Vorratsdatenspeicherung

Eine Übersicht der Rechtslage vor und nach der einstweiligen Anordnung des Bundesverfassungsgerichts

– BVerfG Beschluss vom 11.03.2008 – Az. 1 BvR 256/08 –

stud. jur. Sebastian Sonn, Universität Freiburg

Es überraschte wenig, dass die Wellen des Protestes hoch schlugen, als die Fraktionen von CDU/CSU und SPD im November 2007 schließlich das heftig umstrittene Gesetz zur Neuordnung der verdeckten Ermittlungsmaßnahmen im Strafverfahren und zur Umsetzung der Richtlinie 2006/24/EG[1] im Alleingang gegen den geschlossenen Widerstand der Opposition[2] im Bundestag verabschiedeten; war doch der darin realisierte Gesetzesentwurf zur Umsetzung der EG-Richtlinie hinsichtlich der Vorratsdatenspeicherung (Richtlinie 2006/24/EG), in Form der Neuregelung von Teilen des Telekommunikationsgesetzes und der StPO[3] (Art. 2 TküNG), schon in den vorangegangenen Monaten seit

[1] BGBl I S. 3198, im Folgenden: Telekommunikationsüberwachungs-Novellierungs-Gesetz (TküNG).
[2] Vgl. Abstimmungsergebnis der Abstimmung vom 09.11.2007, bei dem keine Ja-Stimme der Opposition abgegeben wurde, abrufbar unter: http://www.bundestag.de/parlament/plenargeschehen/abstimmung/20071109_teleueberwtel.pdf.
[3] BT-Drucks. 16/5846.

Erlass der Richtlinie auf erheblichen Widerstand in Bundestag[4], Berufsverbänden[5], Literatur[6] und Öffentlichkeit[7] gestoßen. Eine Verfassungsbeschwerde gegen das am 01.01.2008 in Kraft getretene Gesetz war angesichts dessen also vorprogrammiert und wurde bereits am 31.12.2007 in Form eines Antrags auf einstweilige Anordnung zur Aussetzung der streitigen Normen im Namen von 34.000 Beschwerdeführern beim BVerfG in Karlsruhe eingereicht.

Diesem Antrag hat der Senat mit dem Beschluss vom 11.03.2008[8] im Eilverfahren nun teilweise stattgegeben und sich damit offenbar allseitigen Zuspruch gesichert, denn nach der Urteilsverkündung fühlten sich alle Beteiligten in trauter Eintracht ganz besonders in Ihrer Position bestätigt.[9] Erstaunlich, setzt das Gericht doch immerhin den Vollzug eines von der Bundesregierung hart umkämpften Gesetzes – wenn auch vorerst nur vorübergehend – teilweise aus.

Dabei ist offenbar nichts so deutlich, wie es scheint: Die in dem Beschluss vorläufig ihren Höhepunkt findenden, rasch aufeinander folgenden Änderungen der Rechtslage zur Vorratsdatenspeicherung sorgten bereits für Konfusion bei Behörden und Datenschützern.[10] Dies legt die Fragen

[4] Vgl. nur die vorausgehenden Stellungnahmen zahlreicher Abgeordneter (*van Essen* [FDP], *Jelpke* [DIE LINKE] oder *Ströbele* [B90/Grüne]) bei der Bundestagsdebatte zum entsprechenden Gesetzesentwurf der Bundesregierung am 06.07.2007.
[5] Vgl. Stellungnahmen zum Gesetzesentwurf: *Bundesrechtsanwaltskammer* Nr. 31 /2007, S. 34 ff.; *BITKOM* am 19.01.2007, S. 6, 9 f.; Gemeinsame Stellungnahme von *ARD*, *ZDF*, *Deutschem Presserat* und weiteren (Az.: RB 3-4104/11-R5 884//2006).
[6] Vgl. *Gola*/*Klug*/*Reif*, NJW 2007, S. 2599 ff.
[7] Es gab mehrere groß angelegte Protestaktionen, wie z.B. die Demonstration „Freiheit statt Angst“ am 22.09.2007 in Berlin mit geschätzten 15.000 Teilnehmern.
[8] *BVerfG*, Az.: 1 BvR 256/08.
[9] Vgl. die Stellungnahmen des *AK Vorratsdatenspeicherung*, abrufbar unter: http://www.vorratsdatenspeicherung.de/content/view/209/55/lang,de/
aber auch der Bundesregierung, abrufbar unter:
http://www.bmi.bund.de/cln_028/nn_122688/Internet/Content/Nachrichten/Pressemitteilungen/2008/03/Vorratsdatenspeicherung.html.
[10] Vgl. nur die gegensätzlichen Kommentare von *BfDI Schaar* und zahlreichen Staatsanwälten sowie dem *BMJ* auf Heise online vom 19.03.2008, abrufbar unter: http://www.heise.de/newsticker/Verfassungsgerichtsentscheidung-zur-Vorratsdatenspeicherung-sorgt-fuer-Konfusion--/meldung/105338.

nahe, wie die Rechtslage derzeit einzuschätzen ist, welchen Weg das BVerfG in dem Beschluss geht und was dieser für die Zukunft der Vorratsdatenspeicherung bedeutet.

I. Die Rechtslage vor der Gesetzesnovelle

Um die aktuelle Rechtssituation angemessen beurteilen und zukünftige Entwicklungen abschätzen zu können, empfiehlt es sich, zunächst die Rechtslage vor dem 01.01.2008 und die Entwicklung der Gesetzgebung zur Vorratsdatenspeicherung genauer zu betrachten.

1. Die Berechtigung zur Verkehrsdatenspeicherung

Bevor es Bestrebungen zur Vorratsdatenspeicherung gab, stellte das TKG a. F. die Möglichkeit zu Erhebung und Verwendung von Verkehrsdaten des Kunden durch den Diensteanbieter bereit, wenn dies für die in Teil 7, Abschnitt 2 genannten Zwecke erforderlich war, § 96 Abs. 1 TKG a. F. Verkehrsdaten sind gem. § 3 Nr. 30 TKG a. F. solche Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Welche dieser Verkehrsdaten gem. § 96 TKG a. F. vom Diensteanbieter erhoben werden durften, war in Abs. 1 aufgeführt und umfasste Anschlusskennungen, Rufnummern, Standortdaten, Beginn und Ende der Verbindungen und dergleichen – kurz: Das Erhebungsrecht erfasste alle Daten, die die Umstände des jeweiligen TK-Dienstes beschrieben, nicht jedoch den Inhalt der Kommunikation. Die auf dieser Grundlage während der Verbindung erhobenen Daten durften wiederum nur dann über das Verbindungsende hinaus verwendet – also weiterhin gespeichert – werden, wenn dies zum Aufbau weiterer Verbindungen oder zu gesetzlich genannten Zwecken (insb. §§ 97, 99, 100, 101 TKG a. F.) erforderlich war, § 96 Abs. 2 TKG a. F. Dies umfasste in erster Linie Zwecke der Entgeltermittlung und Abrechnung, § 97 TKG a. F., so dass der Diensteanbieter Rufnummern, Verbindungszeiten und ähnliches nur dann langfristig speichern durfte,

wenn dies für die Rechnungsstellung zwingend war. Alle Daten, die dafür nicht gebraucht wurden, waren unverzüglich zu löschen, sobald die Verbindung beendet wurde[11], § 97 Abs. 3 S. 2 TKG. Lediglich wenn die davon nicht erfassten Verkehrsdaten zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen und zur Abwehr von Gefahren notwendig waren, war eine kurzfristige Speicherung von Verkehrsdaten (ca. 7 Tage) gem. § 100 Abs. 1 TKG a. F. zulässig[12]. Dafür bedurfte es auch keiner konkreten Störung oder Gefahr[13], es handelte sich also um eine Art von zeitlich stark begrenzter „Vorratsdatenspeicherung". Zu einer Verkehrsdatenspeicherung über den eigenen Bedarf hinaus waren die TK-Anbieter bislang somit weder verpflichtet noch berechtigt[14]. Bestandsdaten, also Daten, die für die Begründung, Änderung oder Beendigung eines Vertragsverhältnisses mit dem Diensteanbieter erhoben wurden[15], waren jedoch bereits vor der Gesetzesnovelle langfristig zu speichern, §§ 111, 95 TKG a. F.

2. Abrufermächtigung der Strafverfolgungsbehörden

Von den Speicherungsmöglichkeiten des Diensteanbieters zu trennen war die Möglichkeit der Strafverfolgungsbehörden, die Herausgabe dieser gespeicherten Daten zu verlangen. Die Pflicht zur Herausgabe der *Verkehrsdaten* an die Strafverfolgung ergab sich nach damaliger Rechtslage aus den §§ 100g Abs. 1, 100h StPO a. F.[16], wonach die Access-Provider auf richterliche Anordnung in all denjenigen Fällen Telekommunikationsverbindungsdaten übermitteln mussten, in denen bestimmte Tatsachen den Verdacht begründeten, dass der Täter eine Straftat von erheblicher Bedeutung begangen, im Falle von Versuchsstrafbarkeiten zu begehen versucht, oder mittels einer „TK-

[11] *AG Darmstadt*, Az.: 300 C 397/04; *LG Darmstadt*, Az.: 25 S 118/05.
[12] *LG Darmstadt*, Az.: 10 O 562/03.
[13] *LG Darmstadt*, Az.: 10 O 562/03.
[14] Vgl. *BVerfG*, NJW 2007, S. 3057.
[15] Vgl. § 3 Nr. 3 TKG a. F.
[16] *AG Offenburg*, Az.: 4 Gs 442/07; *Dietrich*, GRUR-RR 2006, 147.

Endeinrichtung“ begangen hatte. Dagegen konnten die Behörden Auskunft über *Bestandsdaten* auf Grundlage der §§ 113, 111, 95 TKG a. F. ohne richterliche Anordnung erlangen, da diese nicht dem Schutzbereich des Art. 10 GG unterstehen und somit lediglich Schutz durch die jeweiligen Datenschutzbestimmungen erfahren können[17].

3. Sonderproblem der „Flatrates“ i.V.m. dynamischen IP-Adressen

Eine besondere Situation ergab sich im Hinblick auf die Verkehrsdaten der Kunden von Internet-Access-Providern. Im Zuge der seit 2005 steigenden Anzahl von Abmahnverfahren zahlreicher Rechteinhaber gegen Urheberrechtsverletzungen auf Internet-Tauschbörsen, wurde in der Praxis deutlich, welche Bedeutung die Erhebung und Übermittlung persönlicher Daten für die betroffenen Bürger haben kann.

Aber auch abseits der überhand nehmenden Urheberrechtsverletzungen hinterließen Straftäter, beispielsweise im Bereich der Kinderpornografie oder des Terrorismus, Spuren im Netz, die von den Strafverfolgungsbehörden natürlich ausgewertet werden wollten. Dabei wurden die IP-Adressen über bestimmte Tracing-Verfahren ermittelt[18], um die Täter zu identifizieren. Aufgrund des alphanumerischen Aufbaus der Adresse[19], war die tatsächliche Identifizierung jedoch nur dann möglich, wenn der Access-Provider die ermittelte IP-Adresse den Bestandsdaten des jeweiligen Kunden zuordnete, dem diese zum fraglichen Zeitpunkt zugeteilt gewesen war, und diese Information auf Anfrage der Behörden herausgab. Hatte der Täter eine feste IP-Adresse, stellte die Zuordnung keine Schwierigkeit dar, da eine feste IP-Adresse ein Bestandsdatum ist[20], welches vom Diensteanbieter gem. §§ 111, 95 TKG a. F. langfristig gespeichert werden musste. Ein Zugriff der Behörden fand also über §§

[17] *Haß* in *Manssen* (Hrsg.), § 85 TKG (a. F.) Rn 13; *Beck*/*Kreißig*, NStZ 2007, 307.
[18] Sog. „Tracerouting“ = die Rückverfolgung einer IP-Adresse.
[19] Z.B. „84.13.43.245“.
[20] *LG Stuttgart*, CR 2005, 598, 599; *Bär*, MMR 2002, 358, 359.

113, 111, 95 TKG a. F. statt, sodass Name und Anschrift des Täters ermittelt werden konnten. Die absolute Mehrheit der Internet-Access-Provider bietet mittlerweile jedoch nur noch dynamische IP-Adressen an, also solche Adressen, die sich bei jeder Einwahl des Kunden ändern und somit nur dann zugeordnet werden können, wenn sie während der Nutzung erhoben und anschließend auch in Verbindung mit den Bestandsdaten des Kunden gespeichert werden.

Die dynamische IP-Adresse wird jedoch bei jeder Einwahl neu zugeordnet und damit nicht für die Begründung, Änderung oder Beendigung eines Vertragsverhältnisses mit dem Diensteanbieter erhoben, § 3 Nr. 3 TKG a. F.. Sie hat folglich nicht den Charakter eines Bestandsdatums[21], sondern stellt, da sie bei jeder Verbindung neu definiert wird, ein verbindungsbezogenes Verkehrsdatum dar, § 3 Nr. 30 TKG a. F.. Wie jedoch festgestellt, durfte der TK-Anbieter sämtliche Verkehrsdaten nicht über die Beendigung der Verbindung hinaus verwenden, sondern musste diese – innerhalb der 7-Tages-Toleranz aufgrund des § 100 Abs. 1 TKG a. F. – unverzüglich löschen, sofern sie nicht gem. § 96 Abs. 1 Nr. 2, 97 TKG a. F. zur Entgeltabrechnung erforderlich waren.

Zwar ist der dynamischen IP-Adresse im Falle eines Call-by-Call Tarifs zur Einzelabrechnung grundsätzlich ein Abrechnungszweck zuzusprechen[22], denn sie wird in diesem Fall benötigt, um den Anfang und das Ende der Verbindung auf der Rechnung nachzuweisen. Allerdings hat sich in den letzten Jahren aufgrund der flächendeckenden Verfügbarkeit von Breitbandinternetanschlüssen die Vertragsgestaltung in Form von Flatrates durchgesetzt, bei der keine Einzelverbindungen mehr zur Entgeltabrechnung benötigt werden, sondern monatlich ein fester Betrag gezahlt wird, gegen den der Kunde unbegrenzten Internet-Zugang erhält.

[21] *LG Darmstadt* GRUR-RR 2006, 173; *Dietrich*, GRUR-RR 2006, S. 147; *Beck*/*Kreißig*, NStZ 2007, S. 307.
[22] Vgl. *Beck*/*Kreißig*, NStZ 2007, S. 307.

Hierbei ist die IP-Adresse keinesfalls mehr zu Abrechnungszwecken erforderlich[23], womit auch das Recht zur Speicherung nach Beendigung der Verbindung entfällt und die Pflicht für den Diensteanbieter entsteht die Daten unverzüglich zu löschen, § 97 Abs. 3 S. 2 TKG a. F.

Da die dynamische IP-Adresse darüber hinaus als Verkehrsdatum, und damit Information zu näheren Umständen des Fernmeldeverhältnisses, dem Schutzbereich des Art. 10 GG unterfällt[24], konnten die Ermittlungsbehörden nicht auf das unkomplizierte Verfahren der §§ 113, 111, 95 TKG a. F. zurückgreifen sondern mussten auf richterliche Anordnung warten, bevor sie die Daten vom Provider über §§ 100g, 100h StPO a. F. herausverlangen konnten. Als Folge konnten die Strafverfolgungsbehörden nur noch dann Zugriff auf die Identität des Täters erlangen, wenn sie sofort vollumfänglich tätig wurden, nachdem sie die IP-Adresse in Erfahrung gebracht hatten.

II. Die EG-Vorgabe in Form der Richtlinie 2006/24/EG[25]

1. Entstehung

Die Diskussion über eine Speicherung von Telekommunikationsdaten auf Vorrat wurde auf europäischer Ebene erstmals im August 2002 geführt, als die damals ratspräsidentschafts-führende dänische Regierung, einen entsprechenden Entwurf vorlegte, welcher jedoch abgelehnt wurde. Einen erneuten Anstoß gaben die Terroranschläge von Madrid am 11.03.2004 und die zunehmende grenzüberschreitende Kriminalität. Frankreich, Schweden, Großbritannien und Irland brachten einen Entwurf

[23] *LG Darmstadt* GRUR-RR 2006, 173; zust. *Spindler*/*Dorschel* (o. Fn 27); *Dietrich* GRUR-RR 2006, 173; *Gercke* Anm. zu LG Stuttgart CR 2005, 598, 601.
[24] Vgl. *OVG Münster*, NJW 1975, S. 1335; BVerfGE 67, 157, S. 172.
[25] Richtlinie 2006/24/EG v. 15.3.2006 des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsnetze oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. EG Nr. L 105 v. 13.4.2006, S. 54 ff.

für einen Rahmenbeschluss in den Ministerrat ein[26], der innerhalb der dritten Säule der EU eine einheitliche Vorratsdatenspeicherung in Europa herbeiführen sollte. Aufgrund von Streitigkeiten über die Speicherfristen und die Kompetenzen der Strafverfolgung beim Zugriff auf die gespeicherten Verkehrsdaten kam es allerdings nie zu einer einstimmigen Befürwortung im Ministerrat – auch aufgrund massiver Intervention der deutschen Seite, die der Ansicht war der Rahmenbeschluss greife zu weit. Im Spätsommer 2005 wurde schließlich ein Kommissions-Entwurf für eine europäische Richtlinie vorgelegt, der nunmehr nicht mehr in der 3. Säule, sondern innerhalb der ersten Säule der EU – auf die Binnenmarktkompetenz der EG aus Art. 95 EGV gestützt – realisiert werden sollte, wie es dann am 14.12.2005 im schnellsten Verfahren der Geschichte der EU auch geschah.

Die Richtlinie 2006/24/EG ist stark kritisiert worden, da vielfach die Ansicht vertreten wird, sie sei auf der falschen Rechtsgrundlage erlassen worden und die EG habe damit ihre Kompetenzen überschritten[27]. Aufgrund dessen wurde von der Republik Irland und der Slowakei im Juli 2006 auch Klage vor dem EuGH auf Nichtigerklärung der Richtlinie erhoben[28], da man der Auffassung war, eine europäische Regelung zur Vorratsdatenspeicherung könne ausschließlich innerhalb des intergouvernmentalen Bereichs der 3. Säule der EU, der polizeilichen und justiziellen Zusammenarbeit in Strafsachen, erlassen werden. Eine Binnenmarktkompetenz sei hier abzulehnen, zumal auch das Harmonisierungsziel der Richtlinie wenig plausibel erscheint[29]. Betrachtet man die jüngste Rechtsprechung des EuGH zur

[26] Rats-Dokument 8958/04.
[27] *Schaar*, MMR 2006, 425, 426; *Simitis*, NJW 2006, 2011, 2013; *Westphal*, EuZW 2006, 555, 557; *Gitter*, MMR 2007, S. 413.
[28] Rs. C-301/06 Irland gegen den Rat der Europäischen Union und das Europäische Parlament, abrufbar unter: http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?where=&lang=de&num=79939084C19060301&doc=T&ouvert=T&seance=REQ_COMM.
[29] *Gitter*, MMR 2007, S. 412.

Fluggastdatenspeicherung, in der der Gerichtshof bei vergleichbarer Lage eine Annexkompetenz der EG ablehnt[30], so würde es kaum überraschen, sollte er auch dieser Klage stattgeben und die RL 2006/24/EG für nichtig erklären.

2. Inhalt

Die RL 2006/24/EG gibt den Mitgliedsstaaten auf, durch entsprechende Maßnahmen dafür Sorge zu tragen, dass Anbieter öffentlich zugänglicher elektronischer Telekommunikationsdienste und Betreiber öffentlicher Kommunikationsnetze Verkehrs- und Standortdaten zum Zwecke der Ermittlung, Feststellung und Verfolgung schwerer Straftaten auf Vorrat gespeichert werden, Art. 1, 2 Abs. 2 a), 3 Abs. 1 RL 2006/24/EG. Was genau diese schweren Straftaten sind, haben die Mitgliedsstaaten ebenso wie die Speicherfristen[31] selbst zu bestimmen, Art. 1 Abs. 1 RL 2006/24/EG. Die Richtlinie bleibt mit diesen Regelungen hinter den tiefgreifenderen vorausgegangenen Entwürfen von 2004 und 2005 zurück, indem sie die minimale Speicherfrist auf 6 Monate senkt und die Zugriffsmöglichkeiten durch die Strafverfolgung auf schwere Straftaten begrenzt. Allerdings wird letzteres dadurch eingegrenzt, dass die Mitgliedsstaaten die Schwere der erforderlichen Straftaten selbst bestimmen können, wobei mit Blick auf den Normzweck auch nicht übersehen werden darf, dass die EG damit wohl kaum die Tore für die Erfassung jeder noch so geringfügigen Straftat öffnen wollte.

Zwingend vorgegeben wurde dem deutschen Gesetzgeber damit im Ergebnis bis zum 15. September 2007 (mit Aufschubsfrist bis zum 15. März 2009) eine Gesetzeslage zu schaffen, die die TK-Diensteanbieter und Netzbetreiber verpflichtet, die in Art. 5 RL 2006/24/EG katalogisierten Verkehrs- und Standortdaten, also umfassende Informationen zum “Ob“

[30] *EuGH,* 2006/C 178/02.
[31] mindestens 6 Monate und höchstens 2 Jahre, Art. 6 RL 2006/24/EG.

und „Wie“ der Telekommunikation, mindestens 6 Monate vorzuhalten und den Strafverfolgungsbehörden im Falle schwerer Straftaten zu übermitteln.

III. Die Umsetzung des deutschen Gesetzgebers

Der deutsche Bundestag hat diese Frist ungeachtet der ausstehenden EuGH Entscheidung sogar unterschritten und ist den Forderungen der Richtlinie mit dem TküNG bereits zum 01. Januar 2008 nachgekommen.

1. Die Pflicht zur Vorratsdatenspeicherung von Verkehrsdaten

Der Gesetzgeber hat den Anbietern öffentlicher TK-Dienste mit dem TküNG entsprechend der Richtlinie umfangreiche Speicherungspflichten von Verkehrsdaten auferlegt. Hierfür wurde gem. Art. 2 Nr. 6 TküNG der neue § 113a TKG in das Telekommunikationsgesetz eingeführt. Danach haben TK-Diensteanbieter die bei der Nutzung des Dienstes erzeugten Verkehrsdaten nach Maßgabe des Abs. 2 sechs Monate lang zu speichern. Eine Pflicht zur Erhebung neuer Daten ist dabei nicht festgesetzt: Es sind lediglich Verkehrsdaten zu speichern, die ohnehin anfallen. Die näheren Umstände der Speicherung werden in § 113a Abs. 2 – 4 TKG festgelegt. Die Speicherpflicht umfasst danach die Rufnummer der Teilnehmer an einem Telefongespräch, Beginn und Ende der Verbindung, Angaben zum genutzten Dienst, die Gerätekennung bei Mobiltelefonen und im Falle von VoIP-Telefonaten die IP-Adresse des Angerufenen[32]. Anbieter von E-Mail Diensten sind verpflichtet, die Kennung und IP-Adresse des Absenders, die Kennung des Empfängers und die IP-Adresse des Abrufenden der E-Mail zu speichern[33]. Internet-Access-Providern wird schließlich die Pflicht auferlegt, Informationen über die IP-Adresse, die Kennung des Anschlusses und den Beginn und das Ende der Internetnutzung des Teilnehmers vorzuhalten[34]. § 113a Abs. 6 TKG bestimmt ferner, dass Anbieter, die Dienste führen, welche nach

[32] vgl. 113a Abs. 2 TKG.
[33] vgl. 113a Abs. 3 TKG.

§ 113a Abs. 2 – 5 TKG zu speichernde Daten verändern, verpflichtet werden, die ursprünglichen und die neuen Daten aufzubewahren und die Änderung damit zu dokumentieren. Dies zielt in erster Linie auf Anonymisierungsdienste ab, welche die IP-Adressen der Nutzer gezielt verfälschen, um diesen ein Mittel zum Selbstdatenschutz an die Hand zu geben[35]. Die Verkehrsdaten müssen schließlich gem. § 113a Abs. 9 TKG so aufbewahrt werden, dass sie bei Auskunftsersuchen durch die Behörden unverzüglich zum Abruf bereit stehen.

2. Verwendungsrecht

Die Datenverwendung wird durch § 113b TKG geregelt, wonach der Anbieter alle Verkehrsdaten, welche aufgrund § 113a TKG gespeichert worden sind, ausschließlich zur Verfolgung von Straftaten, zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit oder zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden und der Nachrichtendienste übermitteln muss, soweit dies in den jeweiligen Normen unter Bezugnahme auf § 113a TKG so bestimmt ist. Außerhalb dieser Bereiche darf er die Daten – mit Ausnahme für die Auskunftserteilung nach § 113 TKG – nicht verwenden[36]. Damit hat der Gesetzgeber umfangreichen Gebrauch von seiner Konkretisierungskompetenz gemacht und ist weit über die Vorgaben der Richtlinie hinausgegangen, die einen Zugriff auf die Vorratsdaten lediglich zur Ermittlung, Feststellung und Verfolgung schwerer Straftaten vorsehen, Art. 1 RL 2006/24/EG. Präventivpolizeiliche oder gar geheimdienstliche Zwecke sind dort nicht vorgesehen. Es ist allerdings zu beachten, dass derzeit keine fachrechtlichen Abrufermächtigungen existieren, die ausdrücklich Bezug auf § 113a TKG nehmen, womit zumindest § 113b S. 1 Nr. 2 TKG bislang noch leer läuft[37].

[34] vgl. 113a Abs. 4 TKG.
[35] vgl. *Gitter*, MMR 2007, S. 415.
[36] vgl. § 113b TKG.
[37] *BVerfG*, 1 BvR 256/08, Rn. 186.

3. Abrufermächtigung der Strafverfolgungsbehörden

Die Abrufermächtigung der Strafverfolgungsbehörden ist in dem durch Art. 1 TküNG ebenfalls neu gestalteten § 100g StPO näher bestimmt. Darin wird die Erhebung der aufgrund von § 113a TKG gespeicherten Verkehrsdaten (§ 96 Abs. 1 TKG) dann gestattet, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand eine Straftat von erheblicher Bedeutung begangen oder bei Versuchsstrafbarkeiten zu begehen versucht hat und das Erheben dieser Verkehrsdaten erforderlich ist, um den Sachverhalt zu erforschen oder den Aufenthaltsort des Beschuldigten zu ermitteln, § 100g Abs. 1 Nr. 1 StPO. Darüber hinaus wird die Möglichkeit einer solchen Erhebung auch für den Fall, dass eine Straftat mittels Telekommunikation begangen wurde, eröffnet, § 100g Abs. 1 Nr. 2 StPO.

Besonders hervorzuheben ist zunächst die Formulierung „Straftat von auch im Einzelfall erheblicher Bedeutung“, womit der Gesetzgeber über die Vorgaben der Richtlinie, welche lediglich „schwere Straftaten“ nennt, hinaus geht. Der Strafverfolgung wird nicht nur beim Vorliegen schwerer, sondern auch beim Vorliegen von Straftaten von erheblicher Bedeutung ein Abruf ermöglicht. Zwar verweist § 100g Abs. 1 Nr. 1 StPO beispielhaft auf die in § 100a Abs. 2 StPO genannten Straftaten, welche vom Gesetzgeber als „schwere Straftaten“ definiert werden, jedoch wird die Abrufermächtigung nicht auf diese Straftaten begrenzt, sondern gilt ausdrücklich auch für andere Straftaten. Durch den Verweis auf § 100b Abs. 1 – 4 StPO wird mit § 100b Abs. 2 StPO sicher gestellt, dass der Abruf der Verkehrsdaten nur durch richterliche Anordnung und auf Antrag der Staatsanwaltschaft geschehen darf.

Ferner wurde die Ermächtigung nicht nur auf Straftaten von erheblicher Bedeutung, sondern auf alle Straftaten, die mit Telekommunikation begangen wurden, erweitert, § 100g Abs. 1 Nr. 2 StPO. Dies eignet sich

jedoch nur dann als Anordnungsgrundlage, sofern die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht, § 100g Abs. 1 S. 2 StPO. Damit öffnet der Gesetzgeber die Verwendung der Vorratsdaten für die Verfolgung von Straftaten, welche von der Richtlinie ausdrücklich nicht vorgesehen waren. Da es sich bei diesen Straftaten in den allermeisten Fällen um Urheberrechtsverletzungen über das Internet, also illegale Musik-, Software- und Film-Downloads handeln wird, liegt die Vermutung nahe, dass der Zusatz durchaus zur Beruhigung der Unterhaltungsindustrie und auf deren Lobbyarbeit zurückzuführen ist.

Festzuhalten bleibt also, dass die bislang bestehende Abrufermächtigung der Strafverfolgungsbehörden mit dem TküNG auf nach § 113a TKG gespeicherte Verkehrsdaten erweitert wurde und diese auch zur Verfolgung von Straftaten von erheblicher Bedeutung sowie mit Telekommunikation begangener Straftaten zur Verfügung stehen. Einschränkend hat der Gesetzgeber mit dem Verweis auf § 100 Abs. 2 StPO dahin gewirkt, dass Verkehrsdaten nur noch auf richterliche Anordnung abgerufen werden dürfen. Unverändert bleibt die Ermächtigung der Strafverfolgungsbehörden auf die Bestandsdaten, welche weiterhin auf § 113, 111, 95 TKG gestützt wird.

4. Folgen der Gesetzgebung für das Sonderproblem der „Flatrates“ i.V.m dynamischen IP-Adressen

Dynamische IP-Adressen werden in der neuen Fassung des TKG ausdrücklich von § 113a Abs. 4 Nr. 1, Nr. 3 TKG unabhängig vom Abrechnungszweck erfasst. Es spielt daher keine Rolle mehr, ob es sich bei der Vertragsgestaltung um Flatrates oder andere Tarife handelt, womit sich das oben dargestellte Problem nach der Gesetzesnovelle nicht mehr stellt.

5. Kurzer Überblick über die Kritik am TküNG

Die Gesetzesnovelle hinsichtlich der Vorratsdatenspeicherung wurde von Öffentlichkeit und Fachkreisen äußerst negativ aufgenommen und vehement als verfassungswidrig kritisiert[38]. Ansatzpunkte für die Kritik finden sich in erster Linie in den erheblichen grundrechtlichen Einschränkungen, welche sich aus den Regelungen zur Vorratsdatenspeicherung ergeben. Dabei wird insbesondere darauf verwiesen, dass die Vorratsdatenspeicherung der Verkehrsdaten einen erheblichen Eingriff in die von Art. 10 GG geschützte Vertraulichkeit der Fernkommunikation darstellt[39]. Darüber hinaus liegt auch ein Eingriff in das Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG vor, welches jedoch gegenüber der spezielleren Gewährleistung aus Art. 10 GG zurücktritt[40]. Eine Einschränkung der Vertraulichkeit der Fernkommunikation ist gem. Art. 10 Abs. 2 GG zwar grundsätzlich, jedoch nicht grenzenlos zulässig. Das grundrechtseinschränkende Gesetz ist vielmehr seinerseits anhand der grundlegenden Bedeutung der die Privatsphäre sichernden Grundrechte (Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG, Art. 10 GG, Art. 13 GG) auszulegen und so in seiner eingreifenden Wirkung selbst im Lichte der Grundrechte einzuschränken[41]. Die Eingriffsqualität in Art. 10 GG ist nicht erst durch den staatlichen Zugriff auf die gespeicherten Verkehrsdaten erfüllt, sondern besteht bereits durch die Speicherungspflicht der Daten aller Kommunikationsteilnehmer[42]. Allein das Wissen darum, dass die bei der Kommunikation erzeugten Verbindungsdaten gespeichert und zu späterem Abruf zur Verfügung stehen, schränkt den Kommunikationsteilnehmer erheblich in seiner unbefangenen Nutzung des

[38] Vgl. *Gola*/*Klug*/*Reif*, NJW 2007, S. 2599 ff.; *Simitis* RDV 2007, S. 143 ff.; Die Zeit online vom 27.12.2007, abrufbar unter: http://www.zeit.de/online/2007/52/vorratsspeicherung.
[39] *Ulmer*/*Schrief*, DuD 2004, S. 594; *Gitter*, MMR 2007, S. 413.
[40] BVerfGE 100, 313, S. 358; 110, 33, S. 53 (st. Rspr.).
[41] Sog. Schranken-Schranke, vgl. BVerfGE 67, 157, S. 172; BVerfGE 59, 231, S. 264 f. (st. Rspr.).

Kommunikationsmittels ein und verursacht ein Gefühl des Überwachtwerdens[43].

Fraglich bleibt, ob dieser Eingriff eine verfassungsrechtliche Rechtfertigung haben kann. Bereits bei der Frage der Bestimmtheit, ergeben sich hier jedoch Zweifel, da nach den Grundsätzen des Volkszählungsurteils[44] ein Eingriff in die Privatsphäre – und damit auch die Vertraulichkeit der Fernkommunikation – nur dann gerechtfertigt sein kann, wenn der Verwendungszweck präzise bestimmt ist. § 113b TKG nennt jedoch lediglich die „Verfolgung von Straftaten“ und damit die Effektivität der Strafverfolgung als Ziel, was jedoch zwingend zu uferlosen Maßnahmen führen würde und damit nicht als Normzweck taugt. Die Norm kann also bereits dem Bestimmtheitsgrundsatz nicht gerecht werden[45].

Darüber hinaus scheint die Geeignetheit der Vorratsdatenspeicherung zur Bekämpfung organisierter Kriminalität äußerst zweifelhaft. Abgesehen von den einfachen Möglichkeiten, die Straftäter zur Verschleierung ihrer Spuren im Internet nutzen können[46], ist auch kaum damit zu rechnen, dass Verkehrsdaten zur Aufklärung schwerer Straftaten führen können, denn Inhaltsdaten dürfen ja gerade nicht gespeichert werden. Dementsprechend können die Ermittler zwar feststellen, wem eine bestimmte IP zugeordnet war, diese muss hierfür jedoch zunächst bei einer Straftat im Internet aufgegriffen werden. Der Abgleich mit den nach § 113a TKG gespeicherten Daten soll dann in erster Linie die Identifizierung des Täters bewirken. Die Hauptproblematik ist jedoch, dass Täter schwerer Straftaten, die es gemäß der Richtlinie in erster Linie

[42] *BVerfG*, NJW 2000, S. 59; *Gitter*, MMR 2007, S. 413; *Gola*/*Klug*/*Reif*, NJW 2007, S. 2599.
[43] *BVerfG*, NJW 2003, S. 1793.
[44] BVerfGE 65, 1.
[45] *Simitis*, RDV 2007, S. 146; *Gola*/*Klug*/*Reif*, NJW 2007, S. 2599.

anzuvisieren gilt, sich meist zu geschickt verhalten, als dass sie überhaupt verwertbare Spuren im Netz hinterlassen, die lediglich noch eines Abgleichs bedürfen. Hier bescheinigt eine kürzlich erschienene Studie des Freiburger Max Planck Instituts für ausländisches und Internationales Strafrecht[47], dass die Zugriffe der Strafverfolgungsbehörden der letzten Jahre sich zu 50 % mit Betrug und zu 25 % mit Urheberrechtsdelikten befasst haben. Der als Hauptargument für die Vorratsdatenspeicherung vorgebrachte Bereich des Terrorismus spielt bei den bislang vorgenommenen Abfragen dagegen keinerlei Rolle[48].

Jedenfalls scheint die Vorratsdatenspeicherung auch keinen angemessenen Eingriff in Art. 10 GG darzustellen. Eine unbefangene und freie Kommunikation der Bürger ist die absolute Grundvoraussetzung zur Gewährleistung einer freien demokratischen Gesellschaft, denn nur so ist eine aktive staatliche Mitwirkung des Volkes gewährleistet. Demgegenüber wiegt der Zweck, die Strafverfolgung effektiver zu gestalten, erheblich geringer, zumal nur ein minimaler Teil der gespeicherten Daten überhaupt in diesem Rahmen zum Einsatz kommen würde[49].

Neben dem Eingriff in Art. 10 GG wird ferner der Eingriff in die Pressefreiheit gem. Art. 5 Abs. 1 S. 2 Var. 1 GG kritisiert, da Befürchtungen bestehen, dass sich Informanten aufgrund enorm erhöhter Entdeckungsgefahr aus der Kommunikation mit der Presse zurückziehen werden[50].

---

[46] Z.B. IP-Verschleierung mit Programmen wie Tor oder Privoxy, vgl. Heise Online vom 15.03.2007, abrufbar unter: http://www.heise.de/tp/r4/artikel/24/24778/1.html.
[47] „Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO“, abrufbar unter: http://www.bmj.de/files/7d48ca9ff0c0b6994570498ea2757477/3045/MPI-GA-2008-02-13%20Endfassung.pdf.
[48] Vgl. MPI-Gutachten [Fn. 47], S. 159.
[49] *Gola*/*Klug*/*Reif*, NJW 2007, S. 2600.
[50] So *Gola*/*Klug*/*Reif*, NJW 2007, S. 2600; vgl. auch *BVerfG*, NJW 2003, S. 1793.

Zusammenfassend muss sich der Gesetzgeber die Kritik gefallen lassen, dass der Erlass des TküNG bei diesen erheblichen Zweifeln an der Verfassungsmäßigkeit der Vorratsdatenspeicherung und an der Rechtmäßigkeit der Richtlinie auf europäischer Ebene vorschnell und unangebracht war. Ratsam wäre gewesen, zumindest das ausstehende Urteil des EuGH abzuwarten, bevor Gesetze zur Vorratsdatenspeicherung erlassen werden. Ende 2007 wurde daher eine in diesem Umfang in der Geschichte der BRD nie dagewesene Massen-Verfassungsbeschwerde und ein Antrag auf einstweilige Aussetzung der §§ 113a, 113b TKG beim BVerfG eingereicht.

IV. Die einstweilige Anordnung des Bundesverfassungsgerichts (Az. 1 BvR 256/08)

1. Prüfungskompetenz des Bundesverfassungsgerichts

Die Bundesregierung bezweifelte bei diesem Antrag bereits die Prüfungskompetenz des BVerfG und bestritt daher die Zulässigkeit der Verfassungsbeschwerde. Die Zweifel ergaben sich daraus, dass die streitgegenständlichen Normen aufgrund zwingender Vorgaben einer europäischen Richtlinie erlassen worden sind und daher gemäß den Grundsätzen der Solange II-Entscheidung nur dann vom BVerfG überprüft werden können, wenn die EG im Bereich der betroffenen Grundrechte nicht einen vom Grundgesetz als unabdingbar angesehenen Grundrechtsschutz gegenüber europäischer Hoheitsgewalt gewährleistet.[51] Vorliegend wird jedoch über europäische Grundrechte, insbesondere Art. 8 EMRK und Art. 7, 8 GrCH, ein hinreichender Schutz geboten, womit das BVerfG die Normen nicht am GG messen darf. Allerdings gilt dies nur insoweit, als sich der deutsche Gesetzgeber bei der Umsetzung an zwingende Vorgaben einer Richtlinie gehalten hat. Das BVerfG kann die Umsetzung hingegen dahingehend überprüfen, soweit

die nationale Umsetzung über die Richtlinie hinaus geht, oder der Gesetzgeber die Vorgaben in eigener Kompetenz konkretisiert hat[52]. Der Gesetzgeber ist darüber hinaus grundsätzlich zu einer grundrechtsschonenden Umsetzung verpflichtet[53]. Dies ist vorliegend insbesondere hinsichtlich der Abrufermächtigung der Strafverfolgungsbehörden, aber auch hinsichtlich einiger Speicherungspflichten[54], nicht geschehen. Die Umsetzung geht über die zwingenden Vorgaben hinaus und konkretisiert diese in eigener Kompetenz, weshalb das BVerfG die davon betroffenen Regelungen überprüfen kann[55].

2. Der Beschluss

Eine einstweilige Anordnung kann das Gericht dann erlassen, wenn dies zur Abwehr schwerer Nachteile dringend geboten ist, § 32 BVerfGG. Darüber hinaus stellen die Richter eingangs fest, dass bei der vorliegenden Entscheidung besonders hohe Grenzen zu beachten sind, da es über die vorläufige Aussetzung des Vollzugs eines Gesetzes, das aufgrund von zwingenden Richtlinienvorgaben erlassen wurde, entscheiden muss[56]. Eine solche Entscheidung darf nur dann ergehen, wenn den Betroffenen durch den Vollzug des Gesetzes ein besonders schwerwiegender und irreparabler Schaden droht, dessen Gewicht das Interesse der Gemeinschaft am effektiven Vollzug des Gemeinschaftsrechts – und das damit zusammenhängende Risiko, die dem Gericht zustehende Entscheidungskompetenz im Eilverfahren zu überschreiten – entscheidend überwiegt[57].

[51] Vgl. BVerfGE 73, 339, S. 387; BVerfGE 102, 147, S. 162 ff.
[52] *BVerfG*, BvR 1 256/08, Rn. 135.
[53] *BVerfG*, NJW 2005, S. 2291; *Gola*/*Klug*/*Reif*, NJW 2007, S. 2601.
[54] Z.B. § 113a Abs. 6 TKG.
[55] *BVerfG*, BvR 1 256/08, Rn. 135.
[56] *BVerfG*, BvR 1 256/08, Rn. 144; vgl. auch *EuGH*, C-143/88, C-92/89; *EuGH*, C-334/95; *EuGH*, C-461/03.
[57] *BVerfG*, BvR 1 256/08, Rn. 145.

Eine Aussetzung des Vollzugs von § 113a TKG im Eilverfahren schließt das BVerfG aus. Zunächst stellt es fest, dass diese Norm in weiten Teilen den zwingenden Richtlinienvorgaben entspreche und daher ohnehin nicht in seine Entscheidungskompetenz falle – zumindest solange noch keine Entscheidung des EuGH zur Nichtigkeit der Richtlinie ergangen sei. Darüber hinaus ließe sich im zeitlich begrenzten Rahmen bis zum Hauptverfahren auch kein irreparabler Nachteil für den betroffenen Kommunikationsteilnehmer durch die bloße Speicherung feststellen. Zwar unterstreicht das Gericht den erheblichen Einschüchterungseffekt der Speicherung auf Vorrat[58], jedoch verdichte sich der Nachteil für die Freiheit des Einzelnen während des Zeitraums zwischen Eilverfahren und Hauptentscheidung erst im Abruf der gespeicherten Daten zu einer irreparablen Beeinträchtigung[59]. Das BVerfG sieht hier also keinen Handlungsbedarf, sondern beschränkt sich darauf die Weite der Übermittlungsermächtigung in § 113b TKG zu verringern.

Der Senat gibt dabei nochmals zu bedenken, dass bei einer Entscheidung im Eilverfahren der Nachteil für die Betroffenen, falls sich die streitigen Normen im Hauptverfahren als verfassungswidrig herausstellen sollten, gegen den durch die Aussetzung des Vollzugs entstehenden Nachteil, falls sich die Normen im Hauptverfahren als verfassungskonform darstellen sollten, abzuwägen ist. Diesen Konflikt löst der Beschluss damit, dass er den Strafverfolgungsbehörden die Ermächtigung zum Abruf der Daten gem. § 100g StPO belässt und stattdessen den TK-Diensteanbietern vorerst untersagt, diese Daten zu übermitteln. Die Behörden haben demnach keine Einsichtsmöglichkeit, was eine irreparable Beeinträchtigung der Betroffenen verhindert. Gleichzeitig bleiben die Anbieter nach dem Abrufersuchen jedoch verpflichtet die angeforderten Daten aus der Masse der Vorratsdaten zu erheben und –

[58] *BVerfG*, BvR 1 256/08, Rn. 148.
[59] *BVerfG*, BvR 1 256/08, Rn. 149.

für den Fall, dass sich die streitigen Normen als verfassungsgemäß herausstellen sollten – bis nach dem Hauptsacheverfahren zur Übermittlung bereit zu halten. Die so beantragten Daten stünden den Behörden also nachträglich noch immer zum Abruf zur Verfügung. Damit ist die potentielle Gefahr, dass der Strafverfolgung ein effektives Ermittlungswerkzeug verloren geht, minimiert und der einzige Nachteil besteht in einer Verzögerung des Ermittlungsverfahrens.

Dieses Ergebnis ist zu unterstreichen, zumal die Provider ohnehin erst ab August 2008 zur Umsetzung der Vorratsdatenspeicherung verpflichtet sind und derzeit noch keiner der Anbieter eine entsprechende Umsetzung vorweisen kann, was sich bis 2009 auch kaum ändern wird[60].
Die Nachteile, die sich für die Betroffenen ergeben könnten, sind dagegen aufgrund der erheblichen Streubreite bei einem Abruf der Verkehrsdaten grundsätzlich beträchtlich, denn es wird nicht nur der Verdächtigte erfasst, sondern auch seine vom Tatvorwurf selbst nicht betroffenen Kommunikationspartner[61]. Würden sich die Regelungen anschließend als verfassungswidrig herausstellen, würden auf Grundlage der Vorratsdatenspeicherung ergangene Verurteilungen auf Beweismitteln beruhen, die nicht hätten gewonnen werden dürfen[62]. Diesen Nachteil bewertet das BVerfG bei Straftaten außerhalb des § 100a StPO zu Recht schwer wiegender als die Nachteile für die Strafverfolgung:

> *„Ein solcher Datenabruf ermöglicht es, weitreichende Erkenntnisse über das Kommunikationsverhalten und die sozialen Kontakte des Betroffenen zu erlangen. Zudem werden in vielen Fällen die durch den Verkehrsdatenabruf erlangten Erkenntnisse die Grundlage für weitere Ermittlungsmaßnahmen bilden."*

[60] Vgl. die Übersicht der entsprechenden Umsetzungsdaten der einzelnen Providern unter http://wiki.vorratsdatenspeicherung.de/Provider#.C3.9Cbersicht.
[61] BVerfGE 107, 299, S. 318 ff.
[62] *BVerfG*, BvR 1 256/08, Rn. 158.

Allerdings schränkt das Gericht diese Bewertung für diejenigen Fälle, bei denen es um Katalogtaten des § 100a Abs. 2 StPO geht, folgendermaßen ein:

„Soweit das Ermittlungsverfahren […] sich auf eine Straftat bezieht, die in dem Katalog des § 100a Abs. 2 StPO aufgeführt ist, hat das öffentliche Strafverfolgungsinteresse […] grundsätzlich derartiges Gewicht, dass eine Verzögerung durch eine einstweilige Anordnung nicht hingenommen werden kann."

Dies kann nach Ansicht der Karlsruher Richter aber nur für solche Straftaten, die darüber hinaus auch im Einzelfall schwer wiegen (vgl. §§ 100a Abs. 1 StPO), gelten.

Der Senat begrenzt den Vollzug des § 113b TKG also derart, dass die TK-Anbieter auf Abrufersuchen der Strafverfolgungsbehörden auf Grundlage des § 100g StPO die geforderten Daten zwar erheben und bis zum Hauptverfahren speichern müssen, jedoch nur dann sofort übermitteln dürfen, wenn Gegenstand des Ermittlungsverfahrens eine Katalogtat i.S.d. § 100a Abs. 2 StPO ist bei der darüber hinaus die Voraussetzungen des § 100a Abs. 1 StPO vorliegen.

Damit wird der Vorratsdatenzugriff bei Ermittlungen zu erheblichen Straftaten, schweren Straftaten außerhalb des § 100a Abs. 1 StPO, und Straftaten, welche mit Telekommunikation begangen wurden, vorerst unterbunden. Weitere Einschränkungen – etwa hinsichtlich der Übermittlungsberechtigung für Präventivmaßnahmen und Geheimdienste in § 113b S. 1 Nr. 2, Nr. 3 TKG – nimmt das Gericht nicht vor, da hierfür noch keine Bezug nehmenden Regelungen existieren und somit für die Zeit bis zum Hauptsacheverfahren keine Nachteile für die Betroffenen drohen.

3. Bewertung des Urteils

Das BVerfG ist traditionell sehr zurückhaltend bei einstweiligen Anordnungen, insbesondere wenn es um die Aussetzung des Vollzugs von Gesetzen geht, und weist auch in diesem Beschluss mehrfach auf die strengen Voraussetzungen hin, die dafür vorliegen müssen. Dass der Senat die einstweilige Anordnung dennoch recht deutlich ausspricht, deutet an, wie besorgt die Karlsruher Richter bezüglich der Auswirkungen der Vorratsdatenspeicherung sind. Diese Besorgnis unterstreicht das Gericht an zahlreichen Stellen mit (für die Anordnung selbst eigentlich überflüssigen) Hinweisen auf die „erheblichen Grundrechtsbeeinträchtigungen", die durch die Speicherung und insbesondere die anschließende Übermittlung zu befürchten sind.
Darüber hinaus finden sich immer wieder Seitenhiebe auf die extensive Konkretisierung der Richtlinienvorgaben durch den Gesetzgeber:

„Dabei ist im Verfahren über den Erlass einer einstweiligen Anordnung nicht zu prüfen, ob der deutsche Gesetzgeber durch die Richtlinie 2006/24/EG verpflichtet war, sämtliche der in § 100a Abs. 2 StPO aufgeführten Straftaten in die Abrufermächtigung des § 100g StPO einzubeziehen."

Und weiter:

„Es ist nicht ersichtlich, dass der Gesetzgeber aufgrund der Richtlinie verpflichtet war, noch weitere, in dem Katalog nicht genannte Straftaten als Anlasstaten für einen Verkehrsdatenabruf ausreichen zu lassen."

Dies lässt auch für die Hauptverhandlung eine entsprechend deutliche Absage an die Vorratsdatenspeicherung erwarten. Auch die mehrfache Bezugnahme auf das ausstehende Urteil des EuGH verspricht, dass das BVerfG die Vorratsdatenspeicherung im Falle der Nichtigerklärung der Richtlinie erheblich einschränken, wenn nicht gar ganz aufheben wird. Selbst wenn der EuGH sich jedoch anders entscheiden sollte, ist kaum anzunehmen, dass das BVerfG im Hauptverfahren von der Regelung in

der einstweiligen Anordnung Abstand nehmen und eine Übermittlung der Daten auch für die Ermittlung über Straftaten außerhalb von § 100a Abs. 1, 2 StPO möglich machen wird.

4. Folgen des Beschlusses für die Übermittlung von zu eigenen Zwecken gespeicherten Verkehrsdaten (§§ 96 Abs. 1, 97, 100 Abs. 1 TKG)

Die vorläufige Absage des BVerfG an die Verwendung der auf Vorrat gespeicherten Verkehrsdaten für andere als schwere Straftaten i.S.d. § 100a Abs. 1, 2 StPO hat für Uneinigkeit bezüglich der Rechtslage außerhalb der §§ 113a, 113b TKG geführt[63] und ist hinsichtlich der Übermittlung von Verkehrsdaten an Strafverfolgungsbehörden in der Tat äußerst widersprüchlich.

Zunächst ist festzustellen, dass die von § 113a TKG erfassten Verkehrsdaten nahezu vollumfänglich automatisch bei der Verbindung anfallen und somit vom Anbieter ohnehin gem. §§ 96, 97 oder § 100 TKG zur eigenen Verwendung gespeichert werden dürfen. Dies betrifft zunächst die Daten, die der Anbieter zur Entgeltermittlung und Abrechnung benötigt, aber für einen kurzen Zeitraum auch diejenigen Verkehrsdaten, die er nicht dafür benötigt[64]. Einerseits untersagt das Gericht nun die Übermittlung aller auf Grundlage von § 113a TKG gespeicherter Daten, sofern es sich nicht um Ermittlungen im Zusammenhang mit einer Straftat i.S.d. § 100a Abs. 1, 2 StPO handelt. Gleichzeitig genehmigt es aber den schon bisher praktizierten Abruf, indem es die Strafverfolgungsbehörden auf die *„ihnen schon bisher eröffneten Möglichkeiten des Zugriffs auf die von den Telekommunikations-Diensteanbietern im eigenen Interesse, etwa gemäß*

[63] So geht der *BfDI Schaar* entgegen der Ansicht des *BMJ* davon aus, dass nach der Vorabentscheidung kein Raum mehr für die Übermittlung von Verkehrsdaten außerhalb schwerer Straftaten besteht, vgl. Stellungnahmen, oben [Fn. 10].
[64] § 100 TKG, vgl. oben Punkt II. 1.

§ 97 in Verbindung mit § 96 Abs. 1 TKG zur Entgeltabrechnung, gespeicherten Telekommunikations-Verkehrsdaten"[65] verweist. Dieser Zugriff erfolgt jedoch auf Grundlage des § 100g StPO, womit er auch in Fällen der Ermittlung erheblicher Straftaten oder solcher Straftaten, welche mit Telekommunikation begangen wurden, möglich ist. Verkehrsdaten, die zu eigenen Zwecken der TK-Diensteanbieter gespeichert werden dürfen, werden von den Richtern demnach anders bewertet als Verkehrsdaten, die über § 113a TKG gespeichert werden müssen.

Bei den Daten i.S.d. §§ 96, 97, 100 TKG handelt es sich jedoch um dieselben Daten, die auch nach § 113a TKG gespeichert werden müssen[66]. Es ist kein Grund ersichtlich, weshalb diesen Datensätzen weniger verfassungsrechtlicher Schutz zukommen sollte, als denjenigen, welche gem. § 113a TKG erhoben werden. Der Zweckbindungsgrundsatz kann jedenfalls nicht als Rechtfertigung hierfür herangezogen werden. Wenn danach überhaupt Verkehrsdaten zur Übermittlung in Betracht kommen sollten, dann doch wohl diejenigen, welche auch zu Strafverfolgungszwecken, also auf Grundlage von § 113a TKG, gespeichert wurden und nicht diejenigen Verkehrsdaten, welche zu eigenen Zwecken (§§ 97, 100 TKG) gespeichert wurden[67].

Darüber hinaus ist zu bezweifeln, dass die TK-Diensteanbieter beim Speicherungsvorgang unterschiedlich vorgehen werden, denn die Daten fallen gleichermaßen bei der Verbindung an und müssten dann für die Speicherung künstlich in Vorratsdaten und Rechnungsdaten gesplittet werden. Naheliegender ist vielmehr die Annahme, dass die Speicherprozedur derart ablaufen wird, dass alle Daten geschlossen auf

[65] *BVerfG*, BvR 1 256/08, Rn. 173.
[66] zumindest innerhalb der ersten Tage nach Verbindungsende dürften die Daten identisch sein, da in diesem Zeitraum auch nicht für die Abrechnung benötigte Daten gespeichert bleiben dürfen, vgl. oben Punkt II. 1.

bestimmten Massenspeichern abgelegt werden und entweder nach kurzer Zeit in „Vorratsdatenspeicherungs-Verzeichnisse“ verschoben oder direkt von Anfang an nur dort gespeichert und anschließend lediglich als Vorratsdaten gekennzeichnet werden. Der Unterschied zwischen den gem. §§ 97 oder 100 TKG und den gem. § 113a TKG gespeicherten Verkehrsdaten würde sich dann lediglich auf die neue Deklarierung nach einigen Tagen beschränken – faktisch wären es jedoch dieselben Datensätze.

Weshalb der Senat dennoch nach § 113a TKG gespeicherte Daten – zumindest während der Dauer der einstweiligen Anordnung – privilegiert, ist nicht nachvollziehbar. Der Grundrechtseingriff durch die Übermittlung von zu eigenen Zwecken gespeicherten Verkehrsdaten wiegt keinesfalls geringer als bei der Übermittlung der fast identischen Vorratsdaten. Dementsprechend muss konsequenterweise für Verkehrsdaten, welche zu eigenen Zwecken der TK-Diensteanbieter gespeichert werden, der gleiche oder gar ein noch stärkerer Schutz wie für Vorratsdaten bestehen, denn es handelt sich nicht nur um dieselben Datensätze, sondern es mangelt hierbei auch an einem Speicherungszweck zur Strafverfolgung.

V. Fazit und Ausblick

Sieht man von dieser Inkonsequenz ab, ist die Entscheidung des BVerfG jedoch zu begrüßen, da sie das Hauptproblem der Vorratsdatenspeicherung, nämlich das erhebliche Überschreiten der Richtlinienvorgaben, vorerst weiträumig eliminiert bis eine Entscheidung des EuGH und Statistiken über die Nutzung der Vorrastdatenspeicherung vorliegen. Gleichzeitig ist zu loben, dass die Karlsruher Richter der Versuchung widerstehen, die Vorratsdatenspeicherung vorschnell zu verhindern und damit ihre Kompetenz in europarechtlicher Hinsicht zu überschreiten. Bei einer solch diplomatischen Übergangslösung verwundert es dann auch nicht, dass sich sowohl

[67] Z.B. die Dynamische IP-Adresse bei Flatrates, vgl. oben Punkt II. 3.

Vorratsdatenspeicherungsgegner als auch Befürworter als klare Sieger der Sache sehen. Dennoch muss stark bezweifelt werden, dass sich die Bundesregierung auch nach der Hauptsacheentscheidung noch zu diesen Gewinnern zählen kann, denn der vorliegende Beschluss legt die Vermutung nahe, dass die deutsche Gesetzgebung zur Vorratsdatenspeicherung in ihrer derzeitigen Form – wie auch immer die Entscheidung des EuGH ausfallen sollte – nicht bestehen bleiben wird.