

Das Schicksal der Vorratsdatenspeicherung

Am 11. März 2008 beschloss das Bundesverfassungsgericht Teile der umstrittenen Vorratsdatenspeicherung im Wege der einstweiligen Anordnung auszusetzen. Vorratsdatenspeicherung meint dabei die Einführung einer Mindestspeicherpflicht für Telekommunikationsverbindungsdaten.

1 Der Weg zum Gesetz

Dem Gesetz zur Änderung der StPO und des TKG, das Bundespräsident Horst Köhler am 26.12.2007 verkündete und das am 1.1.2008 in Kraft trat, geht eine lange Geschichte voraus.¹

Erste Gesetzesvorhaben

Die Geschichte der Vorratsdatenspeicherung in Deutschland reicht zurück ins Jahr 1996. Im Rahmen der Einführung der RegTP nahm der Bundesrat die TKG-Novelle zum Anlass neben der Einführung einer Höchstspeicherfrist die Einführung einer Mindestspeicherfrist zu fordern. Dies lehnte die Bundesregierung mit Hinweis auf die Unzulässigkeit einer solchen Speicherung auf Vorrat ab.²

Bereits im Jahr 2000 tauchte die Vorratsdatenspeicherung in Forderungen des Innenausschusses des Bundesrats wieder auf. Im Rahmen der anstehenden Novellierung der Telekommunikationsdatenschutzverordnung schlug dieser vor, eine Vorschrift einzufügen, welche die Provider verpflichten sollte, alle Verbindungsdaten zum Zwecke der Verbrechensbekämpfung sechs Monate lang zu speichern.³ Diese Verordnung wurde jedoch ohne Mindestspeicherfrist erlassen.

Am 29.8.2001 brachten Abgeordnete der CDU/CSU-Fraktion einen Gesetzesentwurf in den Bundestag ein⁴, der u. a. vorsah § 89 TKG 1997, der eine Verordnungsermächtigung für eine Datenschutzverordnung beinhaltete, um die Ermächtigung zur Einführung einer Mindestspeicherfrist auf dem Verordnungsweg zu ergänzen. Der Vorschlag wurde am 21. März 2002 vom Bundestag abgelehnt.⁵

Bereits 3 Monate später fand sich erneut ein Gesetzesentwurf⁶ des Bundesrats im Bundestag ein, der ebenfalls über den Verordnungsweg die Vorratsdatenspeicherung einführen wollte. Die rot-grüne Bundesregierung lehnte die Pläne

damals in ihrer Stellungnahme ab.⁷ Zu einer Abstimmung im Bundestag kam es aufgrund des Endes der 14. Legislaturperiode am 17.10.2002 nicht mehr.

Der Regierungsentwurf eines neuen TKG vom März 2003 sah zunächst keine Vorratsdatenspeicherung vor. Es war der Bundesrat, der erneut die Einführung forderte.⁸ Nachdem der Bundesrat u. a. aufgrund der fehlenden Vorratsdatenspeicherung⁹ seine Zustimmung zu dem Gesetz verweigerte, kam es zu einem Verfahren im Vermittlungsausschuss, in dem die Vorschriften nicht ins Gesetz aufgenommen wurden.

In insgesamt fünf Anläufen war es den Innenpolitikern daher nicht gelungen sich mit ihrem Vorhaben durchzusetzen, eine Mindestspeicherfrist für Verbindungsdaten einzuführen.

Damit zeigte der Bundestag mehrfach, dass er aufgrund verfassungsrechtlicher Bedenken einer Einführung der Vorratsdatenspeicherung nicht zustimmen will.

Europäisches Ausland

Nachdem die EG mit Art. 15 der Richtlinie 2002/58/EG den strengen Datenschutz von Art. 6 der Richtlinie 95/46/EG aufgehoben hatten, war es den Mitgliedsstaaten möglich, die Anbieter von Telekommunikationsdiensten zu verpflichten, die Verkehrsdaten ihrer Nutzer zum Zwecke der Bekämpfung von Terrorismus und zur Unterstützung der Strafverfolgung zu erlauben.

Die Richtlinie sah jedoch keinesfalls eine Verpflichtung zur Vorratsdatenspeicherung - sie ermöglichte sie lediglich.

In Irland fand die Vorratsdatenspeicherung von Telefonverbindungen bereits im April 2001 Eingang in nationale Gesetze.

Rahmenbeschluß

Im April 2004 brachten Frankreich, Irland, Schweden und das Vereinigte Königreich einen Vorschlag für einen Rahmenbeschluss im Rahmen der justiziel- len Zusammenarbeit ein. Dieser Rahmenbeschluß kam jedoch aufgrund von

Protesten der Kommission und des EU-Parlaments nicht zustande. Beide argumentierten, dass eine solche Regelung als Richtlinie erlassen werden müsste. Darüber hinaus war nicht zu erwarten, dass der Rat die benötigte Einstimmigkeit für einen Rahmenbeschluß würde herstellen können. Sodann nahm die Kommission ihre Arbeit an der Richtlinie auf.¹⁰

Die Richtlinie

Der Bundestag bekräftigte während der Verhandlungen der Bundesregierung über RL 2006/24/EG durch eine erneute Entschließung zunächst seine Position.¹¹ Nach der Bundestagswahl 2005 änderte der Bundestag jedoch dahingehend seine Meinung und lehnte zwei Anträge¹² sich erneut gegen eine europaweite Vorratsdatenspeicherung auszusprechen ab.¹³ Ein Antrag¹⁴, die Richtlinie vom EuGH überprüfen zu lassen und sie bis zu dessen Entscheidung nicht umzusetzen, fand ebenfalls keine Mehrheit.¹⁵

Dies verwundert jedenfalls insoweit, als drei Legislaturperioden lang der Bundestag offensichtlich der Auffassung war, eine solche Speicherung sei unnötig und vor allem verfassungswidrig.

Schließlich fand die Richtlinie am 15. März 2006 ihren Weg durch die europäische Legislative und sah eine Umsetzungsfrist für klassische Telefonie bis zum 15. September 2007 vor. Für die Speicherung von Internetzugängen, Internettelefonie und E-Mails sieht die Richtlinie eine zwingende Umsetzung bis zum 15. März 2009 vor, um den Providern bei den zu erwartenden Schwierigkeiten bei der Bewältigung der unglaublichen Datenmengen entgegenzukommen.

Nichtigkeitsklage

Mit Aktenzeichen C-301/06 legte Irland gegen die Richtlinie beim EuGH Nichtigkeitsklage ein, Art. 230 EG. Das er-

¹ Zu den Details: Gietl, K&R, 2007, 545ff.

² Bt-Drs. 13/4437, 39.

³ <http://www.heise.de/newsticker/Datenschutz-beauftragte-gegen-unnoetige-Eingriffe-in-das-Fernmeldegeheimnis-/meldung/12145>

⁴ Bt-Drs. 14/6834, 7.

⁵ Bt-Drs. 14/227, S. 22515.

⁶ Bt-Drs. 14/9801, S. 8.

⁷ Bt-Drs. 14/9801, S. 16

⁸ BR-Drs. 755/03

⁹ BR-Drs. 200/1, S. 3

¹⁰ Vgl. zum Ganzen: Rusteberg, VblBW 2007, 171, 173.

¹¹ Bt-Drs. 15/4748

¹² Bt-Drs. 16/128, 16/273

¹³ BT-Prot. 16/ S. 1430B

¹⁴ BT -DRS 16/1622

¹⁵ BT-Prot. 16, S. 3527C

scheint insofern interessant, als Irland als eines der ersten europäischen Länder selbst schon vor der Richtlinie die Vorratsdatenspeicherung einführt.

Die beachtliche Begründung der Nichtigkeitsklage beruft sich auf einen Kompetenzverstoß. Schwerpunkt der Regelung zur Vorratsdatenspeicherung sei nicht die Herstellung von gleichen Bedingungen für einen europäischen Binnenmarkt, wie es Art. 95 EG fordert. Vielmehr handle es sich um eine Form der justiziellen Zusammenarbeit, die im Rahmen der dritten Säule der EU hätte verabschiedet werden müssen. Insofern fehle der EG die Verbandszuständigkeit.

Dies ist zumindest insofern richtig, als die Richtlinie von vornherein auf die Verfügbarkeit der Daten für die Strafverfolgung abzielte. Allerdings zielt die Richtlinie tatsächlich zunächst auf Private und regelt so den Wettbewerb in der EU zwischen Zugangs Providern. Der EuGH könnte also durchaus geneigt sein, die Richtlinie nicht aufgrund eines Kompetenzverstosses für nichtig zu erklären.¹⁶ Das deutsche Schrifttum nimmt dagegen einhellig an, dass die Vorschrift nicht als Richtlinie hätte ergehen dürfen.¹⁷

Keine Verbandszuständigkeit

Tatsächlich war die EG befugt im Rahmen des Art. 95 EG Richtlinien zum Umgang mit Verbindungsdaten zu regeln. Dabei hat die EG bisher lediglich Regeln aufgestellt, welche die Speicherung bestimmter Daten durch die Provider verboten oder nur zu bestimmten Zwecken erlaubten. Damit verfolgte die EG Ziele des Wettbewerbs- und Verbraucherschutzes. Dies v.a. deshalb da die Richtlinie dem Wettbewerb dadurch diene, da sie womögliche vorteilhafte Speicherungen durch die Provider verbote, die diese zu statistischen Zwecken oder zum Marketing hätten nutzen können.

Nun kehrte die EG mit ihrer Richtlinie die Regelung allerdings um und sieht eine Verpflichtung zur Speicherung zum Zweck der Strafverfolgung vor. Damit schafft die EG zwar auch einen einheitlichen Wettbewerbsrahmen, da die Provider in allen Mitgliedsstaaten zur Speicherung verpflichtet werden. Die Tatsa-

che der Verpflichtung zur Speicherung kann so womöglich noch erklärt werden. Allerdings kann dies den Regelungen zur Verwendung der Daten durch die Sicherheitsbehörden wohl nicht mehr nachgesagt werden. Ohne diese Abrufverpflichtung jedoch wäre die Pflicht zur Speicherung völlig sinnlos. Daher handelt es sich um eine Regelung, die lediglich der Strafverfolgung dient. Dies wird auch dadurch klar, dass es den Providern weiterhin versagt bleibt die Daten zu ihren eigenen Zwecken zu nutzen.

Der Wettbewerb wird nur soweit geregelt, als alle Wettbewerber im europäischen Binnenmarkt durch die Vorschriften belastet werden. Mit dieser Argumentation könnte man aber alle Regelungen, die Unternehmen in belasten im Rahmen der Wirtschaftskompetenz des Art. 95 EG erlassen.

Ähnlich hat der EuGH bereits in der Frage entschieden, ob die Umsetzung des Abkommens der EG mit den USA zur Fluggastdatenübermittlung auf Art. 95 EG gestützt werden darf: „Es trifft zwar zu, dass die PNR-Daten von den Fluggesellschaften ursprünglich im Rahmen einer unter das Gemeinschaftsrecht fallenden Tätigkeit erhoben worden sind, nämlich im Rahmen des Verkaufs eines Flugscheins, der zu einer Dienstleistung berechtigt; die Datenverarbeitung, die in der Angemessenheitsentscheidung Berücksichtigung findet, ist jedoch von ganz anderer Art. Denn diese Entscheidung bezieht sich, wie in Randnummer 55 des vorliegenden Urteils ausgeführt, auf eine Datenverarbeitung, die nicht für die Erbringung einer Dienstleistung erforderlich ist, sondern zum Schutz der öffentlichen Sicherheit und zu Strafverfolgungszwecken als erforderlich angesehen wird.“¹⁸

Die Frage, ob die Richtlinie von Art. 95 EG gedeckt ist, wird auch für die Entscheidung des BVerfG in der Hauptsache womöglich entscheidend sein, wie noch zu zeigen sein wird.

Irland hatte im Vorfeld der Richtlinie mehrmals versucht, eine Verpflichtung der Mitgliedstaaten im Rahmen der dritten Säule zu erreichen.

Gemeinschaftsgrundrechte

Da die Gemeinschaftsgrundrechte nach Art. 46 lit. d EUV vom EuGH auch in Verfahren gegen Rahmenbeschlüsse der EU, die ja außerhalb des Gemeinschaftsrechts stehen, und eher dem Völkerrecht zugeordnet werden, prüft, kommt der Frage des Verstoßes gegen Gemein-

schaftsgrundrechte ein erhebliches Gewicht zu. Würde der EuGH einen Verstoß gegen Gemeinschaftsgrundrechte feststellen, könnte die Vorratsdatenspeicherung auch nicht als Rahmenbeschluss umgesetzt werden.

Auch europäische Grundrechte könnten den EuGH veranlassen die Richtlinie für nichtig zu erklären. Zweifel an der grundrechtlichen Zulässigkeit einer solchen Richtlinie hatte in einem anderen Verfahren jedenfalls die Generalanwältin in ihrem Schlussplädoyer. Dabei nahm sie ausdrücklich auf die Richtlinie zur Vorratsdatenspeicherung Bezug.¹⁹

Ein Eingriff in Art. 8 EMRK durch die Erhebung und Verarbeitung personenbezogener Daten²⁰ liegt hier sicher vor. Es stellt sich jedoch die Frage, ob der EuGH einen gerechtfertigten Eingriff annimmt.

Eine Nichtigkeitsklage einzelner Bürger oder Bürgerrechtsverbände gegen die Richtlinie ist dagegen am EuGH nicht möglich. Der EuGH lässt Nichtigkeitsklagen nach Art. 230 Abs. 4 EG nur zu, wenn die Voraussetzungen der sog. Plaumann-Formel vorliegen. Dazu müssten die Beschwerdeführer wie die Adressaten einer Entscheidung individuell und unmittelbar betroffen sein,²¹ was regelmäßig nicht der Fall ist.

Irland rügt in seiner Nichtigkeitsklage ausdrücklich nur einen Verstoß gegen Art. 95 EG und nicht einmal hilfsweise einen Verstoß den EG-Vertrag als solchen.

Der EuGH prüft die Frage der Verbandszuständigkeit von Amts wegen.²² Was die Frage der Verletzung materiellen Vertragsrechts angeht, hat der EuGH bisher von einer Prüfung von Amts wegen abgesehen.²³

Daher haben am 8. April 2008 43 Verbände aus 11 EU-Staaten in einem Brief an den EuGH diesen aufgefordert auch die grundrechtliche Problematik der Richtlinie im Nichtigkeitsverfahren zu prüfen.²⁴

Eine weitere Möglichkeit, die Richtlinie wegen Verstoßes gegen Art. 8 EMRK auf übernationaler Ebene zu Fall zu bringen könnte eine Klage vor dem Europäischen Gerichtshof für Menschenrechte sein. Dessen Verwerfung der Richtlinie würde die Mitgliedsstaaten völkerrechtlich binden, so dass sie

¹⁶Rusteberg, VblBW, 2007, 171, 174.

¹⁷Gitter/Schnabel, MMR 2007, 411, 412 f.; Leutheusser-Schnarrenberger, ZRP 2007, 9, 11 ff.; Rusteberg, VBIBW 2007, 171; Breyer, StV 2007, 214, 215 f.; Wüstenberg, RDV 2006, 102-104; Gola/Klug, NJW 2006, 2454, 2459 f.; Westphal, EuR 2006, 706-723; Köcher/Kaufmann, DuD 2006, 360, 364; Westphal, EuZW 2006, 555, 557 f.; Bizer, DuD 2007, 586, 587.

¹⁸EuGH C317/04, Abs-Nr. 58.

¹⁹Schlussantrag zu EUGH C-275/06, Abs-Nr.

82.
²⁰EuGH C-465/00, Abs.-Nr. 73ff.

²¹Calliess, NJW 2002, 3577, 3579.

²²Streinz, EGV/EUV, Art. 230 EGV Rdnr. 68.

²³EuGH C-367/95, Abs-Nr. 67.

²⁴<http://www.vorratsdatenspeicherung.de/content/view/216/1/lang.de/>

die Richtlinie national nicht anwenden dürften.²⁵ Aufgrund der Öffnungsklausel des Art. 307 Abs. 1 EG, die völkerrechtlichen Altverträge vom Geltungsvorrang des Gemeinschaftsrecht ausnimmt, würde dies zu keinem Konfliktfall mit EG-Recht führen, da Deutschland die EMRK vor dem EGV ratifiziert hat.²⁶

Überschießende Umsetzung

Letztlich fand die Richtlinie ihre Umsetzung im Rahmen des TKG und der StPO. Das Gesetz sieht jedoch einige Regelungen vor, die weit über die Vorgaben der Richtlinie hinausgehen.²⁷

So sieht § 113 a Abs. 6 TKG verpflichtend eine Speicherung von Ausgangs- und Enddaten vor, wenn ein Anonymisierungsdienst betrieben wird. Die Vorschrift dürfte darüber hinaus öffentliche WLANs betreffen, wenn man sie weit auslegt. Eine Regelung die ihren Zweck nur dann erfüllen kann, wenn sie nicht nur IP-Adressen speichert, wie gefordert, sondern auch den Zielpunkt und damit Rückschlüsse auf benutzte Internetseiten und Dienste zulässt. Ein Eingriff in das Fernmeldegeheimnis, der noch weiter geht, als die gesetzlich vorgesehene Speicherung der IP-Adressen, die beim Internetzugang zugewiesen werden.²⁸

Weiter setzte der Gesetzgeber die Bestimmungen zum Abruf der Daten bei den Providern überschießend um. Dies betrifft vor allem den Katalog der Straftaten, bei denen die Behörden die Daten abrufen dürfen. Nachdem die Richtlinie verlangt den Abruf für schwere Straftaten zu ermöglichen, weitete der deutsche Gesetzgeber diesen Katalog aus. Dabei übernahm er den Katalog des alten § 100 g StPO für die Abfrage von Verbindungsdaten. Es reichte nun eine Straftat, die mittels Telekommunikation begangen wurde, die Erforschung des Sachverhalts oder die Bestimmung des Aufenthaltsorts des Beschuldigten anderweitig aussichtslos sein und die Erhebung in einem angemessenen Verhältnis zur Bedeutung der Sache stehen. Wurde die Tat nicht mittels Telekommunikation begangen, so genügt eine im Einzelfall erhebliche Straftat. Dabei blieben die Anforderungen an die Straftat im wesentlichen unverändert. Es gilt jedoch zu bedenken, dass der Datenpool, aus dem

die Ermittler hier schöpfen können, ungleich größer wurde und mit Beginn der Speicherpflicht für E-Mails, VOIP-Telefonate und Internetzugänge erheblich anwachsen wird. Denn bisher waren die Daten von den Betreibern nachdem sie sie für die Abrechnung nicht mehr benötigten im Regelfall zu löschen. Im Fall von E-Mails werden derzeit im Regelfall gar keine Protokollierungen vorgenommen.

2 Die Verfassungsbeschwerden

Daraufhin reichte am 31.12.2007 der AG Vorrat, eine Bürgerrechtsinitiative, Verfassungsbeschwerde gegen das Umsetzungsgesetz ein.²⁹ Dabei wurde auch eine Aussetzung des Gesetzes im Verfahren der einstweiligen Anordnung nach § 32 BVerfGG beantragt. Beachtenswert in diesem Zusammenhang ist auch die Tatsache, dass die Verfassungsbeschwerde insgesamt über 34 000 Beschwerdeführer fand, auch wenn aus organisatorischen Gründen auf Seiten der Kläger zunächst nur acht Beschwerdeführer Klage einreichten, demonstriert die Zahl dennoch die hohe Zahl an Bürgern, die von diesem Gesetz beunruhigt sind und es für verfassungswidrig halten.

Daneben hat Burkhard Hirsch eine Verfassungsbeschwerde angestrengt, die sich ebenfalls vor allem gegen die Speicherung wenden.

Einer Pressemitteilung des Bundesverfassungsgerichts ist außerdem zu entnehmen, dass es noch weiter Beschwerden gibt, die sich im Kern gegen die Auskunftsmöglichkeiten richten.³⁰

Auch die Fraktion der Grünen im Bundestag hat Organklage gegen das Gesetz beim Bundesverfassungsgericht eingelegt, da auch die Abgeordnetenrechte der Bundestagsabgeordneten verletzt seien.³¹

3 Die Entscheidung

Das Bundesverfassungsgericht entschied am 11.3.2008 im Verfahren des Eilrechtsschutzes nach § 32 BVerfGG über eine Verfassungsbeschwerde gegen die Änderungen am TKG und am StPO.

Querelen am BVerfG

Dieser Entscheidung waren interne Diskussionen der Richter über die Zuständigkeit vorangegangen. Das Bundesverfassungsgericht bestimmt für jedes Verfahren einen Berichterstatter, dem es obliegt die Entscheidung vorzubereiten und nach dem Votum der anderen Richter die gemeinsame Entscheidung auszuformulieren. Darüber hinaus war streitig, welcher Senat zuständig sein sollte.

Ursache der Diskussionen war, dass die Vorratsdatenspeicherung den Bereich Datenschutz des Richters Wolfgang Hoffmann-Riem aus dem ersten Senat unterfällt. Darüber hinaus beanspruchten aus dem zweiten Senat Udo di Fabio aufgrund des Bezugs zum Europarecht und Rudolf Mellinghoff wegen der strafprozessualen Regelungen die Zuständigkeit für sich.³²

Schließlich fand der 6er Ausschuss des BVerfG nach § 14 Abs. 5 BVerfG folgende Lösung: der erste Senat und damit Hoffmann-Riem bearbeiteten die Massenverfassungsbeschwerde und die Verfassungsbeschwerde von Burkhard Hirsch. Die weiteren Verfassungsbeschwerden, die sich v. a. gegen die strafprozessualen Regelungen richten, wurden dem zweiten Senat zugewiesen.³³

Im Verfahren nach § 32 BVerfGG erging nun die beantragte einstweilige Anordnung, die im Rahmen der Massenverfassungsbeschwerde beantragt wurde.

Einstweilige Anordnung

Im Gegensatz zum Verfahren im einstweiligen Rechtsschutz vor den Fachgerichten, bei dem das erkennende Gericht anhand des vorgebrachten Sachverhalts die Rechtslage vollumfänglich prüft und anschließend bei Vorliegen von Anordnungsgrund und Anordnungsanspruch die begehrte Verfügung erlässt, prüft das Bundesverfassungsgericht im Rahmen der einstweiligen Anordnung nicht die Begründetheit der Verfassungsbeschwerde. Lediglich bei offensichtlicher Begründetheit oder Unbegründetheit stellt das Gericht auf die Erfolgswahrscheinlichkeit ab. Es führt ansonsten eine Folgenabwägung zwischen den Folgen durch, die eine Aussetzung des Gesetzes für die vom Gesetzgeber angestrebten Ziele hätte und den Folgen für diese Ziele durch die Anwendung des Gesetzes, wenn es sich im Hauptsacheverfahren

²⁵ Sauer, [Jurisdiktionskonflikte in Mehrebenen-systemen](#), 2008, S. 320f.

²⁶ aaO S. 321 Fn 198.

²⁷ Zu den Details des Gesetzes: Gietl, K&R 2007, 545ff.

²⁸ Siehe dazu Gietl, K&R 2007, 545, 548f.

²⁹ <http://www.vorratsdatenspeicherung.de>

³⁰ Pressemitteilung Nr. 11/2008 vom 30. Januar 2008

³¹ http://gruene-bundestag.de/cms/presse/dok/219/219756.weg_i_n_den_ueberwachungsstaat_stoppen.html

³² <http://www.heise.de/newsticker/Bundesverfassungsgericht-klaert-Zustaendigkeit-fuer-Klage-gegen-Vorratsdatenspeicherung-/meldung/102693>

³³ Pressemitteilung Nr. 11/2008 vom 30. Januar 2008

ren als verfassungswidrig herausstellen sollte. Dabei ist insbesondere auch darauf abzustellen, inwieweit die Folgen reparabel sind und wie schwer diese jeweils wiegen.³⁴ Insgesamt spricht das Gericht in ständiger Rechtsprechung davon, dass es für die Anordnung einer einstweiligen Anordnung gegen Gesetze einen strengen Maßstab anlegt und nur mit äußerster Zurückhaltung davon Gebrauch machen will.³⁵

Vorliegend hatte das Bundesverfassungsgericht also nicht über die Frage zu entscheiden, ob die Speicherung rechtmäßig ist oder nicht, da das Gericht Verfassungsbeschwerde nicht offensichtlich unzulässig oder unbegründet hielt.³⁶

Keine offensichtliche Unzulässigkeit der Beschwerde

Eine Unzulässigkeit könnte sich dabei zwar insbesondere daraus ergeben, dass eine europäische Richtlinie vom Gesetzgeber zwingend umgesetzt werden musste. Zweifelsfrei, so das Gericht, sei die Verfassungsbeschwerde zulässig, soweit sie Teile des Gesetzes angreift, die nicht zwingend von der Richtlinie vorgeschrieben sind, insofern also überschneidend umgesetzt wurden.³⁷

Allerdings sagt das Gericht, die Beschwerde ist auch insofern nicht offensichtlich unzulässig, als sie sich mit Teilen des Gesetzes befasst, die zwingende Teile umsetzen.³⁸ Angesichts der hohen Hürden, die Karlsruhe in der Entscheidung zur Bananenmarktordnung³⁹, für die Zulässigkeit einer Verfassungsbeschwerde gegen die Umsetzung von Gemeinschaftsrecht aufgestellt hat, ein klarer Sieg für die Beschwerdeführer. Immerhin stellte das BVerfG im ersten Leitsatz der genannten Entscheidung fest, Verfassungsbeschwerden seien „vornherein unzulässig, wenn ihre Begründung nicht darlegt, dass die europäische Rechtsentwicklung einschließlich der Rechtsprechung des Europäischen Gerichtshofs nach Ergehen der Solange II-Entscheidung (BVerfGE 73, [339, 378-381](#)) unter den erforderlichen Grundrechtsstandard abgesunken

sind“.⁴⁰ Das Gericht scheint also davon auszugehen, dass diese Voraussetzung nicht evident fehlt, ansonsten hätte es die Beschwerde nur soweit für nicht offensichtlich unzulässig erachten dürfen, wie sie sich gegen überschneidend umsetzende Teile des Gesetzes richtet.

Keine offensichtliche Unbegründetheit der Beschwerde

Konsequenterweise geht das Gericht bei der Prüfung, ob die Beschwerde womöglich offensichtlich unbegründet ist, nicht mehr auf die europarechtliche Grundlage ein. Denn wäre die Zulässigkeit gegeben, lebt die Prüfungskompetenz des Bundesverfassungsgerichts wieder vollständig auf und es prüft das Gesetz alleine an den Vorgaben des Grundgesetzes.

Das Gericht verweist daher lediglich darauf, dass die Erhebung der gespeicherten Daten in Art 10 GG eingreift und dass sich das Gewicht dieses Eingriffs womöglich dadurch ändert, dass diese Daten vorher auf Vorrat gespeichert werden und der Zweck dieser Datensammlung im Voraus nicht feststeht.⁴¹

Folgenabwägung

Im Rahmen der Folgenabwägung will das Bundesverfassungsgericht, den ohnehin bereits scharfen Maßstab, den es an einstweilige Anordnungen gegen Gesetze anlegt, noch einmal verschärft wissen, soweit zwingende Vorgaben des Gemeinschaftsrecht vom Gesetzgeber umgesetzt wurden.

Dabei spricht das Gericht insbesondere davon, dass eine derartige Entscheidung im Rahmen der einstweiligen Anordnung über die Prüfungskompetenz des Bundesverfassungsgerichts in der Hauptsache hinaus gehen könnte.⁴²

Damit weist der Senat auf die offene Frage der Zulässigkeit hin. Die Frage der Zulässigkeit wurde wie oben gezeigt nicht abschließend geklärt. Für diese Entscheidung wäre zu prüfen, ob der Grundrechtsstandard in der Europäischen Gemeinschaft soweit abgesunken ist, dass die Verfassungsbeschwerde wieder zulässig wäre. Daher addiert sich zu dem Risiko, eine Entscheidung des nationalen Gesetzgebers womöglich verfassungswidrig aufzuschieben, das Risiko womöglich die eigene Kompetenzverteilung zum EuGH zu stören und den effektiven Vollzug des Gemeinschaftsrechts zu verhindern.

Letztlich lässt das Gericht die Frage jedoch offen, ob es generell einstweilige

Anordnungen erlassen dürfte, die ein Umsetzungsgesetz suspendieren. Denn es suspendierte nur überschneidend umgesetzte Teile des Gesetzes. Der Senat stellt jedoch fest, dass zur Aussetzung eines Umsetzungsgesetzes den Gesetzesbetroffenen mindestens ein schwerer und irreparabler Schaden drohe müsse, der das Risiko hinnehmbar erscheinen lässt, die eigene Entscheidungskompetenz zu überschreiten und den effektiven Vollzug des Gemeinschaftsrechts schwerwiegend zu beeinträchtigen.⁴³

Speicherung

Unter Berufung auf diese Formel, lehnt das Gericht es ab § 113 a TKG, der die Provider zur Speicherung verpflichtet, außer Vollzug zu setzen. Zwar habe die Speicherung den Effekt, eine erhebliche Einschüchterung der Bürger hervorzurufen. Auch sei dieser Effekt irreparabel, wiege aber alleine noch nicht schwer genug, um die oben genannten Risiken aufzuwiegen. Dies sei vor allem deshalb der Fall, weil die Einschüchterung der Betroffenen auch mit den Voraussetzungen zusammen hänge, unter denen der Staat auf diese Daten Zugriff habe.⁴⁴

Kein Zugriff

Da der Abruf der Verbindungsdaten für den Betroffenen zu erheblichen und irreparablen Schäden in Gestalt von strafrechtlichen Verurteilungen, Wohnungsdurchsuchungen oder Überwachungen, der Aufdeckung sozialer Netze des Betroffenen und der Erforschung seines Kommunikationsverhaltens führe könne, sei dies hier anders.⁴⁵ Alle diese Maßnahmen würden, wenn das Gesetz verfassungswidrig ist, auf verfassungswidrigen Eingriffen des Staates in das Grundrecht aus Art. 10 GG beruhen. Die Folgen dieser Eingriffe könnten womöglich nicht vollständig beseitigt werden.

Darüber hinaus bestehe die Möglichkeit, begrenzte Rückschlüsse auf den Kommunikationsinhalt zu ziehen. Durch die Streubreite der Abfrage, bei der jeweils auch nicht Tatbeteiligte betroffen sind, die mit einem Verdächtigen elektronisch kommuniziert haben, erhöhe sich zudem die Schwere des Eingriffs.⁴⁶

Verböte das Gericht den Abruf vollständig, könnten jedoch Nachteile für die öffentliche Strafverfolgung entstehen, da Ermittlungsverfahren womöglich nicht erfolgreich abgeschlossen

³⁴Vgl. zum Ganzen: Graßhof, Maunz/Schmidt-Bleibtreu/Klein/Betge, Kommentar zum BVerfGG, Stand Juli 2007, § 32 Rdnr. 108ff

³⁵vgl. BVerfGE 3, 41, 44; 104, 51, 55; 112, 284, 292.

³⁶BVerfG, 1 BvR 256/08 vom 11.3.2008, Abs.-satz-Nr. 133.

³⁷Vgl. dazu Gietl, K&R 2007, 545, 549;

³⁸BVerfG, 1 BvR 256/08 vom 11.3.2008, Abs.-satz-Nr. 136.

³⁹BVerfGE 102, 147.

⁴⁰BVerfGE 102, 147, 147.

⁴¹Abs.-Nr. 138

⁴²Abs.-Nr. 142

⁴³Abs.-Nr. 145

⁴⁴Abs.-Nr. 148ff

⁴⁵Abs.-Nr. 155ff.

⁴⁶Abs.-Nr. 156.

werden könnten, wenn die Verbindungsdaten nicht zur Verfügung stehen.

Daher ordnet das Gericht an, dass die Behörden weiterhin nach § 100g Abs. 2 Satz 1 StPO in Verbindung mit § 100 b Abs. 1 und 2 StPO an die Provider richten dürfen. Diese dürfen allerdings nur insoweit die Daten herausgeben, soweit es sich um Daten handelt, die aufgrund der §§ 97ff TKG vom Provider gespeichert werden dürfen, nicht jedoch soweit es um die Daten geht, die aufgrund des § 113 a TKG gespeichert werden müssen und nach den Regeln der §§ 97ff TKG eigentlich schon hätten gelöscht werden müssen.⁴⁷

Handelt es sich um Daten, die nach § 113 a TKG gespeichert werden mussten, so müssen die Provider die Daten erheben und sodann speichern. Sie dürfen diese jedoch nicht an die Behörden herausgeben.⁴⁸

Zugriff bei schweren Straftaten

Dies gilt aber nicht, soweit die Anordnung sich auf eine Straftat aus dem Katalog des § 100 a Abs. 2 StPO bezieht und die Voraussetzungen des § 100a Abs. 1 StPO vorliegen. Damit verlangt das Gericht die selben Voraussetzungen, wie sie der Gesetzgeber für die Anordnung der Telekommunikationsüberwachung vorsieht. Bei Vorliegen dieser Voraussetzungen, wiegen nach Einschätzung des Gerichts die möglichen Nachteile einer Erschwerung des strafrechtlichen Ermittlungen aufgrund der Schwere der Taten schwerer als die Schäden durch eine möglicherweise auf verfassungswidriger Basis vorgenommenen, oben aufgezeigten, Maßnahmen. Daher müssen die Provider die Daten bei Auskunftsverlangen bzgl. Straftaten nach § 100 a Abs. 2 StPO nicht nur erfassen, sondern auch an die Behörden herausgeben.⁴⁹

Bericht der Bundesregierung

Das Verfassungsgericht legte darüber hinaus der Bundesregierung die Pflicht auf ihm bis zum 1. September 2008 einen Bericht über die praktischen Auswirkungen der Vorratsdatenspeicherung und ihrer Aussetzung durch das Gericht vorzulegen.⁵⁰

Befristung

Die einstweilige Anordnung ist auf sechs Monate befristet, wie es § 32 Abs. 6 BVerfGG vorsieht, läuft also am 11. September aus. Das Gericht lässt jedoch durchblicken, dass es aufgrund des Berichts der Bundesregierung ggf. gewillt ist die Anordnung zu verlängern. Dies wäre nur mit einer 2/3 Mehrheit des Senats möglich und wird nur nötig sein, wenn die Hauptsacheentscheidung bis dahin nicht spruchreif ist.

4 Kritik

Insgesamt ist die Entscheidung des Senats zu begrüßen, auch wenn sich die Beschwerdeführer und viele Aktivisten sicherlich mehr erwartet hatten. Der größte Erfolg ist dabei sicherlich, dass das Gericht nicht von einer offensichtlichen Unzulässigkeit ausgeht und den Ausgang des Verfahrens insoweit als offen ansieht.

Im Moment ist der Zustand den das BVerfG dadurch herstellte auch aus einem Grund noch erträglich: Die Pflicht zur Speicherung trifft bis zum 1.1.2009 nur Telefon- und SMS-Verbindungsdaten. Dabei handelt es sich um Daten, die von den Providern meist ohnehin bis zur Abrechnung gespeichert werden und daher den Strafverfolgern wenigstens einige Wochen zur Verfügung standen.

Ungleich schwerer wiegen dagegen die neuen Verpflichtungen aller Internet-Zugangs und E-Mail-Provider. Vor allem bei E-Mails fallen Datenmengen an, die viele kleinere und mittelständische Anbieter an den Rand ihrer Leistungsfähigkeit bringen werden. Auch ist bei der Vielzahl dieser Anbieter keinesfalls sichergestellt, dass diese in der Lage sind die Daten sicher aufzubewahren, wie es die eher großen Firmen in der Telefonbranche vermeintlich können.

Aufgrund dieses Aufschubs sah das Bundesverfassungsgericht sich wohl auch nicht genötigt zur Frage Stellung zu nehmen, inwieweit die Berufsfreiheit mancher Anbieter betroffen ist. Für einen Beschwerdeführer, der einen Internet-Anonymisierungsdienst kommerziell betreibt dürfte die Einführung des § 113 a Abs. 6 TKG jedenfalls einem Berufsverbot gleich kommen. Insofern fällt in der Hauptsache auch noch die Berufsfreiheit mit in die Abwägung, die das Gericht bisher nicht angesprochen hat.

Auch der Einfluss der Vorratsdatenspeicherung auf Berufsgeheimnisträger, hat das Gericht bisher noch ausgeblendet.

In der Vergangenheit verfuhr das Bundesverfassungsgericht bei den meisten Sicherheitsgesetzen nach der Devise „Ja, aber ...“. Es erlaubte die heimliche Onlinedurchsuchung, aber verlangte Maßnahmen zum Schutz des Kernbereichs privater Lebensgestaltung.⁵¹ Dazu ersann das Gericht sogar ein neues Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Es erlaubte die akustische Wohnraumüberwachung, aber fordert schon hier den Schutz des absoluten Kernbereichs privater Lebensgestaltung.⁵² Es erlaubte das KFZ-Kennzeichenscanning, aber will Schutzvorkehrungen gegen die Speicherung der Ergebnisse und will genau formulierte Gesetze und will diese keinesfalls flächendeckend erlauben.⁵³ Diesen Weg hat das Gericht nun auch bei der Vorratsdatenspeicherung eingeschlagen. Es erlaubt die Speicherung, aber beschränkt die Auskunft über die Daten.

Dabei ist jedoch zu beachten, dass es sich hier um eine einstweilige Anordnung handelt, bei dem das Gericht, nur ungern mit dem Europäischen Gerichtshof in Konflikt geraten will.

Das zeigt das Ergebnis der Folgenabwägung: in keinem Punkt hat der Senat eine Regelung außer Kraft gesetzt, die zwingendes Europarecht umsetzen würde. Bei der Auskunft geht das Gericht sogar über die von der Richtlinie geforderten Katalog hinaus und erlaubt diese bei allen Katalogtaten des § 100 a Abs. 2 StPO, auch wenn es deutlich zeigt, dass ihm dieser eigentlich schon zu weit ist.⁵⁴

5 Ausblick

Diesen Weg wird der Senat aber in der Hauptsacheentscheidung nicht weiter gehen können.

Zwar stimmt es, dass der Einschüchterungseffekt der Speicherung auch von den Möglichkeiten der Ermittlungsbehörden zu deren Abruf beeinflusst wird. Letztlich ist der Schwerpunkt des Eingriffs jedoch in der Speicherung zu sehen. Die Speicherung der Verbindungsdaten beeinflusst unmittelbar und nicht erst durch ihren Abruf die Unbefangtheit der Telekommunikation aller Bürger, wie das Bundesverfassungsgericht noch in der Entscheidung zur Onlinedurchsuchung klarstellte.

⁴⁷Abs.-Nr. 173; Zur Unterscheidung: Gietl, K&R 2007, 545, 549.

⁴⁸Abs.-Nr. 160

⁴⁹Abs.-Nr. 164ff.

⁵⁰Abs.-Nr. 177ff

⁵¹BVerfG, 1 BvR 370/07 vom 27.2.2008

⁵²BVerfGE 109, 279.

⁵³BVerfG, 1 BvR 2074/05 vom 11.3.2008

⁵⁴Abs.-Nr. 174

Besonderes Gewicht erhält der Eingriff dadurch, dass sie flächendeckend erfolgt, so dass ein Gefühl des „Überwachtwerdens“ entsteht. Dies stellte das Gericht in der vom selben Tag datierten Entscheidung über die Kennzeichenerfassung klar.

Ebenfalls in dieser Entscheidung stellt der Senat fest, dass das Gewicht mit der Verwertbarkeit der erhobenen Daten für Folgeeingriffe und der Möglichkeit der Verknüpfung mit anderen Daten zunimmt. Dieses Risiko ist bei der Sammlung durch Private im Auftrag womöglich weniger hoch als bei direkter Sammlung der Daten durch den Staat. Allerdings kann nicht sichergestellt werden, dass die Daten jeweils nur nach rechtmäßiger Anordnung herausgegeben werden, da insbesondere die Überlastung der Ermittlungsrichter keine eingehende Prüfung erwarten lässt.⁵⁵

Neben das Risiko der Verwertung der Daten durch staatliche Stellen tritt das Risiko, dass diese Daten unzulässigerweise durch Private genutzt werden. Sei es direkt durch den Provider oder durch Kriminelle die sich durch Hackerangriffe Zugang zu den Daten verschaffen. Insofern trifft den Staat eine Schutzpflicht bzgl. dieser Daten, der er m. E. alleine durch den Erlass von Sicherheitsvorschriften nicht genügen kann. Da der Staat die Privaten zur Erhebung der Daten verpflichtet, ist ihm das Missbrauchsrisiko durch diese im Rahmen der grundrechtlichen Abwägung zuzurechnen.

Die Vorratsdatenspeicherung als flächendeckende, anlasslose Speicherung hochsensibler⁵⁶ Daten stellt den bisher intensivsten Eingriff in Art. 10 GG dar. Darüber hinaus greift die Speicherung in die Beziehung vieler Berufsgeheimnisträger ein. Abgeordnete, Strafverteidiger, Journalisten, sie alle können sich nicht mehr über elektronische Kanäle mit ihren Informanten/Mandanten austauschen, ohne eine Entdeckung der Kommunikation auch sechs Monate später befürchten zu müssen. Ein Verwertungsverbot dieser Daten, wie es § 53 a StPO teilweise für diese Daten aufstellt, kann dieses Vertrauen nicht wiederherstellen, da es den Ermittlern schon genügt, zu wissen, dass sie womöglich in eine bestimmte Richtung ermitteln müssen. Als

Beweismittel sind die Daten dabei nicht von Nöten.

Ein „Ja, aber ...“ kann es bei der Vorratsdatenspeicherung nur insoweit geben, als die Abrufbefugnisse eingeschränkt werden. Dies aber würde das Vertrauen der Bürger in moderne Telekommunikationsmittel nicht wieder herstellen.

Demgegenüber steht ein zu erwartender äußerst geringer Nutzen bei der Aufklärung von Straftaten, der sich nach Schätzungen lediglich in einer im Promille-Bereich liegenden erhöhten Aufklärungsquote zeigen wird.⁵⁷

Damit ist die Rechtmäßigkeit der Vorratsdatenspeicherung bei Anlegung des grundgesetzlichen Grundrechtsmaßstabs jedenfalls höchst fraglich.

Allerdings ist das Gericht aufgrund des Geltungsvorrangs des Gemeinschaftsrechts gehindert diesen Maßstab einfach anzulegen, nationale Umsetzungsakte europäischen Gemeinschaftsrechts haben sich vor dem BVerfG bisher immer als grundrechtsimmun erwiesen.⁵⁸

Die relevante Frage ist demnach lediglich, wie das Bundesverfassungsgericht in Zukunft sein Verhältnis zum EuGH definieren wird.

Sollte die Nichtigkeitsklage Irlands vor dem EuGH Erfolg haben, stellt sich diese Frage nicht mehr. Dass diese Klage nicht aussichtslos ist, sieht auch der Senat so.⁵⁹

Vor diesem Hintergrund ist m. E. die ganze Entscheidung zu sehen. Wie schon bei der Frage, ob das Gericht überhaupt Gesetze, die auf Europarecht basieren, einstweilig außer Kraft setzen darf, lässt sich das Bundesverfassungsgericht hier alle Möglichkeiten offen. Wollte der Senat unter allen Umständen an seiner Solange-Rechtsprechung festhalten, hätte es die Verfassungsbeschwerde jedenfalls teilweise als offensichtlich unzulässig abweisen müssen, wie es das in der Vergangenheit selbstverständlich getan hat.⁶⁰ Der Senat stellt ja fest, dass sich die Beschwerde größtenteils gegen Normen richtet, die sich auf die Umsetzung von Gemeinschaftsrecht beziehen. Ginge der Senat, wie bisher, stets davon aus, dass der EuGH den Grundrechtsstandard in der Europäi-

schen Union aufrecht erhält, hätte er insoweit eine offensichtliche Unzulässigkeit annehmen können.

Hierin scheint sich der Senat jedoch nicht sicher zu sein. Die Einschätzung des Gerichts, ob der EuGH dazu in der Lage ist, wird wohl maßgeblich vom Ausgang der Nichtigkeitsklage abhängen. Lässt der EuGH die Richtlinie passieren, wird der Senat Farbe bekennen müssen.

Keine Kompetenz-Kompetenz

Er kann unter Rückgriff auf die Maastricht-Entscheidung seine Prüfungskompetenz dahingehen wieder aufleben lassen, ob Gemeinschaftsrecht die Grenzen des deutschen Zustimmungsgesetzes zum EG-Vertrag überschreitet.⁶¹ Dies hat sich das BVerfG in mit den Worten: „Dementsprechend prüft das Bundesverfassungsgericht, ob Rechtsakte der europäischen Einrichtungen und Organe sich in den Grenzen der ihnen eingeräumten Hoheitsrechte halten oder aus ihnen ausbrechen“⁶² eindeutig vorbehalten. Dies ist aus Sicht des nationalen Rechts auch korrekt und nachvollziehbar. Die EG erhält ihre Kompetenz zum Erlass von Rechtsnormen kraft der mitgliedstaatlichen Ermächtigung. Diese Ermächtigung ist in der Zustimmung zum EG-Vertrag zu sehen. Erlässt die EG daher eine Richtlinie, die nicht vom nationalen Zustimmungsgesetz gedeckt ist, fehlt es an einer demokratischen innerstaatlichen Legitimation, die den Staat binden könnte, die Richtlinie umzusetzen. Bei der Frage, ob die EG daher ihre Kompetenz überschritten hat, handelt es sich um eine Frage des nationalen Rechts, die das BVerfG zu entscheiden hat.

Der Europäischen Gemeinschaft fehlt insofern eine Kompetenz-Kompetenz, der es ihr erlauben würde, sich selbst neue Kompetenzen zu schaffen. Die Mitgliedsstaaten haben lediglich Einzelkompetenzen auf die EG übertragen. Die Entwicklung einer Kompetenz-Kompetenz verstieße aus nationaler Sicht gegen Art. 23 Abs. 1 Satz 2 GG.

Sollte das Gericht dabei zu dem Schluss kommen, dass die Richtlinie nicht im Rahmen der Kompetenzen des EG für den einheitlichen Binnenmarkt hätte zustande kommen dürfen, kann es die Nichtanwendung der Richtlinie für Deutschland anordnen und die Vorratsdatenspeicherung voll am Grundgesetz prüfen.

⁵⁵ Albrecht/Grafe/Kilching, Rechtswirklichkeit der Auskunftserteilung über

Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO, S. 410, ; zu finden unter <http://www.vorratsdatenspeicherung.de/images/m-pi-gutachten.pdf>
⁵⁶ aaO, S.

⁵⁷ <http://www.heise.de/newsticker/meldung/92746>; Detaillierte Berechnung unter http://www.vorratsdatenspeicherung.de/images/schriftsatz_2008-03-17.pdf

⁵⁸ Holz, NVwZ 2007, 1153ff.

⁵⁹ Abs-Nr. 137

⁶⁰ BVerfG, 1 BvR 2036/05 vom 14.5.2007, Absatz-Nr. 7; BVerfG, 1 BvR 1036/99 vom 9.1.2001, Absatz-Nr. 15;

⁶¹ BVerfGE 89, 155, 188.

⁶² BVerfGE 89, 155, 188.

Nach abgeschlossener Nichtigkeitsklage dürfte das BVerfG in dieser Frage keine Vorlagepflicht nach Art. 234 Abs. 3 EG mehr treffen.⁶³

Solange-Rechtsprechung

Zweite Variante wäre die bereits skizzierte Berufung auf die Solange-Rechtsprechung. Dabei wird insbesondere relevant sein, wie das Bundesverfassungsgericht die Absenkung des Grundrechtsstandards im Einzelfall sehen will. Geht es generell um den Standard aller Grundrechte zusammen, oder um den Standard bei einzelnen Grundrechten.⁶⁴ Da die Solange-Rechtsprechung die Darlegung des Absinkens vom Kläger verlangt, wird ersteres sicher nicht gelingen.

Sollte der EuGH im Rahmen der Nichtigkeitsklage die Gemeinschaftsgrundrechte nicht prüfen, wird das BVerfG nach Art. 234 Abs. 3 EGV verpflichtet sein, bzgl. der Frage der Vereinbarkeit mit Gemeinschaftsgrundrechten im Vorabentscheidungsverfahren vorzulegen.

Kassation des überschießenden Teils

Die letzte Möglichkeit wäre für das Verhältnis zum EuGH wohl die schonendste, aber für das Grundrechte wohl die denkbar schlechteste Alternative: Das Gericht stützt die Vorratsdatenspeicherung auf die verpflichtend umzusetzenden Teile zurecht.

Sollte nach einem positiven Urteil des EuGH ein Rahmenbeschluß aus Europa folgen, um die Vorratsdatenspeicherung einzuführen, hätte das Bundesverfassungsgericht weitaus mehr Möglichkeiten diesen zu Fall zu bringen, als bei einer Richtlinie. Da es diese als Völkerrecht ansieht und nicht als Teil des Gemeinschaftsrechts kann es niedrigere Hürden schaffen, um das Umsetzungsgesetz alleine an den Vorgaben Grundgesetz zu messen.⁶⁵

6 Fazit

Die Entscheidung des Bundesverfassungsgerichts ist zu begrüßen, als sie nicht von einer offensichtlichen Unzulässigkeit der Verfassungsbeschwerde ausgeht.

Der Ausgang der Hauptsache wird maßgeblich davon abhängen, wie der EuGH die Nichtigkeitsklage über die Richtlinie bescheidet und wie Karlsruhe

sein Verhältnis zum EuGH in Zukunft sieht. Dabei bleibt zu hoffen, dass der EuGH die Richtlinie für nichtig erklärt und somit der Weg für das BVerfG frei wird, die Änderungen der StPO und des TKG zur Einführung der Vorratsdatenspeicherung voll am Grundgesetz zu prüfen.

⁶³ Streinz, EGV/EUV, Art. 234 EGV Rdnr. 44

⁶⁴ Papier, Speyerer Vorträge Heft 89, S. 9

⁶⁵ Papier, Speyerer Vorträge Heft 89, S. 10.