E n t s c h e i d u n g s b e s p r e c h u n g

Vorratsdatenspeicherung im Mehrebenensystem: Die Entscheidung des BVerfG vom 2.3.2010

1. Eine sechsmonatige, vorsorglich anlasslose Speicherung von Telekommunikationsverkehrsdaten durch private Diensteanbieter, wie sie die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 (ABl L 105 vom 13. April 2006, S. 54; im Folgenden: Richtlinie 2006/24/EG) vorsieht, ist mit Art. 10 GG nicht schlechthin unvereinbar; auf einen etwaigen Vorrang dieser Richtlinie kommt es daher nicht an.

2. Der Grundsatz der Verhältnismäßigkeit verlangt, dass die gesetzliche Ausgestaltung einer solchen Datenspeicherung dem besonderen Gewicht des mit der Speicherung verbundenen Grundrechtseingriffs angemessen Rechnung trägt. Erforderlich sind hinreichend anspruchsvolle und normenklare Regelungen hinsichtlich der Datensicherheit, der Datenverwendung, der Transparenz und des Rechtsschutzes.

3. Die Gewährleistung der Datensicherheit sowie die normenklare Begrenzung der Zwecke der möglichen Datenverwendung obliegen als untrennbare Bestandteile der Anordnung der Speicherungsverpflichtung dem Bundesgesetzgeber gemäß Art. 73 Abs. 1 Nr. 7 GG. Demgegenüber richtet sich die Zuständigkeit für die Schaffung der Abrufregelungen selbst sowie für die Ausgestaltung der Transparenz- und Rechtsschutzbestimmungen nach den jeweiligen Sachkompetenzen.

4. Hinsichtlich der Datensicherheit bedarf es Regelungen, die einen besonders hohen Sicherheitsstandard normenklar und verbindlich vorgeben. Es ist jedenfalls dem Grunde nach gesetzlich sicherzustellen, dass sich dieser an dem Entwicklungsstand der Fachdiskussion orientiert, neue Erkenntnisse und Einsichten fortlaufend aufnimmt und nicht unter dem Vorbehalt einer freien Abwägung mit allgemeinen wirtschaftlichen Gesichtspunkten steht.

5. Der Abruf und die unmittelbare Nutzung der Daten sind nur verhältnismäßig, wenn sie überragend wichtigen Aufgaben des Rechtsgüterschutzes dienen. Im Bereich der Strafverfolgung setzt dies einen durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat voraus. Für die Gefahrenabwehr und die Erfüllung der Aufgaben der Nachrichtendienste dürfen sie nur bei Vorliegen tatsächlicher Anhaltspunkte für eine konkrete Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für eine gemeine Gefahr zugelassen werden.

6. Eine nur mittelbare Nutzung der Daten zur Erteilung von Auskünften durch die Telekommunikationsdiensteanbieter über die Inhaber von Internetprotokolladressen ist auch unabhängig von begrenzenden Straftaten- oder Rechtsgüterkatalogen für die Strafverfolgung, Gefahrenabwehr und die Wahrnehmung nachrichtendienstlicher Aufgaben zulässig. Für die Verfolgung von Ordnungswidrigkeiten können solche Auskünfte nur in gesetzlich ausdrücklich benannten Fällen von besonderem Gewicht erlaubt werden. (Amtliche Leitsätze)

GG Art. 10 Abs. 1; AEUV Art. 267; EGRL 24/2006 Art. 1 Abs. 1, Art. 3 Abs. 1, Art. 6; StPO §§ 100a Abs. 1 und 2, 100b Abs. 1 und 2, 100g Abs. 1, 100g Abs. 1 S. 1, 100g Abs. 2 S. 1; TKG vom 21.12.2007 §§ 113a, 113b S. 1 Nr. 1, Nr. 2 und Nr. 3; TKÜNReglG Art. 2

BVerfG, Urt. v. 2.3.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08[1]

A. Einleitung

Mit Urteil vom 2.3.2010 hat der *1. Senat* des Bundesverfassungsgerichts die Regelungen des TKG und der StPO über die Vorratsdatenspeicherung für insgesamt verfassungswidrig und nichtig erklärt und zudem angeordnet, die bisher gespeicherten Daten unverzüglich zu löschen.[2] Er beurteilt die Regelungen allerdings nicht als schlechthin unvereinbar mit den grundrechtlich geschützten Freiheiten der Bürger. Vielmehr formuliert er aus dem Übermaßverbot abgeleitete materielle sowie organisations- und verfahrensrechtliche Anforderungen an die Speicherung, Übermittlung und Verwendung der Daten. Sie beziehen sich vor allem auf die Gewährleistung hinreichender Datensicherheit, auf eine hinreichende Begrenzung der Verwendungszwecke der Daten sowie auf Gesichtspunkte der Transparenz und des Rechtsschutzes. Das Urteil enthält eine Reihe neuer Ausführungen, die auf Grundlagenebene und in sicherheitsrechtlicher Hinsicht über den entschiedenen Fall hinaus von Bedeutung sind.

B. Sachverhalt

Ende 2007 hatte der Bundesgesetzgeber nach erheblichen gesellschaftlichen und parlamentarischen Kontroversen im „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“[3] Regelungen zur anlasslosen Speicherung von Telekommunikationsverkehrsdaten, zur nachfolgenden Übermittlung an unterschiedliche Sicherheitsbehörden und zur Verwendung durch Strafverfolgungsbehörden getroffen. Im Kern wurden die Anbieter öffentlich zugänglicher Telekommunikationsdienste verpflichtet, die bei der Kommunikation anfallenden Daten länger als für eigene Zwecke (also insbesondere für die Abrechnung) erforderlich zu speichern und sie unter bestimmten Voraussetzungen an Sicherheitsbehörden zu übermitteln, die sie dann zwecks Erfüllung ihrer Aufgaben verwenden durften.

[1] BVerfG, Urt. v. 2.3.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, abrufbar unter http://www.bverfg.de, im Folgenden nachgewiesen durch Angabe der Rn. im Text.

[2] Zur vorangegangenen einstweiligen Anordnung BVerfG, Beschl. v. 11.3.2008 – 1 BvR 256/08 = BVerfGE 121, 1.

[3] Vom 21.12.2007, BGBl. I S. 3198.

1. Europarechtlicher Hintergrund: Die EG-Vorratsdatenspeicherungsrichtlinie

Als Mitgliedstaat der Europäischen Union unterliegt die Bundesrepublik Deutschland den Vorgaben der Richtlinie 2006/24/EG[4]. Ziel dieser Richtlinie ist ausweislich des Art. 1 Abs. 1 RiL 2006/24/EG die Harmonisierung der mitgliedstaatlichen Verpflichtungen der Betreiber öffentlicher Kommunikationsnetze oder der Anbieter elektronischer Kommunikationsdienste zur Vorratsspeicherung der anfallenden Daten, damit sichergestellt ist, dass die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von den Mitgliedstaaten bestimmt werden, zur Verfügung stehen. Nach Art. 3 RiL 2006/24/EG müssen die Mitgliedstaaten sicherstellen, dass Netzbetreiber und Diensteanbieter die in Art. 5 Abs. 1 RiL 2006/24/EG bestimmten Daten auf Vorrat speichern. Diese Norm enthält einen umfangreichen Katalog sowohl der Daten über Kommunikationen natürlicher und juristischer Personen als auch der über einzelne Kommunikationen hinaus gespeicherten Daten über die Teilnehmer oder die registrierten Benutzer. Aufgelistet werden je nach Kommunikationsmedium etwa Datum und Uhrzeit des Beginns und Endes eines Kommunikationsvorgangs, die Rufnummern der beteiligten Anschlüsse, zugewiesene Benutzerkennungen oder Namen und Anschriften der Teilnehmer, denen eine Rufnummer, IP-Adresse oder Benutzerkennung zum Zeitpunkt der Nachricht zugewiesen war. Nicht erfasst wird dagegen der Inhalt der Kommunikationen. Art. 5 Abs. 2 RiL 2006/24/EG verbietet ausdrücklich die Vorratsspeicherung solcher Daten, die Aufschluss über den Inhalt einer Kommunikation geben. Zeitlich wird die Mindestspeicherungsdauer grundsätzlich auf sechs Monate, die maximal zulässige, allerdings unter besonderen Umständen noch verlängerbare Speicherungsdauer auf zwei Jahre ab dem Zeitpunkt der Kommunikation festgelegt (Art. 6 RiL 2006/24/EG). Art. 4 und 8 RiL 2006/24/EG geben den Mitgliedstaaten für die Weiterleitung der Daten auf, dafür zu sorgen, dass die gespeicherten Daten sowie alle damit zusammenhängenden erforderlichen Informationen unverzüglich an die zuständigen Behörden weitergeleitet werden können, dies allerdings nur auf deren Anfrage hin und unter weiteren Voraussetzungen, die der jeweilige Mitgliedstaat auf nationaler Ebene festlegt.

In europarechtlicher Hinsicht hat der Europäische Gerichtshof die Richtlinie unter kompetenziellen Aspekten bereits überprüft: Irland hatte Nichtigkeitsklage mit dem Vorbringen erhoben, die Richtlinie sei von der Kompetenz zur Angleichung der Rechts- und Verwaltungsvorschriften bezüglich des Funktionierens des Binnenmarktes (zuvor: Art. 95 EG, jetzt: Art. 114 AEUV) nicht gedeckt. Trotz der Entscheidungen über die Tabakwerbungsrichtlinie[5] und über die Übermittlung von Fluggastdaten in die USA[6] hat der EuGH diese Sicht jedoch nicht geteilt, Art. 95 EG als eine hinreichende Kompetenzgrundlage angesehen und die Richtlinie insoweit nicht als europarechtswidrig beurteilt.[7] Eine Überprüfung unter materiellen Aspekten, namentlich anhand der Maßstäbe der Grundrechte der EU-Charta, steht freilich noch aus. Dem EuGH liegt eine darauf gerichtete Vorlage des irischen High Court in Dublin vor.[8]

2. Beschwerdegegenstand: Die angegriffenen bundesgesetzlichen Regelungen

Auf nationaler Ebene verpflichtete der Bundesgesetzgeber mit der Regelung des § 113a TKG Diensteanbieter dazu, die Verkehrsdaten von Telefondiensten, E-Mail-Diensten und Internetdiensten für die Zeit von sechs Monaten vorsorglich zu speichern. Telekommunikationsdiensteanbieter, die – wie Anonymisierungsdienste – die nach Maßgabe dieser Vorschrift zu speichernden Angaben veränderten, wurden zur Speicherung der ursprünglichen und der neuen Angabe sowie des Zeitpunktes der Umschreibung dieser Angaben verpflichtet (§ 113a Abs. 6 TKG). Nicht zu speichern war der Inhalt der Kommunikation (§ 113a Abs. 8 TKG). § 113b TKG bezeichnete allgemein die Nutzungszwecke, zu denen die Telekommunikationsunternehmen die Daten an Behörden übermitteln dürfen, nämlich die Verfolgung von Straftaten, die Abwehr von erheblichen Gefahren für die öffentliche Sicherheit und die Erfüllung nachrichtendienstlicher Aufgaben. Ferner wurde die mittelbare Nutzung der Daten für Auskünfte nach § 113 Abs. 1 TKG in Form eines Auskunftsanspruchs gegenüber den Diensteanbietern zur Identifizierung von IP-Adressen erlaubt. Behörden sollten danach, wenn sie etwa durch Anzeige oder durch eigene Ermittlungen eine IP-Adresse schon kennen, Auskunft verlangen können, zu welchem Anschlussnehmer die Adresse gehört.

Bundesgesetzlich wurden zugleich strafprozessuale Bestimmungen getroffen. § 100g Abs. 1 Satz 1 StPO gestattete es den Strafverfolgungsbehörden unter Bezugnahme auf § 113a TKG, ohne Wissen des Betroffenen Verkehrsdaten zu erheben, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts eines Beschuldigten erforderlich ist. Dies galt allerdings nur für Straftaten von erheblicher Bedeutung und für mittels Telekommunikation begangene Straftaten. Die Datenerhebungen durften nach § 100g Abs. 2 Satz 1 in Verbindung mit § 100b Abs. 1 Satz 1 und 2 StPO außer bei Gefahr im Verzug nur durch den Richter angeordnet werden. Die richterliche Anordnung ermächtigte die Behörden nicht zu einem Direktzugriff auf die Daten, sondern verpflichtete die Diensteanbieter, diese in einem eigenen Zwischenschritt nach den Maßgaben der Anordnung herauszufiltern und zu übermitteln.

Damit hatten die angegriffenen bundesgesetzlichen Regelungen teils richtlinienumsetzenden, teils richtlinienüberschießenden Charakter. Sie setzten die Richtlinie insbesondere

[4] Vom 15.3.2006, ABl.EG L 105 vom 13.4.2006, S. 54.

[5] EuGH, Urt. v. 5.10.2000 – C-376/98 = NJW 2000, 3701.

[6] EuGH, Urt. v. 30.5.2006 – C-317/04 und C-318/04 = MMR 2006, 527.

[7] EuGH, Urt. v. 10.2.2009 – C-301/06, abrufbar unter http:/curia.europa.eu/de/actu/communiques/cp09/aff/cp090011de.pdf. Dazu *Terhechte*, EuZW 2009, 199; *Gundel*, EuR 2009, 536; *Rossi*, ZJS 2009, 298.

[8] beck-aktuell v. 11.5.2010 (http://beck-aktuell.beck.de).

insoweit um, als den Telekommunikationsdiensteanbietern eine anlasslose Vorratsdatenspeicherung für eine Zeitspanne von sechs Monaten aufgegeben wurde. Sie gingen über die Richtlinie etwa hinsichtlich der Zulassung der Übermittlung auch für gefahrenabwehrbezogene und nachrichtendienstliche Zwecke oder der Verwertung für „Straftaten von erheblicher Bedeutung" hinaus.

C. Zentrale Entscheidungsgründe

1. Zulässigkeitsprobleme: Prüfungskompetenzen des BVerfG im Verhältnis zum EuGH

Das Gericht beurteilt die Verfassungsbeschwerde als insgesamt zulässig. Die Zulässigkeit wird auch bejaht, soweit die angegriffenen Vorschriften in Umsetzung der Richtlinie 2006/24/EG ergangen sind. Die Argumentation des *1. Senats*, die diese Sicht tragen soll, stellt eine erhebliche Abweichung von der bisherigen Rechtsprechung dar.[9]

Den Umfang der eigenen Prüfungskompetenz im Verhältnis zum EuGH hat das BVerfG bislang anhand seiner „Solange"-Rechtsprechung bestimmt.[10] Danach übt das Bundesverfassungsgericht seine Gerichtsbarkeit über die Anwendbarkeit von abgeleitetem Unionsrecht nicht mehr aus, solange die Europäische Union einen wirksamen und dem Grundrechtsschutz des GG im Wesentlichen gleich zu achtenden Schutz der Grundrechte generell gewährleistet. Diese Grundsätze hat das Gericht auf innerstaatliche Rechtsvorschriften zur Umsetzung von Richtlinien erstreckt: „Auch die innerstaatliche Umsetzung von Richtlinien des Gemeinschaftsrechts, die den Mitgliedstaaten keinen Umsetzungsspielraum belassen, sondern zwingende Vorgaben machen, wird vom Bundesverfassungsgericht und den Fachgerichten nicht am Maßstab der Grundrechte des Grundgesetzes gemessen"[11]. Eine innerstaatliche Rechtsvorschrift, die eine Richtlinie in deutsches Recht umsetzt, kann unter diesen Voraussetzungen nur insoweit an den Grundrechten gemessen werden, als der Gesetzgeber Richtlinienspielräume ausfüllt oder Richtlinienvorgaben in eigener Regelungskompetenz konkretisiert.[12] Die Ermittlung des verfassungsgerichtlichen Prüfungsumfangs kann unter diesen Voraussetzungen eine komplexe Auslegung der unionsrechtlichen Vorgaben erforderlich machen. Denn ob und inwieweit ein Umsetzungsakt aufgrund europäischer Rechtsakte zwingend geboten ist, ist nicht immer ohne Weiteres erkennbar. Der damit verbundene Verlust an Rechtsklarheit ist zuweilen beklagt, jedoch überwiegend akzeptiert worden.[13] Bezogen auf die angegriffenen Vorschriften des TKG würde dies bedeuten, dass das BVerfG – solange die Vorratsdatenspeicherungsrichtlinie in Kraft und nicht vom EuGH für nichtig erklärt worden ist – nur den Teil der nationalen Regelungen am Maßstab der Grundrechte zu überprüfen hätte, der nicht durch zwingende Vorgaben der Richtlinie determiniert wird.

Das BVerfG prüft die angegriffenen Vorschriften jedoch vollumfänglich nach. Es misst insbesondere auch die anlasslose Datenspeicherpflicht, die durch die Richtlinie zwingend vorgegeben ist, am Maßstab der Grundrechte. Zur Begründung dient das Argument, einer Prüfung am Maßstab der Grundrechte stehe jedenfalls dann nichts entgegen, wenn der EuGH die Richtlinie im Wege der Vorabentscheidung für nichtig erklären würde.[14] Die Beschwerdeführer machten im Verfassungsbeschwerdeverfahren geltend, dass die Richtlinie 2006/24/EG sowohl die gemeinschaftsrechtlichen Kompetenzvorgaben als auch europäische Grundrechtsverbürgungen verletze, und erstrebten deshalb, ohne dass sie dies angesichts ihrer unmittelbar gegen das Umsetzungsgesetz gerichteten Verfassungsbeschwerden vor den Fachgerichten hätten geltend machen können, eine Vorlage des BVerfG an den EuGH.

Zutreffend ist, dass das BVerfG dann eine vollumfängliche Prüfung am Maßstab der Grundrechte des Grundgesetzes vorzunehmen hat, wenn eine Richtlinie vom EuGH für nichtig erklärt worden ist. Der Hinweis des BVerfG auf eine bloß denkbare Nichtigkeitserklärung im Rahmen eines Vorabentscheidungsverfahrens stützt sich jedoch allein auf eine Unterstellung und bleibt hypothetisch. Näher liegend als dieser Weg wäre die Konsequenz, dem EuGH die Frage vorzulegen, ob die Vorratsdatenspeicherungsrichtlinie gegen europäische Grundrechte verstößt und unwirksam ist. Die Vereinbarkeit der Richtlinie mit europäischen Grundrechten hat der EuGH, anders als die zum Zeitpunkt der verfassungsgerichtlichen Entscheidung bereits beurteilten Kompetenzfragen[15], noch nicht behandelt.

Im Ergebnis wird der Konflikt mit dem EuGH zwar vermieden, weil das BVerfG zu dem Ergebnis kommt, dass eine sechsmonatige, vorsorglich anlasslose Speicherung von Telekommunikationsdaten, wie sie die Richtlinie vorschreibt, mit Art. 10 GG prinzipiell vereinbar ist. Dennoch bleibt der Eindruck, das Gericht habe einer Vorlage an den EuGH unter allen Umständen ausweichen wollen.[16] Auch wirft die Vorgehensweise Fragen auf. Offen bleibt insbesondere, wie das BVerfG verfahren wäre, wenn es zu dem gegenteiligen Ergebnis gekommen wäre, also hinsichtlich des zwingend vorgeschriebenen Teils einen Widerspruch zu Art. 10 GG gesehen hätte. Offen bleibt auch, ob eine unmittelbar gegen ein Umsetzungsgesetz gerichtete Verfassungsbeschwerde nun immer dann zulässig sein soll, wenn ein Beschwerdeführer geltend machen kann, es bestünde die Möglichkeit, dass der EuGH den zugrundeliegenden Rechtsakt für nichtig erklärt. Letzteres erscheint kaum plausibel. Der Honeywell-Beschluss[17] vom Juli dieses Jahres spricht dann auch schon wieder eine andere Sprache. Zwar hat diese Entscheidung ein vermeintliches ultra-vires-Handeln des Gerichtshofs zum

[9] Dazu bereits *Westphal*, EuZW 2010, 494 (497).
[10] BVerfGE 73, 339.
[11] BVerfGE 118, 79; dazu *Cornils*, ZJS 2008, 69 ff.; vgl. auch die vorausgehenden Kammerentscheidungen BVerfG-K, NJW 1990, 974; NVwZ 1993, 883; NJW 2001, 1267; NVwZ 2004, 1346.
[12] *Augsberg*, DÖV 2010, 153 (156).
[13] *Masing*, NJW 2006, 264 (267).
[14] BVerfG, Urt. v. 2.3.2010 – 1 BvR 256/08 u.a., Rn. 182.
[15] S. oben Punkt I.1.
[16] *Wolff*, NVwZ 2010, 751; *Hornung/Schnabel*, DVBl 2010, 824 (829).
[17] BVerfG, Beschl. v. 6.7.2010 – 2 BvR 2661/06.

Gegenstand.[18] Doch dürfte es in der Konsequenz der betont „zurückhaltend und europarechtsfreundlich“[19] ausgeübten Prüfungskompetenz liegen, dass die Frage einer Vereinbarkeit von Sekundärrecht mit europäischen Grundrechten vom EuGH effektiv beantwortet wird, bevor das BVerfG ein deutsches Umsetzungsgesetz einer unvermittelten Prüfung am Maßstab der Grundrechte des GG unterzieht.

2. Begründetheit: Verfassungsrechtliche Grenzen der Vorratsspeicherung von Telekommunikationsdaten

Das Gericht sieht die Verfassungsbeschwerden im Ergebnis als begründet an, da die angegriffenen Vorschriften die Beschwerdeführer in ihrem Grundrecht aus Art. 10 GG verletzten. Ein Verstoß gegen Art. 12 GG wird dagegen verneint.

a) Prüfung anhand der Vorgaben des Art. 10 GG

aa) Eingriff in den Schutzbereich

Mit der Verbürgung der Unverletzlichkeit des Brief- und Fernmeldegeheimnisses schützt Art. 10 I GG die Freiheit und Unverletzlichkeit der auf Vermittlungstechniken und -leistungen angewiesenen Individualkommunikation. Er gewährleistet, so das BVerfG, eine „Privatheit auf Distanz“[20] und reagiert auf die Freiheitsgefährdungen, die durch die Nutzung der Fernmeldetechnik und der Anlagen Dritter entstehen. Historisch und aktuell bezieht er sich vor allem auf die staatlichen Sicherheitsbehörden und beruht auf der Erfahrung, dass der Staat unter Berufung auf seine eigene Sicherheit sowie die Sicherheit seiner Bürger häufig zum Mittel der Überwachung privater Kommunikation gegriffen hat.[21] Dabei stellt die Gewährleistung auf die Benutzung der jeweiligen Vermittlungstechniken und -leistungen als formalen Anknüpfungspunkt ab und erfasst den Übermittlungsvorgang vom Absenden der Nachricht bis zu ihrem Empfang im Herrschaftsbereich des Empfängers.[22] Sie erstreckt sich im Übrigen über die staatliche Kenntnisnahme hinaus auf die sich daran anschließenden Informations- und Datenverarbeitungsprozesse, insbesondere auch auf die Verwendung erlangter Kenntnisse.[23] Ihr Schutz erfasst nicht nur die Inhalte der Kommunikation.[24] Geschützt ist vielmehr auch die Vertraulichkeit der näheren Umstände des Kommunikationsvorgangs. Dazu gehört, ob, wann und wie oft zwischen welchen Personen oder Telekommunikationseinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist.[25]

Im Folgeschritt spricht das Gericht den im TKG festgehaltenen gesetzlichen Verpflichtungen der Kommunikationsunternehmen, Telekommunikationsdaten zu speichern und an staatliche Stellen zu übermitteln, die Qualität eines Eingriffs in Art. 10 GG zu. Es sieht dies, obwohl die Speicherung statt durch den Staat durch private Diensteanbieter erfolgt, nicht als einen mittelbaren Eingriff, sondern als einen unmittelbaren Eingriff in die Rechte der Kommunizierenden an.[26] Die Diensteanbieter würden, ohne dass ihnen insoweit ein Handlungsspielraum verbleibe, allein als Hilfspersonen für die Aufgabenerfüllung durch staatliche Behörden in Anspruch genommen, so dass die Speicherung der Daten rechtlich dem Gesetzgeber als unmittelbarer Eingriff in Art. 10 Abs. 1 GG zuzurechnen sei (Rn. 193). Praxisrelevant sind die Ausführungen des Gerichts hinsichtlich der den Internetzugang betreffenden Daten. Da Art. 10 Abs. 1 GG nur die Individual-, nicht auch die Massenkommunikation schützt, muss man bei der internetvermittelten Kommunikation den Anwendungsbereich dieser Gewährleistung gegen Art. 5 Abs. 1 S. 2 GG abgrenzen.[27] Art. 10 Abs. 1 GG greift jedoch, solange der Charakter der Kommunikation im Netz nicht erkennbar ist, weil – so das Gericht – eine Unterscheidung zwischen Individual- und Massenkommunikation ohne eine der Schutzfunktion des Grundrechts zuwiderlaufende Anknüpfung an den Inhalt der jeweils übermittelten Information nicht möglich ist (Rn. 192).

bb) Verfassungsmäßigkeit der angegriffenen Regelungen

(1) Die vorsorglich anlasslose Speicherung

Das Problem, dass die von den angegriffenen Regelungen des TKG erfassten Daten anlasslos für sechs Monate von den Diensteanbietern gespeichert werden, erörtert das Gericht im Rahmen der Verhältnismäßigkeitsprüfung. Es grenzt die zu beurteilende Konstellation gegen das im Volkszählungsurteil formulierte strikte Verbot einer Speicherung „von personenbezogenen Daten auf Vorrat zu unbestimmten und noch nicht bestimmbaren Zwecken“ ab (Rn. 206).[28] Zwecks Abgrenzung beschreibt es sie als „vorsorglich anlasslose Speicherung von Telekommunikationsverkehrsdaten zur späteren anlassbezogenen Übermittlung an die für die Strafverfolgung oder Gefahrenabwehr zuständigen Behörden beziehungsweise an die Nachrichtendienste“ (Rn. 207). Es hält sie für nicht schlecht-

[18] Anders als in dem Urteil zur Vorratsdatenspeicherung geht es in diesem Beschluss also nicht um die Grundrechtskonformität von abgeleitetem Unionsrecht.

[19] BVerfG, Beschl. v. 6.7.2010 – 2 BvR 2661/06, Rn. 59 (zitiert nach juris).

[20] BVerfGE 115, 166 (182); BVerfG-K NJW 2007, 351 (356); *Gusy*, in: v. Mangoldt/Klein/Starck (Hrsg.), GG I, 6. Aufl. 2010, Art. 10 Rn. 19.

[21] So BVerfGE 85, 386 (396).

[22] Zu Zuordnungsproblemen im Bereich der Telekommunikation BVerfGE 115, 166 (185 ff.); *M. Baldus*, in: Epping/Hillgruber (Hrsg.), GG, 2009, Art. 10 Rn. 10.

[23] Grundlegend BVerfGE 100, 313 (359).

[24] Dabei kommt es nicht darauf an, ob die Kommunikationen privaten oder anderen, etwa geschäftlichen oder politischen, Inhalts sind, s. z.B. BVerfGE 100, 313 (358).

[25] BVerfGE 67, 157 (172); 85, 386 (396); 107, 299 (329 ff.).

[26] Zur Problematik faktischer und mittelbarer Beeinträchtigungen *Albers*, DVBl 1996, 233 ff.; *Cornils*, in: Detterbeck (Hrsg.), Festschrift für Herbert Bethge zum 70. Geburtstag, 2009, S. 137 ff.

[27] Zur Abgrenzung gegen das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG vgl. etwa BVerfGE 115, 166 (185 ff.).

[28] Vgl. BVerfGE 65, 1 (46 f.); außerdem 100, 313 (360).

hin unvereinbar mit Art. 10 GG, allerdings für nur ausnahmsweise und unter besonders strengen Anforderungen zulässig.

In der Abwägung stuft es die Speicherung zunächst als einen besonders schweren Eingriff ein. Zu den für diese Einstufung maßgeblichen Kriterien gehören die Anlasslosigkeit und der Umfang der Speicherung sowie die weitreichende Aussagekraft der gespeicherten Daten, die auch ohne Erfassung des Kommunikationsinhalts „bis in die Intimsphäre hineinreichende inhaltliche Rückschlüsse" auf die individuelle Lebensführung zuließen. Besonderes Gewicht erhalte der mit der Datenspeicherung verbundene Eingriff auch dadurch, dass die Betroffenen weder die Speicherung noch die vorgesehene Verwendung unmittelbar bemerken, so dass leicht „ein diffus bedrohliches Gefühl des Beobachtetseins" (Rn. 212) entstehen könne. Den Aspekt, dass „Vertrauen" ein für die unbefangene Grundrechtsausübung zentraler Gesichtspunkt ist, hatte das Gericht bereits in seiner Entscheidung zur Online-Durchsuchung hervorgehoben.[29] Die grundrechtliche Freiheitssphäre büßt ein erhebliches Maß ihres Wertes ein, wenn die unbefangene Wahrnehmung des Grundrechts beeinträchtigt wird.

Trotz des Gewichts des Eingriffs hält das Gericht die anlasslose Speicherung dann freilich für verfassungsrechtlich nicht schlechthin verboten. Maßgeblich für die Rechtfertigungsfähigkeit ist – neben der Aussparung der Kommunikationsinhalte – die Ausgestaltung. Die anlasslose Speicherung erfolgt nicht direkt durch den Staat, sondern durch eine Verpflichtung der privaten Diensteanbieter. Die Daten werden damit bei der Speicherung selbst noch nicht zusammengeführt, sondern bleiben verteilt auf viele Einzelunternehmen. Der Abruf der Daten seitens staatlicher Stellen erfolgt erst in einem zweiten Schritt und nunmehr anlassbezogen nach rechtlich näher festgelegten Kriterien. Die Trennung von Speicherung und Abruf und deren jeweilige Ausgestaltung sind somit Kernpunkt der gerichtlichen Argumentation: „Die Ausgestaltung der zum Abruf und zur weiteren Verwendung der gespeicherten Daten ermächtigenden Bestimmungen kann dabei sicherstellen, dass die Speicherung nicht zu unbestimmten oder noch nicht bestimmbaren Zwecken erfolgt." (Rn. 214).

Das seit dem Volkszählungsurteil und auch in der hier besprochenen Entscheidung (Rn. 206 und 213) hervorgehobene strikte Verbot der Sammlung personenbezogener Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken wird damit allerdings erheblich aufgeweicht. Denn es verlangt nicht allein eine Bestimmbarkeit der Zwecke, sondern auch die Erforderlichkeit der Daten für die jeweiligen Zwecke.[30] Eine Zweckfestlegung liefe ohne das Korrelat der Erforderlichkeit leer. Die Erforderlichkeit der Daten für präventive oder strafprozessuale Zwecke steht zum Zeitpunkt der Speicherung gerade nicht fest. Die Diensteanbieter halten die Daten nur für den Fall vor, dass sie sich zukünftig noch als erforderlich erweisen. Das aber ist denkbar ungewiss. Zwar ist nicht jede vorsorgliche Speicherung verfassungswidrig. Die hier in Rede stehenden Speicherpflichten zeichnen sich jedoch dadurch aus, dass die vorsorgliche Speicherung umfassend und zugleich ohne nähere Anknüpfungspunkte erfolgt, die die Prognose einer späteren Erforderlichkeit der Daten stützen und zu denen sonst beispielsweise vorangegangenes Verhalten, Gefahren- oder Verdachtsannahmen, Lagebilder oder kriminalistische Erkenntnisse gehören.[31] Genau deswegen wird die große Mehrzahl der Daten sich eben als nicht erforderlich erweisen. Im Falle des Fehlens relativ zum Speicherumfang zureichender Anknüpfungspunkte für eine Erforderlichkeitsprognose ist aber das Verbot einer Datenspeicherung auf Vorrat betroffen, wenn es einen sinnvollen Inhalt haben soll. Beschränkte es sich auf Aussage, dass der Staat nicht sämtliche Vorkommnisse unter dem Aspekt „alles kann ja irgendwann und irgendwie mal nützlich sein" speichern darf, wäre es praktisch genauso bedeutungslos wie das Verbot eines „umfassenden Persönlichkeitsprofils"[32], weil eine solche Form der Vorratsspeicherung weder realisiert werden kann noch auch nur ein Interesse daran besteht.

Das Gericht schließt seine Ausführungen damit ab, dass die vorsorglich anlasslose Speicherung von Telekommunikationsverkehrsdaten angesichts der Schwere des Eingriffs eine Ausnahme bleiben müsse. Insbesondere dürfe sie nicht „im Zusammenspiel mit anderen vorhandenen Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger führen" (Rn. 218). Die Einführung der Telekommunikationsverkehrsdatenspeicherung könne daher nicht als Vorbild für die Schaffung weiterer vorsorglich anlassloser Datensammlungen dienen, sondern zwinge den Gesetzgeber bei der Erwägung neuer Speicherungspflichten oder -berechtigungen in Blick auf die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen zu Zurückhaltung (Rn. 218). Das Gericht macht dem Gesetzgeber eine Art „Überwachungsgesamtrechnung"[33] auf und markiert eine absolute Grenze für die Zulässigkeit einer flächendeckenden vorsorglichen Speicherung von Daten. Dies bringt es sogar mit dem in der Lissabon-Entscheidung geltend gemachten „Identitätsvorbehalt" in Verbindung (Rn. 218). Die markanten Ausführungen müssen in ihrer praktischen Bedeutung für die Beurteilung künftiger staatlicher Überwachungen jedoch mit Blick auf die Schwierigkeiten einer Operationalisierbarkeit kumulativer Wirkungen von Überwachungsmaßnahmen oder „totaler Erfassung und Registrierung" relativiert werden.[34]

[29] BVerfGE 120, 274.

[30] Vgl. BVerfGE 65, 1 (46).

[31] Man muss die Ausführungen des Gerichts zu den „Besonderheiten der modernen Telekommunikation" (Rn. 216 f.) als Bemühungen deuten, spezifische Anknüpfungspunkte zu finden; diese bleiben aber hochabstrakt und blass.

[32] Dazu näher *Trute*, Verfassungsrechtliche Grundlagen, in: Roßnagel (Hrsg.) Handbuch Datenschutzrecht, 2003, S. 156 ff. Rn. 26: „Persönlichkeitsprofile sind […] Mystifikationen."

[33] *Roßnagel*, NJW 2010, 1238.

[34] Zur Operationalisierbarkeit und ihren Schwierigkeiten vgl. *Hornung/Schnabel*, DVBl 2010, 824 (827 f.). Allgemeiner und grundlegend *Hornung*, Die kumulative Wirkung von Überwachungsmaßnahmen: Eine Herausforderung an die Evaluierung von Sicherheitsgesetzen, in: Albers/Weinzierl

(2) Die Ausgestaltung der Vorratsdatenspeicherung

Es liegt in der Konsequenz der Ausführungen zur prinzipiellen Vereinbarkeit der angegriffenen Form der Vorratsdatenspeicherung mit Art. 10 GG, dass das BVerfG mit Blick auf das Normenklarheitsgebot[35] und das Übermaßverbot konkrete, zum Teil detaillierte Vorgaben für die verfassungskonforme Ausgestaltung herleitet. Dabei greift es teils auf seine bisherige Rechtsprechung zu vergleichbaren Gefährdungslagen zurück[36], teils gelangt es zu weiter führenden Überlegungen. Die Vorgaben betreffen Gesichtspunkte der Datensicherheit, des Umfangs der Datenverwendung, der Transparenz und des Rechtsschutzes.

Für die Stufe der Speicherung der Daten bei den Diensteanbietern stellt das Gericht insbesondere den Gesichtspunkt der Datensicherheit heraus. Hierzu formuliert es neuartige grundrechtliche Vorgaben. Wenn der Gesetzgeber eine Speicherung von Telekommunikationsverkehrsdaten im Umfang des § 113a TKG anordnet, dann muss er zugleich einen besonders hohen Standard der Datensicherheit durch darauf gerichtete, normenklare und verbindliche Verpflichtungen der privaten Diensteanbieter gewährleisten (Rn. 221 ff.). Diese Gewährleistungsverantwortung des Gesetzgebers reagiert darauf, dass die Gefahr eines illegalen Zugriffs auf die angesichts ihrer vielseitigen Aussagekraft attraktiven Daten hoch ist und dass die privaten Diensteanbieter wegen des Kostendrucks von sich aus nur begrenzte Anreize zur Gewährleistung von Datensicherheit haben. Anforderungen an die Datensicherheit gelten sowohl für die Aufbewahrung der Daten als auch für deren Übermittlung; ebenso bedarf es effektiver Sicherungen zur Gewährleistung der Löschung der Daten. Der Datensicherheitsstandard ist dynamisch zu gestalten: Er muss sich – etwa unter Rückgriff auf einfachgesetzliche Rechtsfiguren wie den Stand der Technik – an dem Entwicklungsstand der Fachdiskussion orientieren und neue Erkenntnisse und Einsichten fortlaufend aufnehmen. Insofern sind die zu stellenden Anforderungen entweder durch differenzierte technische Vorschriften, die auf verschiedenen Normebenen gestuft sein können, oder in allgemeingenereller Weise vorzugeben und dann in transparenter Weise durch verbindliche Einzelentscheidung der Aufsichtsbehörden gegenüber den einzelnen Unternehmen zu konkretisieren. Das Gericht nennt beispielhaft eine getrennte Speicherung der Daten, eine anspruchsvolle Verschlüsselung, ein gesichertes Zugriffsregime unter Nutzung etwa des Vier-Augen-Prinzips und eine revisionssichere Protokollierung. Verfassungsrechtlich geboten sind weiterhin eine Kontrolle unter Einbeziehung des unabhängigen Datenschutzbeauftragten sowie ein ausgeglichenes Sanktionensystem, das auch Verstößen gegen die Datensicherheit ein angemessenes Gewicht beimisst.

Auf der Stufe des Abrufs, der Übermittlung und der Nutzung durch die Sicherheitsbehörden verlangt das BVerfG zunächst, dass die Verwendung der gespeicherten Telekommunikationsverkehrsdaten überragend wichtigen Aufgaben des Rechtsgüterschutzes dient. Dies muss sich in der einfachrechtlichen Beschreibung sowohl der geschützten Rechtsgüter als auch der Einschreitschwellen widerspiegeln.[37] Für die Strafverfolgung bedeutet dies, dass ein Abruf der Daten zumindest den durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat voraussetzt. Im Rahmen der Gefahrenabwehr wird die Verwendung der gespeicherten Daten 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 und – wie bereits in dem Urteil zur Online-Durchsuchung – von „tatsächlichen Anhaltspunkten einer konkreten Gefahr“ (Rn. 231) abhängig gemacht.[38] Diese Anforderungen gelten ausdrücklich auch für die Nachrichtendienste (Rn. 233).[39] Das Gericht übersieht dabei nicht, dass deren Aufgaben der Regierungsunterrichtung und der Vorfeldaufklärung nicht allein an konkrete Gefahrenlagen geknüpft sind. Es fordert eine solche Einschreitschwelle jedoch mit Blick auf die mit einer nachrichtendienstlichen Datenverwendung verbundenen Beeinträchtigungen für die Bürger. Die Begrenzung auf bestimmte Zwecke, in denen sich die überragend wichtigen Aufgaben des Rechtsgüterschutzes widerspiegeln, muss auch nach Abruf der Daten und Übermittlung an die abrufenden Behörden sichergestellt und verfahrensmäßig flankiert werden. Insbesondere müssen die Daten nach Übermittlung unverzüglich ausgewertet werden und im Falle ihrer Irrelevanz gelöscht werden. Die abrufenden Behörden dürfen sie allerdings an andere Stellen weiterleiten, soweit dies zur Wahrnehmung von Aufgaben erfolgt, deretwegen ein Zugriff auf diese Daten auch unmittelbar zulässig wäre (so genannter „hypothetischer Ersatzeingriff“). Hinsichtlich des Umfangs der abzurufenden Daten muss der Gesetzgeber für einen engen Kreis von auf besondere Vertraulichkeit angewiesenen Telekommunikationsverbindungen, wie etwa der telefonischen Beratung in seelischen oder sozialen Notlagen, ein grundsätzliches Übermittlungsverbot vorsehen (Rn. 238). Das BVerfG gibt dem Gesetzgeber außerdem auf, effektive Vorkehrungen zur Transparenz der Datenverwendung zu treffen. Eine heimliche Verwendung von Daten komme nur dann in Betracht, wenn anderenfalls der Zweck der Untersuchung, dem der Datenabruf dient, vereitelt wird. Für die Gefahrenabwehr und die Wahrnehmung der Aufgaben der Nachrichtendienste dürfe der Ge-

(Hrsg.), Menschenrechtliche Standards in der Sicherheitspolitik, 2010, S. 65 ff.

[35] Zur zunehmenden Bedeutung des Bestimmtheitsgrundsatzes und des Normenklarheitsgebots in der verfassungsgerichtlichen Rechtsprechung s. etwa BVerfGE 110, 33 (53 ff.); 113, 348 (375 ff.).

[36] Vgl. zuletzt insbesondere die Entscheidungen zur Telekommunikationsüberwachung (BVerfGE 113, 348), zur Rasterfahndung (E 115, 320) und zur Online-Durchsuchung (E 120, 274).

[37] Näher zu solchen Eingrenzungen *Albers*, Die Determination polizeilicher Tätigkeit in den Bereichen der Straftatenverhütung und der Verfolgungsvorsorge, 2000, S. 297 ff.

[38] Kritisch *Möstl*, DVBl 2010, 808 (809).

[39] Kritisch etwa *Wolff*, NVwZ 2010, 751 (753).

setzgeber dies grundsätzlich annehmen, nicht jedoch für die Strafverfolgung. Hier sei der Betroffene vor der Abfrage beziehungsweise Übermittlung seiner Daten grundsätzlich zu benachrichtigen. Soweit die Verwendung der Daten heimlich erfolgt, müssen die Betroffenen im Regelfall zumindest nachträglich benachrichtigt werden. Darüber hinaus unterstellt das Gericht die Abfrage und Übermittlung der Daten einem – angemessen auszugestaltenden[40] – Richtervorbehalt (Rn. 247 ff.), obwohl Art. 10 Abs. 2 GG, anders als Art. 13 Abs. 2-4 GG, einen solchen nicht vorsieht.[41]

Damit wird zumindest die Ausgestaltung der Speicherung, des Abrufs, der Übermittlung, der Verwendung und der Weiterleitung hohen Anforderungen unterstellt. Da der Umgang mit personenbezogenen Daten und Informationen prozesshaft verläuft, sind die grundrechtlichen Vorgaben des Art. 10 GG – ebenso wie die des Rechts auf informationelle Selbstbestimmung – verarbeitungsorientiert.[42] Die jeweils auszugestaltenden Phasen verweisen aufeinander, und dementsprechend gibt es auch zwischen den grundrechtlichen Vorgaben Wechselbezüge. So ist die Speicherung nur im Falle einer verfassungsmäßigen Ausgestaltung der Datenverwendung zulässig: „Die verhältnismäßige Ausgestaltung dieser Verwendungsregeln entscheidet dann nicht nur über die Verfassungsmäßigkeit dieser einen eigenen Eingriff begründenden Bestimmungen selbst, sondern wirkt auf die Verfassungsmäßigkeit schon der Speicherung als solcher zurück“ (Rn. 226). Vor diesem Hintergrund gelangt das BVerfG zu einem Netzwerk materieller und verfahrensrechtlicher Maßgaben für die gesetzgeberische Ausgestaltung. Für die mittelbare Nutzung der Daten für Auskünfte nach § 113 Abs. 1 TKG in Form eines Auskunftsanspruchs gegenüber den Diensteanbietern zur Identifizierung von IP-Adressen formuliert es dann freilich weniger strenge Anforderungen (Rn. 254 ff.).

Im Ergebnis genügten die angegriffenen Vorschriften allerdings sämtlich nicht den verfassungsrechtlichen Vorgaben. Sie waren daher insgesamt mit Art. 10 Abs. 1 GG unvereinbar.

b) Prüfung anhand der Vorgaben des Art. 12 GG

§ 113a TKG verpflichtet die Telekommunikationsunternehmen, hier ausdrücklich auch die Anonymisierungsdienste, zur Speicherung der genannten Verkehrsdaten, wobei die Kosten für die nötige Infrastruktur von den Unternehmen zu tragen sind. Die darin liegenden Beeinträchtigungen sind am Maßstab von Art. 12 Abs. 1 GG zu messen. Diskutiert worden sind sowohl die Beschränkungen für die Anonymisierungsdienste als auch die Verhältnismäßigkeit der Indienstnahme Privater für öffentliche Aufgaben.[43]

Das BVerfG sieht hingegen keine verfassungsrechtlichen Bedenken hinsichtlich Art. 12 GG (Rn. 293 ff.).[44] Es stuft die Speicherungspflicht auch hinsichtlich der Anonymisierungsdienste nicht als Berufswahlregelung ein, denn § 113a Abs. 6 TKG mache das Angebot eines Anonymisierungsdienstes nicht faktisch unmöglich. Vielmehr könnten Anonymisierungsdienste ihren Nutzern weiterhin anbieten, ohne Identifizierungsmöglichkeit der IP-Adresse durch Private im Internet zu surfen; aufgehoben werde die Anonymität nur gegenüber den staatlichen Behörden unter den engen Voraussetzungen eines zulässigen Datenabrufs. Allerdings hat es – damit setzt sich das Gericht nicht gesondert auseinander – Anonymisierungsdiensteanbieter gegeben, die ihre besondere Leistung gerade darin gesehen haben, die Daten mittels technischer Konstruktionen so zu anonymisieren, dass sie selbst die sie in Anspruch nehmenden Nutzer nicht identifizieren konnten.[45] Das Unmöglichwerden eines solchen Angebots stellt aber ebenfalls (nur) eine Berufsausübungsregelung dar, die man für verhältnismäßig halten kann. Auch im Übrigen stuft das BVerfG weder den technischen Aufwand (Rn. 300) noch die finanziellen Belastungen (Rn. 301 ff.) als eine unverhältnismäßige Beeinträchtigung der Berufsausübungsfreiheit der Telekommunikationsdiensteanbieter ein. Eine grundsätzliche Unzulässigkeit einer Indienstnahme für Gemeinwohlzwecke von Privaten auf deren Kosten folgt aus der Verfassung nicht. Dem Gesetzgeber wird im Gegenteil ein weiter Gestaltungsspielraum zuerkannt, welche Pflichten zur Sicherstellung von Gemeinwohlbelangen er Privaten im Rahmen ihrer Berufstätigkeit auferlegt. Grundsätzlich könne er, so erläutert das Gericht, Lasten und Maßnahmen zur Wahrung von Gemeinwohlbelangen, die als Folge kommerzieller Aktivitäten regulierungsbedürftig sind, den Marktakteuren auferlegen, um die damit verbundenen Kosten auf diese Weise in den Markt und den Marktpreis zu integrieren. Eine erdrosselnde Wirkung der Kostenlasten sei weder substantiiert vorgebracht noch erkennbar.

[40] Dies im Anschluss an BVerfGE 103, 142 (160 f.); 109, 279 (358 f.)

[41] Vgl. für das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme BVerfGE 120, 274 (331).

[42] Vgl. *Simitis*, NJW 1984, 398 (402), für das Recht auf informationelle Selbstbestimmung.

[43] Vgl. etwa *Vogel*, in: Griesbaum (Hrsg.), Strafrecht und Justizgewährung, Festschrift für Kay Nehm zum 65. Geburtstag, 2006, S. 81, 90 ff.; *Breyer*, Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, 2005, S. 277 ff.

[44] Vgl. zum Problem *Eckhardt/Schütze*, CR 2010, 225, 231; ferner *Greenawalt*, Die Indienstnahme privater Netzbetreiber, Berlin 2009, sowie *Braun*, K&R 2009, 386 und *Hoeren*, JZ 2008, 668.

[45] Z.B. JAP, s. unter http://anon.inf.tu-dresden.de.

D. Ausblick

Es ist Sache des Gesetzgebers, bei der erneuten Umsetzung der Richtlinie die Vorratsdatenspeicherung so auszugestalten, dass sie den Vorgaben des BVerfG entspricht. Auch der EuGH wird infolge der irischen Vorlage voraussichtlich noch einmal Gelegenheit haben, über die Vereinbarkeit der Vorratsdatenspeicherung mit europäischen Grundrechten nachzudenken.

Prof. Dr. Marion Albers, Wiss. Mitarbeiter Dr. Jörn Reinhardt, Hamburg