Inhalt der Kommunikation, sondern auch die äußeren Umstände derselben, wer hat wann, mit wem, von wo und unter Benutzung welcher Medien kommuniziert, betroffen. [3]

Der Schutzbereich "...erstreckt sich auch auf die Informations- und Datenverarbeitungsprozesse, die sich an die Kenntnisnahme von geschützten Kommunikationsvorgängen anschließen, und auf den Gebrauch, der von den erlangten Kenntnissen gemacht wird (vgl. BVerfGE 100, 313 <359>) " [4]

1.1.3. Schranken

Einschränkungen stehen gemäß Art. 10 Abs. 2 S. 1 GG unter Gesetzesvorbehalt und

1 BVerfG Beschl. v. 24.01.2012 - 1 BvR 1299/05 – Ls. 1; diese und alle weiteren Entscheidungen des Bundesverfassungsgerichts zitiert nach http://www.bundesverfassungsgericht.de
2 BVerfG aaO Ls. 1 und Rn. 116
3 BVerfG U. v. 02.03.2010 - 1 BvR 256/08 u.a. - Rn 189; st. Rspr., vgl. die dortigen Nachweise
4 BVerfG aaO Rn. 190

müssen darüberhinaus verhältnismäßig sein.

Bei der Verhältnismäßigkeitsprüfung ist das BVerfG in seinem Urteil vom 02.03.2010 von der grundsätzlichen Eignung und Erforderlichkeit der Vorratsdatenspeicherung für den angestrebten Zweck ausgegangen.[5]

Es hat den Eingriff, der in der Speicherung der Kommunikationsverbindungsdaten liegt, wegen der seiner Streubreite, des Fehlens jeglichen Bezuges der betroffenen Bürger zu einer Straftat und der Aussagekraft dieser Daten für besonders schwerwiegend gehalten.[6]

Das Bundesverfassungsgericht hat hieran anknüpfend die Vorratsdatenspeicherung nur als Ausnahmemaßnahme zugelassen, sie dürfe insbesondere nicht im Zusammenspiel mit anderen Dateien zu einer Rekonstruierbarkeit "...praktisch aller Aktivitäten der Bürger führen." [7]

Der Spielraum des Gesetzgebers für weitere Datenspeicherungspflichten sei daher und im Hinblick auf die schon bestehenden Datensammlungen erheblich eingeschränkt und auch nicht durch europäische Regelungen erweiterbar, da es zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland gehöre, die Freiheitswahrnehmungen der Bürger nicht total zu erfassen und zu registrieren.[8]

Die Verhältnismäßigkeit der Vorratsdatenspeicherung im TKG ist nach Auffassung des Bundesverfassungsgerichts nur zu wahren, wenn besonders strenge Sicherheitmaßnahmen für die Speicherung und Weiterverarbeitung der Daten Platz greifen, wobei dies vom Gesetzgeber hinreichend normenklar selbst angeordnet werden müsse.[9]

1.2. Europäische Grundrechte als Prüfungsmaßstab

1.2.1 Anwendbarkeit der Grundrechtecharta

Der Gesetzentwurf selbst geht von der Anwendbarkeit der Europäischen Grundrechte auf die Regelungsmaterie aus.

Lediglich klarstellend sei hervorgehoben dass die vorliegenden Regelungen zur Datenspeicherung und -verarbeitung unter den Anwendungsbereich der Richtlinie 95/46 EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr sowie der Richtlinie 2002/58 EG (Datenschutzrichtlinie für elektronische Kommunikation) fallen.[10]

Nach der Entscheidung in der Rechtssache C-617/10 (Åkerberg Fransson) gilt die Grundrechtecharta der EU (EuGRCh) auch für das Verhältnis der EU-Bürger zu einem Mitgliedsstaat, wenn eine nationale Rechtsvorschrift in den Geltungsbereich des Unionsrechts fällt,[11] vgl. Art. 51 Abs. 1 EuGRCh.

---

5 BVerfG aaO Rn. 207f.
6 BVerfG aaO, Rn. 210f.
7 BVerfG aaO, Rn. 218
8 BVerfG ebenda
9 BVerfG aaO, Ls. 2, 4 und 5 und Rn. 220ff.
10 Vgl. EUGH, Urteil vom 08.04.2014, Rs. C-293/12 und C-594/12, Rn. 4-10 (diese und alle weiteren Entscheidungen des EUGH zitiert nach: http://eur-lex.europa.eu
11 EUGH, Urteil vom 26.02.2013, RS 617/10 Rn. 17-23; zur Abgrenzung vgl. BVerfG, Urteil vom

1.2.2 Art. 7 EuGRCh - Achtung des Privatlebens und Art. 8 EuGRCh – Schutz personenbezogener Daten

Der EUGH erklärte in seinem Urteil vom 08.04.2014 die Richtlinie 2006/24 (Vorratsdatenspeicherungsrichtlinie) für nichtig. Er bejaht sowohl einen Eingriff in das Grundrecht aus Art. 7 EuGRCh als auch aus Art. 8 EuGRCh, verneint trotz des besonders schwerwiegenden Charakters des Eingriffs eine Verletzung der Wesensgehaltsgarantie, bejaht das Vorliegen einer dem Gemeinwohl dienenden Zielsetzung und prüft sodann die Verhältnismäßigkeit des Eingriffs.[12] Für die Zwecke dieser Stellungnahme braucht zwischen den unterschiedlichen Schutzbereichen nicht differenziert zu werden.

1.2.3 Verhältnismäßigkeit des Eingriffs

Der EUGH bejaht die Eignung der Vorratsdatenspeicherung zur Bekämpfung schwerer Kriminalität,[13] verneint dagegen die Erforderlichkeit.[14]

Hierzu führt der EUGH aus, dass selbst die Bekämpfung schwerer Kriminalität für sich genommen die Erforderlichkeit einer Speicherungsmaßnahme, wie sie die Richtlinie zur Vorratsdatenspeicherung vorsah, nicht rechtfertigen kann.[15]

Der Schutz personenbezogener Daten verlangt nach ständiger Rechtsprechung des EUGH, dass sich die Ausnahmen auf das absolut Notwendige beschränken.[16]

Dies verneint der EUGH zum einen, weil die Richtlinie sich auf sämtliche Kommunikationsdaten erstreckte, ohne anhand des Zieles der Bekämpfung schwerer Straftaten eine Differenzierung, Einschränkung oder Ausnahmen vorzunehmen. Insbesondere könnten die gespeicherten Daten sich auf Personen beziehen, die in keinerlei Zusammenhang mit schweren Straftaten stünden. Ferner nehme die Richtlinie die Berufsgeheimnisträger nicht von ihrem Anwendungsbereich aus.[17]

Zum anderen lege die Richtlinie keinen Zusammenhang zwischen den zu speichernden Daten und einer Bedrohung der öffentlichen Sicherheit fest. Insbesondere enthalte die Richtlinie keine Beschränkung auf die Daten eines bestimmten Zeitraumes, eines bestimmten geografischen Gebietes und/oder von Personen, die in eine schwere Straftat verwickelt sein, bzw. deren Daten zur Aufklärung von Straftaten beitragen könnten.[18]

Weitere vom EUGH aufgeführten Unwirksamkeitsgründe betreffen fehlende Einschränkungen der Richtlinie betreffend die Zugangsberechtigung zu den Daten in materieller und personeller Hinsicht und die Unverhätnismäßigkeit der Speicherfrist.[19]

Hinsichtlich der Datensicherheit rügt der EUGH das Fehlen klarer und strikter Vorkehrungen für den Schutz und die Sicherheit der Daten zur Gewährleistung von

---

24.04.2013, 1 BvR 1215/07, Rn. 88-91

12 Vgl. EUGH, Urteil vom 08.04.2014, Rs. C-293/12 und C-594/12, Rn. 32-43

13 EUGH aaO, Rn. 59f.

14 EUGH aaO, Rn. 51-59

15 EUGH aaO, Rn. 51

16 EUGH aaO, Rn. 52 mit weiteren Nachweisen

17 EUGH aaO, Rn. 57f.

18 EUGH aaO, Rn.

19 EUGH aaO, Rn. 60-65

deren Unversehrtheit und Vertraulichkeit.[20]

Schließlich gewährleiste die Richtlinie nicht, dass die Telekommunikationsanbieter ein besonders hohes Sicherheitsniveau für die Speicherung und Verarbeitung der Daten ohne Kostenerwägungen realisieren müssten. Auch die unwiderrufliche Datenvernichtung nach Ablauf der Spericherungsfrist sei nicht gewährleistet und der Schutz der Daten durch Speicherung auf dem Unionsgebiet einschließlich der Überwachung durch eine unabhängige Stelle seien nicht vorgesehen.[21]

2. Anwendung der Prüfungsmaßstäbe der vorerwähnten Rechtsprechung auf den Gesetzentwurf

2.1 Speicherpflichten - §§ 113 a und b TKG

Die verfassungsrechtlichen Bedenken meinerseits richten zunächst sich gegen die uneingeschränkte Anordnung der Speicherpflicht.

2.1.1 Überwachungsgesamtrechnung

Das Bundesverfassungsgericht hat bereits im Jahre 2010 die Anordnung einer Vorratsdatenspeicherung als nur ausnahmsweise zulässig bezeichnet und den Gesetzgeber verpflichtet bei der Anordnung weiterer Speicherpflichten äußerste Zurückhaltung zu üben. Heute, mehr als fünf Jahre später, ist die Situation umgekehrt. Es ist zu überprüfen, ob die Anordnung der umfassenden Kommunikations- und Bewegungsüberwachung angesichts der bereits vorhandenen Datensammlungen gegen das Übermaßverbot verstößt. Hierbei sind insbesondere die tatsächlichen Entwicklungen neben der Fortschreibung der durch Gesetz angeordneten Datensammlungen zu berücksichtigen. Allgemein wird dies unter dem Stichwort “Überwachungsgesamtrechnung" behandelt.[22]

Hierzu würde eine Überprüfung der vorhandenen Anfragen – etwa im Bereich der Bestandsdatenabfragen, der Kontenabfragen, der Funkzellenabfragen- als auch die grundsätzlich angeordneten Kombinationsdateien – vergleiche "Anti-Terrordatei“ – gehören. Zu so einer Bestandsaufnahme gehört auch die Betrachtung erweiterter polizeilicher Überwachungsbefugnisse. In eine Überwachungsgesamtrechnung gehören auch die außerhalb öffentlich-rechtlicher Anordnung vorhandenen privaten Datensammlungen, die im Wege der allgemeinen Ermittlungsbefugnisse der Strafverfolgungsbehörden grundsätzlich der Beschlagnahme unterliegen.

Der Gesetzentwurf hat im bisherigen Verfahren die Überwachungsgesamtrechnung nicht thematisiert. Hält man aber, wie das Bundesverfassungsgericht, die Gesamtheit der vorhandenen Datensammlungen für eine verfassungsrechtlich zu beachtende Gefahr, weil die unbeobachtete Ausübung der Freiheitsrechte zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland gehört und die Möglichkeiten der Erzeugung von Persönlichkeitsprofilen bereits anhand der vorhandenen Datensammlungen nicht mehr fern liegt, so steht die Einbindung der geplanten Speicherung von Kommunikationsdaten gerade unter dem aufgezeigten Gesichtspunkt der Verhältnismäßigkeit auf dem Prüfstand.

---

20 EUGH aaO, Rn. 66

21 EUGH aaO, Rn. 67f.

22 Vgl. Roßnagel, die “Überwachungs-Gesamtrechnung” - Das BVerfG und die Vorratsdatenspeicherung, in: NJW 2010, 1238

Meines Erachtens führt eine solche Prüfung bereits zu dem Ergebnis, dass die geplante Speicherung von Kommunikationsdaten bei einer Gesamtbetrachtung der vorhandenen Datensammlungen in tatsächlicher und rechtlicher Hinsicht, unverhältnismäßig ist. Der Gesetzgeber muss sich mit diesem Bedenken auseinandersetzen und einen entsprechenden Abwägungsprozess einleiten. Hierbei sind auch die weiteren Planungen, wie das geplante Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes, sowie sämtliche Ansammlungen von Passagierdaten in die Erwägung mit einzubeziehen.

Entsprechend hat die EU-Kommission in ihrem Schreiben an die Bundesregierung gerügt: "Die faktischen Elemente und Nachweise (d. h. statistische Daten oder Studien), die der Bewertung zugrunde liegen, dass eine Speicherfrist von 4 bzw. 10 Wochen unbedingt notwendig ist, um das verfolgte Ziel des Allgemeininteresses zu erreichen, sollten bereitgestellt und erläutert werden."

2.1.2 Ausnahmen für Berufsgeheimnisträger

Die Überwachung der Kommunikation eines Strafverteidigers mit seinem Mandanten ist bereits von Verfassungs wegen unstatthaft.[23]

Entsprechend gilt dies für sämtliche Berufsgeheimnisträger. Hierbei genügt das in § 100g Absatz 4 StPO-E angeordnete Verwertungsverbot der Daten von Berufsgeheimnisträgern bereits deshalb nicht, weil es die Übermittlung dieser Daten im Strafverfahren zulässt und die Übermittlung und Verwertung für Zwecke der Gefahrenabwehr nicht sperrt, obwohl die Anordnung der Speicherung und Auskunftsberechtigung der Telekommunikationsanbieter Eingriffe in das Grundrecht aus Art. 10 Abs. 1 GG darstellen und zur Gesetzgebungskompetenz des Bundes gehören.[24]

Verfassungsrechtlich kann dieser Mangel nur durch ein Speicherungsverbot, wie es in § 99 Abs. 6 TKG-E für die anonymen Beratungsstellen geregelt ist, behoben werden. Dem stehen insbesondere keine unüberwindbaren technischen Hürden entgegen, weil die Berufsgeheimnisträger verkammert sind und die Berufskammern bereits elektronische Verzeichnisse der Kommunikationsanschlüsse der Berufsgeheimnisträger führen. Für die nicht verkammerten Personen wäre ein entsprechendes Verzeichnis einzurichten.

Europarechtlich verstößt die Speicherung der Daten der Berufsgeheimnisträger gegen das Gebot der Eingriffsbeschränkung auf das absolut Notwendige, wie oben dargestellt.[25]

2.1.3 Beschränkung auf das absolut Notwendige

Schärfer als das Bundesverfassungsgericht hat der EUGH bereits bei der Datenspeicherungsanordnung der nichtigen Richtlinie 24/2006 gerügt, dass sie sich nicht auf das absolut Notwendige beschränke.[26]

---

23 Vgl. im Einzelnen BVerfG, 3. Kammer des Zweiten Senats, NJW 2007, 2749 ff.
24 Vgl. BVerfG aaO, Rn. 194 und 201f.
25 Vgl. FN 17 und Punkt 1.2.3
26 ebenda

Dieser Mangel besteht auch bei der Speicherungsanordnung nach §§ 113a und 113b TKG-E.

Es werden keine anlaß-, gebiets, zeitraum- oder personenbezogenen Einschränkungen vorgesehen. Damit dürfte aus europarechtlicher Sicht ein Verstoß gegen das Verbot der Beschränkung von Grundrechtseingriffen auf das absolut Notwendige vorliegen.

2.2 Übermittlung von Internet-Protokolladressen (IP-Adressen)

Wegen der Knappheit von Adressen im IP-IV-Adressbereich gehen die Provider zunehmend dazu über, eine IP-Adresse für mehrere Nutzer zu vergeben. Dies erfolgt durch die Zuweisung eines Ports für eine bestimmte Internetanwendung des Nutzers. Der Port hat die Funktion einer Sub-Adresse.

Diesen Sachverhalt hat das Gesetz nicht erfasst, wenn es anordnet, dass die dem Teilnehmer zugeordnete Internetadresse, eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt und die dem Teilnehmer zugewiesene IP-Adresse sowie Beginn und Ende von deren Nutzung zu speichern seien, § 113b Abs. 3 TKG-E.

Die vom Gesetzgeber gewollte Identifizierung des Internetnutzers ist nur unter gleichzeitiger Speicherung der genutzten Ports und der millisekundengenauen Aufzeichnung der Nutzung derselben technisch möglich. Angesichts der Zuweisung einer Internetadresse an bis zu 200 Nutzer dürfte ein außerordentlich erheblicher technischer Aufwand für die Speicherpflichtigen anfallen.

Das Gesetz ist jedenfalls insofern uneindeutig und damit unbestimmt. Die Verlagerung der Verpflichtung zur Datenspeicherung auf eine technische Umsetzungsrichtlinie dürfte verfassungsrechtlich nicht zulässig sein.

Hinzu kommt, dass der Port auch Details zum genutzten Dienst verrät, so gibt der Port z.B. Auskunft darüber, was der Nutzer „von der anderen Seite will“ - konkret ist so z.B. in der Regel die Nutzung verschiedener Dienste an der Port-Nummern erkennbar und in Folge, mit wem kommuniziert wurde.

Berlin, den 21.09.2015
Meinhard Starostik - Rechtsanwalt

DEUTSCHER BUNDESTAG

AUSSCHUSS FÜR RECHT UND VERBRAUCHERSCHUTZ

ÖFFENTLICHE ANHÖRUNG

ZUM

ENTWURF EINES GESETZES ZUR EINFÜHRUNG EINER SPEICHERPFLICHT UND EINER HÖCHSTSPEICHERFRIST FÜR VERKEHRSDATEN

STELLUNGNAHME

FRANK THIEDE

KRIMINALDIREKTOR

LEITER DER BERATUNGSSTELLE FÜR POLIZEIPRAKTISCHE RECHTSFRAGEN UND RECHTSPOLITIK, BUNDESKRIMINALAMT WIESBADEN

ORT:	BERLIN PAUL-LÖBE-HAUS RAUM 4.900
ZEIT:	21.09. 2015 16:00 UHR

1. Grundsätzliches zum polizeifachlichen Bedarf der anlassbezogenen Verwendung und Bedeutung von Verkehrsdaten

Bei der 2008 in Kraft getretenen (und 2010 vom BVerfG für nichtig erklärten) Regelung der sog. Vorratsdatenspeicherung in §§ 113a ff. TKG und der Befugnis ihrer Abfrage nach § 100g StPO und (2009 in Kraft getretenen Regelung des) § 20m BKAG i.V.m. § 4a BKAG ist dem Fachbereich KI 15 des Bundeskriminalamtes, in dem die Rechtstatsachensammel- und Auswertestelle (RETASAST) zur Bündelung des polizeifachlichen gesetzlichen Änderungsbedarfs geführt wird - von Polizeien des Bundes und der Länder der erkannte gesetzgeberische Regelungsbedarf berichtet worden. Während der polizeifachliche Bedarf der Auskunft über Telekommunikationsverkehrsdaten für eine effektive Ermittlungsarbeit im Bereich der Gefahrenabwehr wie Strafverfolgung unstreitig sein dürfte, war ein zunehmender Verlust von Verkehrsdaten bei zugleich heterogener Speicherpraxis der Betreiber festzustellen, da bei einer Vielzahl unterschiedlichster Geschäftsmodelle eine Speicherung der Daten durch den Betreiber „zu Abrechungszwecken“ nicht erforderlich und damit ggf. auch nicht zulässig wurde. Ohne eine einheitliche Verpflichtung der Betreiber war festzustellen, dass die Daten entweder nicht mehr vorhanden waren oder es vom Zufall abhing, bei welchem Anbieter die Zielperson ihren Vertrag mit welchem Geschäftsmodell geschlossen hat.

Besonders eklatant zeigte sich schon frühzeitig das Defizit bei Auskunftsersuchen zu einer dynamischen IP-Adresse, um anhand der IP mit Zeitstempel den konkreten Nutzer/Anschlussinhaber beim Betreiber zu ermitteln: Auskunftsersuchen nach §§ 161, 163 StPO i.V.m. § 113 TKG, später 2013 aufgrund der Gesetzesänderung nach dem dann einschlägigen § 100j StPO i.V.m. § 113 TKG, gingen und gehen wieder ohne Vorratsdatenspeicherung in den meisten Fällen ins Leere, da der Betreiber intern eine Zuordnung zu einem Anschluss zu einem bestimmten Zeitpunkt gar nicht (mehr) vornehmen konnte und kann, da die Verbindungsdaten – etwa mangels Abrechnungsinteresse – nicht mehr gespeichert waren/sind. Gerade bei IP-Adressen zeigt sich heute wie damals, dass ohne Zuordnung zu einem Anschluss oftmals schon der erste und meist einzige Ermittlungsansatz fehlt.

Dieser defizitäre Zustand vor 2008 wurde mit der Einführung der o.g. Regelungen zunächst geheilt, fiel dann aber mit der Entscheidung des BVerfG 2010 auf den alten Zustand zurück

und verschärfte sich dabei zusätzlich, da etwa Flatrate-Angebote mittlerweile fast „Standard“ geworden waren.

Umso wichtiger war es für die deutsche Polizei, den Gesetzgeber im Interesse einer möglichst zeitnahen wie verfassungskonformen Regelung der Vorratsdatenspeicherung zu beraten und ihm Rechtstatsachen zur Verfügung zu stellen. Das hat das Bundeskriminalamt gemeinsam mit den Polizeien von Bund und Ländern umgehend nach der Entscheidung des BVerfG 2010 zu einer bislang einzigartigen wie umfangreichen Erhebung veranlasst. Die 2011/2012 abgeschlossene Erhebung der Rechtstatsachensammel- und Auswertestelle (RETASAST) des BKA in Sachen Mindestspeicherfristen enthält die Darstellung der Ermittlungsdefizite ohne Mindestspeicherfristen nach dem BVerfG-Urteil vom 02.03.2010. Auf den auf der Homepage des BKA (FAQ zum Stichwort „Mindestspeicherfristen“ mit weiteren Erläuterungen) eingestellten Abschlussbericht und Falldarstellungen wird hingewiesen.

Kernaussagen:

- Im Rahmen der BKA Erhebung vom 02.03.2010 bis 26.04.2011 wurden insgesamt Auskunftsersuchen zu 5.082 Anschlüssen gestellt, wovon 84% nicht beauskunftet wurden.
- 83% der nicht beauskunfteten „Negativ“-Fälle erfolgten zur Strafverfolgung in den Bereichen (Computer- und Subventions-) Betrug (45%) und Kinderpornographie (39%).
- 90% der Auskunftsersuchen lediglich zu einer jeweils bereits vorliegenden IP-Adresse (also gerichtet auf die Auskunft über die hinter der IP mit Zeitstempel stehenden Kunden-/Bestandsdaten) wurden in den Bereichen KiPo und Betrug gestellt.
- In 9% der Fälle wurden retrograd Verkehrsdaten angefragt, v.a. Fälle schwerster Kriminalität. Im Bereich der Strafverfolgung konnte in den Fällen einer Nicht-Auskunft die zu Grunde liegende Straftat in 83% der Fälle nicht aufgeklärt werden.
- Die IP ist in fast allen Fällen immer der erste und einzige Ermittlungsansatz.

Das Bundeskriminalamt sieht seine Rolle im Rahmen der Expertenanhörung des Ausschusses primär in der Darlegung des polizeifachlichen Bedarfs der Regelungen. Die dringende Notwendigkeit, die Beauskunftung von retrograd gespeicherten Verkehrsdaten zu

ermöglichen, wird zudem durch die bei den Ländern, der Bundespolizei und im BKA erhobenen und im anliegenden Fallarchiv zusammengetragenen Rechtstatsachen belegt.

2. Anmerkungen zum vorliegenden Gesetzentwurf:

Ohne an dieser Stelle auf alle Vorschriften des Gesetzentwurfs einzugehen, können aus Sicht des Bundeskriminalamtes zusammenfassen zuvörderst folgende Bewertungen aus polizeifachlicher Sicht vorgenommen werden:

Feststellung Inhaber IP-Adresse

IP-Adresse ist im Bereich Cybercrime häufig der erste und erfolgversprechendste Ermittlungsansatz, um den hinter der vorliegenden IP mit Zeitstempel den Anschlussinhaber zu ermitteln, dem die IP im angegebenen Zeitfenster vom Provider zugewiesen worden. Um diese Zuordnung vornehmen zu können, muss der Provider denknotwendig auf die gespeicherten Verkehrsdaten intern zurückgreifen. Ist das mangels Speicherpflicht nicht möglich, scheitern in der Regel jegliche weiteren Ermittlungen.

Beispiel 1: ***Amok-Drohung***

Wegen eines anonymen Hinweises auf einen möglichen Amoklauf in Hessen wurde in einem Internet-Forum tatsächlich die Ankündigung eines Amoklaufs an einer bestimmten Schule festgestellt. Über die IP zum Eintrag konnte der Provider festgestellt werden. Erste Ermittlungen zur Person des Absenders verliefen jedoch negativ, da der Provider keine retrograden Verbindungsdaten mehr speichert.

Die Person des Absenders/Täters konnte später nur zufällig durch Recherchen über seinen Nickname festgestellt werden, da der Täter in einem anderen Forum mit demselben Nickname angemeldet war und dabei Bruchstücke seines Namens und der Adresse angegeben hatte. Der Täter wurde festgenommen, war geständig und wurde in eine psychiatrische Klinik eingewiesen.

Beim Täter wurde ein hohes Maß an tatsächlicher Amok-Bereitschaft festgestellt. Ort und Datum des Amok-Laufs waren bereits festgelegt. Der Täter hatte bereits erfolglos versucht, sich eine "scharfe" Schusswaffe zu verschaffen. Wegen der fehlenden Verkehrsdaten konnte die Gefahr erst zu einem späteren Zeitpunkt beseitigt und die Tat nur wesentlich erschwert aufgeklärt werden.

Beispiel 2: ***Ermittlungen im Darknet zu Kinderpornographie***

Im Juli 2013 wurde in einer konzertierten Aktion eine der zentralen Plattformen zur Verbreitung von Kinderpornographie abgeschaltet. Auf der Plattform waren insgesamt 2 Millionen kinderpornographische Bilder. Mit Abschalten der Plattform wurden die Online-Aktivitäten von ca. 25.000 Pädophilen unterbrochen, die Szene konnte deutlich verunsichert werden.

Insgesamt wurden 60 europäische IP-Adressen identifiziert, darunter 15 Nutzer mit deutschen IP-Adressen. Zu 13 Adressen konnten Bestandsdaten erhoben und die Nutzer identifiziert werden, in den beiden anderen Fällen waren trotz sofortiger Anfrage bei den entsprechenden Providern aufgrund fehlender Mindestspeicherfristen keine Daten mehr verfügbar.

Das bedeutet im Ergebnis: Trotz aufwendiger Sondervereinbarungen mit unseren internationalen Partnern FBI und Europol, die deutsche IP-Adressen sofort übermittelt haben – alle anderen an der Operation beteiligten Länder erhielten die IP-Adressen ihrer Länder am Ende der Operation gesammelt – und trotz der sofortigen Bearbeitung der Daten (in 24/7 Schichtdiensten), konnte in diesen beiden Fällen die IP-Adresse keinem Nutzer, keiner real existierenden Person zugeordnet werden.

Über die Sichtung der verschiedenen Boards der Plattform nach deren Abschaltung (retrograd) konnten ca. 200 weitere mutmaßlich deutsche Nutzer festgestellt werden. Zu diesen Usern liegen lediglich Nick-Name und E-Mail-Adressen, keine IP-Adressen vor. Eine Identifizierung ist so nur in wenigen Ausnahmefällen möglich.

- Die im Gesetzentwurf vorgesehene Speicherpflicht – wenn auch nur für 10 Wochen – vermeidet immerhin, dass die Ermittlungen, wie der Bericht des BKA belegt, in vielen Fällen andernfalls scheitern würden.

Funkzellenauswertung

Die Erhebung eingeloggter Mobiltelefone in bestimmter Funkzelle zu bestimmten Zeitpunkt (Ort-Zeit-Datum) ist für die Polizeiarbeit von zentraler Bedeutung, um etwa bei Tatserien Kreuztreffer zu ermitteln und so Ermittlungsansätze erst zu generieren oder bereits identifizierten Tätern/Tatverdächtigen die Tat nachzuweisen.

Beispiel 3: ***Autobahnschütze***

Über 760-mal schoss der Täter deutschlandweit aus seinem Lkw auf Transporter, Pkws und Gebäude. Eine Pkw-Fahrerin wurde schwer verletzt; Lkw-Fahrer hatten schlicht Glück, wenn das Geschoss das Seitenfenster durchschlug und um Haaresbreite den Kopf verfehlte. Tatorte waren überwiegend Autobahnen deutschlandweit.

Die Mobilfunkdaten des Verdächtigen haben wir mit den Funkzellen mutmaßlicher Tatörtlichkeiten und Tatzeiten auf Hunderten von Kilometern deutscher Autobahnen abgeglichen. Dadurch verdichtete sich der Verdacht zum Beweis. Wir konnten weitestgehend Übereinstimmungen mit den relevanten Tatstrecken und Tatzeiten feststellen. Dieser Abgleich mit Verkehrsdaten aus Funkzellen war besonders wichtig, weil wir außerhalb von Autobahnen keine Kennzeichenlesegeräte aufstellen konnten. Insbesondere bei den außerhalb von Autobahnen abgegebenen Schüssen konnten nun örtliche Bezüge auch zu diesen Tatorten hergestellt werden.

Beispiel 4: ***Enkeltrick***

Zunehmend geraten auch ältere Menschen in das Visier von Kriminellen. Ein Beispiel ist der sog. Enkeltrick, bei dem die Täter vorher ausfindig gemachte ältere Menschen anrufen und ihnen vorgaukeln, in einem verwandtschaftlichen Verhältnis zu stehen und dringend Geld zu benötigen. Diese Form des gewerbsmäßigen Betrugs hat häufig schwerwiegende finanzielle, seelische und gesundheitliche Folgen für die Opfer. Um die Täter ermitteln zu können, ist es nötig zu wissen, wer das Opfer von wo aus angerufen hat, wer vom Täter zur Geldabholung

beauftragt wurde und wer das Geld wo abgeholt hat. Hierzu sind Verkehrsdaten als Ermittlungsansatz zwingend erforderlich.

- Explizite Regelungen der Erhebung von Funkzellendaten im Gesetzentwurf der Bundesregierung zur Einführung einer Speicherpflicht und einer Höchstspeicherpflicht für Verkehrsdaten finden sich in §§ 100g Abs. 3, 101a Abs. 1 S. 2 StPO-E.

  § 100g StPO-E differenziert in Abs. 1 und Abs. 2 grundsätzlich zwischen dem Zugriff auf Daten gem. § 96 TKG (Daten, welche die TK-Unternehmen zu geschäftlichen Zwecken zu speichern befugt sind) und dem Zugriff auf die sogenannten Vorratsdaten, die nach § 113b TKG-E verpflichtend zu speichern sind. Für letztere finden sich in § 100g Abs. 2 StPO-E weitaus strengere Voraussetzungen der Datenerhebung, insbesondere muss ein Anfangsverdacht bezüglich einer besonders schweren Straftat aus dem angeführten Straftatenkatalog vorliegen.

  Auch § 100g Abs. 3 StPO-E, der explizite Regelungen zur Funkzellenabfrage enthält, knüpft an diese Differenzierung an. Je nachdem ob Daten gem. § 96 TKG oder solche nach § 113b TKG-E erhoben werden sollen, gelten unterschiedliche Voraussetzungen:

- Die Frist von vier Wochen zur retrograden Erhebung von auf Vorrat gespeicherten Daten liegt deutlich unter den Erwartungen des Bundeskriminalamts. Ob und ggf. wie schwer sich das Defizit für die polizeiliche Praxis auswirkt, wird sich in Zukunft erweisen.

  Ferner kommt künftig eine Anfrage – ungeachtet der kurzen Frist – bei einigen Straftatbeständen, bei denen ein Rückgriff auf Standort- oder (ohne Abrechnungszweck gespeicherte) Funkzellendaten wesentlich ist, schon in Ermangelung der Qualifikation gem. § 100g Abs.2 StPO nicht in Betracht, etwa bei (noch nicht) qualifizierten Fällen des Wohnungs-Einbruchsdiebstahls oder des Computerbetrugs. Sollten sich in der Praxis die befürchteten Defizite zeigen, werden wir berichten.

Retrograde Telekommunikationsdaten

Der Rückgriff auf Verkehrsdaten ist im Zuständigkeitsbereich des BKA etwa zur Erhellung von Netzwerkstrukturen im Bereich Terrorismus und Organisierte Kriminalität elementar. Die Verbindungen von Personen zu kennen, ist auch wichtig, um effektive Gefahrenabwehr zur Verhütung von Straftaten des internationalen Terrorismus (§ 4a BKAG) zu betreiben.

Beispiel 5: ***NSU***

Wegen fehlender Verbindungsdaten bis heute nicht klar, ob alle Kontakte und Verbindungen des Trios bekannt sind, wie der NSU die begangenen Verbrechen logistisch organisierte und ob es weitere Unterstützer oder weitere Zellen gab und gibt, die Anschläge planen.

In 1 658 Fällen wurden Verkehrsdaten bei Providern angefragt. Nur in 113 Fällen (7%) waren bei den Providern noch Daten vorhanden und konnten übermittelt werden.

- Auffällig ist im Gesetzentwurf, dass bei anschlussbezogenen Standortdaten ein Rückgriff auf diese Daten – ungeachtet ihres „Status“ als Abrechnungs- oder Vorratsdaten – nur in einem Zeitraum von vier Wochen und zugleich bei Vorliegen der Voraussetzungen einer Katalogtat nach § 100g Abs.2 StPO-E zulässig ist. Das Bundeskriminalamt wird aufmerksam beobachten, ob und ggf. wie sich Defizite in der polizeilichen Praxis auswirken.

  Dabei weist das Bundeskriminalamt vorsorglich noch einmal darauf hin, dass die von den Polizeien von Bund und Ländern in der o.g. Erhebung für notwendig erachtete gesetzliche Speicherfrist von sechs Monaten (auch für Standortdaten) nicht etwa übermäßig war, sondern vielmehr folgendem Umstand Rechnung trägt: Die polizeiliche Reaktionszeit (vom Eingang der Information bis zur Antragstellung beim Provider) hat nur einen geringen Einfluss auf die erforderliche Mindestspeicherfrist, denn nicht die polizeiliche Reaktionszeit, sondern das „Alter“ der Verkehrsdaten bestimmt den Speicherzeitraum (Beispiel: Spätes Bekanntwerden der Straftat oder lange Dauer der Datenträgerauswertung). Polizei und StA haben meist keinen Einfluss

darauf, wie schnell sie durch Anzeige oder von anderen (ausländischen) Stellen von einem Sachverhalt erfahren und somit Verkehrsdaten anfragen können. D.h. an der polizeilichen Reaktionszeit liegt es nicht: Zwischen dem Zeitpunkt der Kenntniserlangung des BKA über das Vorliegen ermittlungsrelevanter Verkehrsdaten und dem Moment der Stellung des Auskunftsersuchens lagen ausweislich der statistischen Erhebung des BKA in 86% der der Fälle, in denen keine Auskunft erteilt werden konnte, höchstens sieben Tage.

Annex: Einführung eines neuen Straftatbestands der „Datenhehlerei“ im Gesetzentwurf

Die geltende Rechtslage gem. StGB enthält keine Rechtsvorschrift, in der explizit die Strafbarkeit des Weiterverkaufs unerlaubt erlangter Daten unter Strafe gestellt wird. Die Justizministerkonferenz hatte am 13./14.06.2012 die Initiative der Einführung des Straftatbestandes der Datenhehlerei beschlossen. Der bereits seit 2013 vorliegende Gesetzentwurf des Landes Hessen, der sich inhaltlich mit den Forderungen des BKA im Wesentlichen deckt, wurde mit Bundesratsbeschluss vom 14.30.2014 erneut in den Bundestag eingebracht. Inhaltlich sieht dieser Entwurf

- neben der Einführung des Straftatbestands der Datenhehlerei (§ 202d StGB-E)
- auch eine Erhöhung des Strafrahmens des Ausspähens und Abfangens von Daten (§§ 202a, 202b StGB-E)
- Qualifikationstatbestände für Fälle des gewerbs- oder bandenmäßigen Handelns
- eine Versuchsstrafbarkeit

vor.

Für Fälle der gewerbs- oder bandenmäßigen Begehung sollte aus Sicht des BKA zudem das Recht der Telekommunikationsüberwachung in der StPO angepasst werden.

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).