



*Institut für Rechtsinformatik*

Universität

Leibniz  
Universität Hannover 

## **Vorratsdatenspeicherung – quo vadis?**

Eine datenschutzrechtliche Bewertung des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 unter Betrachtung der Verfahren vor dem Bundesverfassungsgericht

Seminararbeit von Jan Philipp Albrecht

Im LL.M.-Studiengang Rechtsinformatik

Bei Prof. Dr. Nikolaus Forgó

# Inhalt

Inhalt .....	II
Literaturverzeichnis.....	III
I. Einleitung.....	1
II. Grundzüge der Richtlinie.....	2
1. Speicherungspflicht und Zweck.....	3
2. Umfang der Datenspeicherung .....	3
III. Deutsches Umsetzungsgesetz .....	4
IV. Datenschutzrechtliche Beurteilung.....	6
1. Personenbezogene Daten .....	6
2. Datenschutzgrundsätze .....	6
a. Datensparsamkeit .....	6
b. Datensicherheit.....	7
c. Zweckbindung .....	7
V. Verfassungsrechtliche Beurteilung .....	8
1. Eingriffe in Verfassungsgüter.....	8
a. Grundgesetz .....	8
b. EMRK und Grundrechtecharta.....	9
2. Verfassungsmäßige Rechtfertigung.....	9
VI. Eilbeschlüsse des BVerfG .....	13
1. Einstweilige Anordnung.....	13
2. Verlängerungsbeschluss und Erweiterung .....	14
VII. Ausblick zur Entscheidung.....	15
VIII. Schluss.....	16



Jarass, Hans /  
Pieroth, Bodo  
(zitiert: Grundgesetz)

Grundgesetz: Kommentar, 9. Auflage, Verlag C.H. Beck,  
München 2007

Leutheusser-  
Schnarrenberger, Sabine

Vorratsdatenspeicherung – Ein vorprogrammierter Ver-  
fassungskonflikt, ZRP 2007, S. 9 ff.

Meyer, Franz C.

Individualrechtsschutz im Europäischen Verfassungs-  
recht, DVBl 2004, S. 606 ff.

Puschke, Jens /  
Singelstein, Tobias

Telekommunikationsüberwachung, Vorratsdatenspei-  
cherung und (sonstige) heimliche Ermittlungsmaßnah-  
men der StPO nach der Neuregelung zum 1.1.2008,  
NJW 2008, S. 113 ff.

Roßnagel, Alexander

Die EG-Richtlinie zur Vorratsdatenspeicherung von  
Kommunikationsdaten, EuZ 2006, S. 30 ff.

Simitis, Spiros  
(zitiert: BDSG)

Bundesdatenschutzgesetz: Kommentar, 6. Auflage, No-  
mos Verlag, Baden-Baden 2006

## I. Einleitung

Die Richtlinie 2004/24/EG vom 15. März 2006<sup>1</sup> ist eine grundlegende Richtungsentscheidung im europäischen Kommunikations- und Datenschutzrecht. Mit ihr entscheidet sich der Europäische Gesetzgeber für die so genannte Vorratsdatenspeicherung von Kommunikationsdaten zum Zwecke der Bekämpfung von Terroranschlägen und schwerster Kriminalität. Insbesondere nach den Bombenanschlägen von Madrid und London in den Jahren 2004 und 2005 verlangten die Sicherheitsbehörden und –politiker nach der Möglichkeit, Zugriff auf die Stamm- und Verkehrsdaten der Kommunikationsteilnehmer zu haben.

Die daraus entstandene Regelung rief erhebliche Kritik hervor.<sup>2</sup> So zog der Berichterstatter im Europäischen Parlament, ALEXANDER ALVARO, seine Unterschrift von der Beschlussvorlage zurück, nachdem der ihm in Absprache mit den Ausschüssen vorgelegte Entwurf, der im Vergleich zum Kommissionsvorschlag deutliche Abschwächungen vorsah, durch Änderungsanträge seitens der großen Parteien in eine noch weitgehendere Form gebracht wurde. Insbesondere Dauer und Umfang der Speicherung sowie die Zweckbestimmung für die Nutzung gespeicherter Daten wurden durch die Parlamentsmehrheit deutlich ausgeweitet.

Die europaweite Empörung zahlreicher Datenschutz- und Verfassungsrechtsexperten konnte die Beschlussfassung in dieser Form nicht verhindern. Der Drang nach einem neuen und (vermeintlich) schlagkräftigen Instrument zur Terrorbekämpfung war so groß, dass das Vorhaben binnen kürzester Zeit verabschiedet

---

<sup>1</sup> Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG; abgedruckt im ABl. EU Nr. L 105 S. 54–60, Jahr 2006. Im Folgenden schlicht „Richtlinie“.

<sup>2</sup> Vgl. GOLLA/KLUG, NJW 2008, S. 2481.

und umgesetzt wurde. Diese Arbeit soll die Richtlinie und ihre Umsetzung beleuchten und unter Berücksichtigung des aktuellen Verfahrens vor dem Bundesverfassungsgericht die datenschutz- und verfassungsrechtlichen Problemstellungen darstellen.

## II. Grundzüge der Richtlinie

Auf einen ursprünglich im Rahmen der so genannten dritten Säule der Union vorgeschlagenen Rahmenbeschluss zur Vorratsdatenspeicherung konnten sich die Mitgliedstaaten 2005 nicht einigen. So nahm sich die Europäische Kommission des Vorhabens an und legte einen Richtlinienentwurf vor, der auf Art. 95 EG gestützt ist und keine Einstimmigkeit im Rat erfordert.<sup>3</sup> Dieser Kompetenztitel verleiht der Gemeinschaft die Befugnis, Maßnahmen zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten zu erlassen, welche die Errichtung und das Funktionieren des Binnenmarktes zum Gegenstand haben.

Am 6. Juli 2006 reichte die Republik Irland beim EuGH eine Nichtigkeitsklage gegen die Richtlinie zur Vorratsdatenspeicherung ein, weil sie diese Kompetenzwahl für unzulässig hielt. Die Erfolgsaussichten dieser Klage gegen das formelle Zustandekommen der Richtlinie wird als aussichtsreich betrachtet, da es sich bei der Vorratsdatenspeicherung offenbar um eine Regelung zum Schutz der öffentlichen Sicherheit handelt, ähnlich wie bei der Fluggastdatenübermittlung an US-Behörden.<sup>4</sup> Im letzteren Fall hatte der EuGH selbst eine Annexkompetenz der Gemeinschaft in diesem Bereich verneint.<sup>5</sup> Das entsprechende Verfahren ist allerdings zur Zeit der Bearbeitung dieses Textes noch nicht abgeschlossen und

---

<sup>3</sup> Zum teils absurden Gang des Gesetzgebungsverfahrens vgl. ausführlich LEUTHEUSER-SCHNARRENBARGER, ZRO 2007, S. 9f.; zum Vorlauf Gietl, DuD 2008, 317 f.; zur rechtspolitischen Bewertung siehe Albrecht, FoR 1/2007, S. 13f.

<sup>4</sup> So LEUTHEUSER-SCHNARRENBARGER, ZRO 2007, S. 9 (12); Vgl. BREYER, StV 2004, S. 215; a.A. EuGH-Generalanwalt, Schlussanträge zu C-301/06 vom 14. Oktober 2008: <http://curia.europa.eu/de/actu/communiqués/cp08/aff/cp080070de.pdf>

<sup>5</sup> EuGH, NJW 2006, 2029; dazu GRAULICH NVwZ 2008, S. 485 (486) m.w.N.

soll direkt im Anschluss am 10. Februar 2009 entschieden werden.<sup>6</sup> Die formale Rechtmäßigkeit der Richtlinie kann für den Fokus dieser Arbeit allerdings ohnehin dahinstehen.

## 1. Speicherungspflicht und Zweck

Die Richtlinie bestimmt in Art. 1 Abs. 1, dass bestimmte Telekommunikationsdaten zu speichern sind, um sicher zu stellen, dass die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von „schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden“, zur Verfügung stehen. Art. 3 der Richtlinie verpflichtet die Mitgliedstaaten, dafür Sorge zu tragen, dass die in Art. 5 im Einzelnen aufgeführten Daten auf Vorrat gespeichert werden. Nach Art. 4 steht es den Mitgliedstaaten frei, das Verfahren und die näheren Bedingungen für die Einsichtnahme in die gespeicherten Daten unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes festzulegen.<sup>7</sup>

## 2. Umfang der Datenspeicherung

Gespeichert werden sollen Verkehrsdaten nach der Quelle der Nachricht, insbesondere nach Name und Anschrift des Teilnehmers, die zur Identifizierung des Adressaten erforderliche Informationen (Rufnummer, Benutzerkennung), Datum, Uhrzeit und Dauer der Nachrichtenübermittlung, Art der Nachrichtenübermittlung (Telefon, Internet etc.) sowie die Kennung der Endeinrichtung der Benutzer (Rufnummer, IMSI/IMEI, DSL-Teilnehmeranschluss).<sup>8</sup> Selbst Standortdaten von Mobilfunkgeräten werden erfasst. All dies hat auch bei erfolglosem Verbindungsversuch zu erfolgen.<sup>9</sup> Nach Art. 6 muss die Speicherdauer mindestens sechs Monate und darf höchstens zwei Jahre ab dem Zeitpunkt der Kommunikation betragen. Der Erhebung und Speicherung der Kommunikationsin-

---

<sup>6</sup> Siehe Verhandlungskalender des Europäischen Gerichtshofes am 10. Februar 2009 unter <http://curia.europa.eu/de/actu/activites/index.htm>

<sup>7</sup> Vgl. GITTER/SCHNABEL, MMR 2007, S. 411 (412); ROBNAGEL, EuZ 2006, S. 30 (31).

<sup>8</sup> BIZER, DuD 2007, S. 586.

<sup>9</sup> GITTER/SCHNABEL, MMR 2007, S. 411.

halte ist hiervon nach Art. 5 Abs. 2 ausdrücklich nicht umfasst. Es geht im Ergebnis um das Speichern des Ob, Wie und Wo bei allen elektronischen Kommunikationsvorgängen.

### III. Deutsches Umsetzungsgesetz

Die Umsetzung der Vorratsdatenspeicherung wurde im November 2007 vom Bundestag im Rahmen der Neuregelung heimlicher Ermittlungsmaßnahmen beschlossen. Auch hierbei stieß man erneut auf breite Proteste und großen Widerstand. Auch der wissenschaftliche Dienst des Bundestages hatte an der Möglichkeit einer grundrechtskonformen Umsetzung der Richtlinie erhebliche Zweifel.<sup>10</sup> Der Deutsche Bundestag selbst hatte in den drei vorhergehenden Legislaturperioden bei fünf verschiedenen Vorstößen für die Einführung einer Vorratsdatenspeicherung ein solches Vorhaben für unnötig und auch verfassungswidrig erklärt und abgelehnt.<sup>11</sup> Dennoch ist am 1.1.2008 das „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ in Kraft getreten.<sup>12</sup> Am Tag zuvor ging eine Verfassungsbeschwerde samt Antrag auf eine Aussetzung des Gesetzes durch einstweilige Anordnung beim Bundesverfassungsgericht ein, die von über 34.000 Beschwerdeführern unterzeichnet ist.<sup>13</sup>

Wegen der weitgehenden Verwendungs- und Missbrauchsmöglichkeiten von Kommunikationsdaten erlaubte es das Telekommunikationsgesetz den Anbietern von TK-Dienstleistungen bisher nur, zu Abrechnungszwecken Verkehrsdaten zu speichern, wenn der Kunde keine Anonymisierung verlangte (§ 97 III TKG).<sup>14</sup> Diese konnten dann rückwirkend nach § 100g StPO abgefragt

---

<sup>10</sup> <http://www.heise.de/newsticker/Neue-Zweifel-an-der-Rechtmaessigkeit-der-TK-Vorratsdatenspeicherung--/meldung/76921> (abgerufen am 5.2.2009)

<sup>11</sup> GIETL, DuD 2008, 317f.

<sup>12</sup> BGBl I 2007, 3197.

<sup>13</sup> [www.vorratsdatenspeicherung.de](http://www.vorratsdatenspeicherung.de); Vgl. dazu auch GIETL, DuD 2008, 317 (319).

<sup>14</sup> BREYER, StV 2007, S. 214.

werden. Nunmehr sind die Anbieter verpflichtet, die Daten zu staatlichen Sicherheitszwecken unanonymisiert auf Vorrat zu speichern.<sup>15</sup> Kernstück der Vorratsdatenspeicherung ist der neue § 113a TKG, in dem die Pflicht zur Speicherung von Verkehrsdaten für die Betreiber öffentlich zugänglich gemachter Telekommunikationsdienste geregelt ist.<sup>16</sup> Der Umfang wurde in den § 113a II-IV TKG weitestgehend an den in der Richtlinie vorgeschriebenen Speicherumfang angepasst, geht in Teilen aber darüber hinaus.<sup>17</sup>

Mit § 113b TKG lässt der deutsche Gesetzgeber die Nutzung der gespeicherten Daten sowohl zur Strafverfolgung, als auch zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit und zur Erfüllung der Aufgaben der Geheimdienste zu. Der neu gefasste § 100g StPO stellt dafür eine umfassende Ermächtigungsgrundlage der staatlichen Behörden zum Zugriff auf die Vorratsdaten beim Verdacht „erheblicher Straftaten“ oder „mittels Telekommunikation“ begangener Straftaten dar.<sup>18</sup> Mit dieser Regelung geht das Umsetzungsgesetz deutlich über die Vorgaben der Richtlinie in Art. 1 Abs. 1 hinaus und öffnet die Verwendung der Vorratsdaten im Grunde gar für die Verfolgung von Bagatelldelikten.<sup>19</sup> Zusätzlich müssen selbst bei Prepaid-Lösungen die Inhaberidentifizierung erhoben werden, auch Anonymisierungsdienste werden zu einer Vorratsdatenspeicherung verpflichtet.<sup>20</sup> In § 97 III TKG wird dafür die unverzügliche Löschungspflicht auch für Prepaid- und Flatrate-Dienste aufgehoben und einer Speicherpflicht unterworfen.<sup>21</sup> Lediglich die Speicherdauer orientiert sich an der von der Richtlinie vorgeschriebenen Mindestdauer von sechs Monaten.

---

<sup>15</sup> PUSCHKE/SINGELNSTEIN, NJW 2008, S. 113 (117).

<sup>16</sup> Vgl. PUSCHKE, NJW 2008, S. 2 m.w.N.

<sup>17</sup> GIETL, DuD 2008, S. 317 (319).

<sup>18</sup> HOEREN, JZ 2008, S. 669 (671).

<sup>19</sup> Vgl. BIZER, DuD 2007, S. 586 (587).

<sup>20</sup> Siehe BREYER, StV 2007, S. 214 (215) mit Verweis auf die anhängige Verfassungsbeschwerde gegen die Identifizierungspflicht (1 BvR 1299/05).

<sup>21</sup> GRAULICH, NVwZ 2008, S. 485 (487).

## **IV. Datenschutzrechtliche Beurteilung**

Gerade die Bedenken in Bezug auf den Datenschutz und die Datensicherheit haben viele Experten dazu gebracht, die Vorratsdatenspeicherung abzulehnen. Im Folgenden wird die Datenschutzproblematik zunächst isoliert erläutert. Dies ist allerdings regelmäßig nur schwer zu trennen von der verfassungsrechtlichen Bewertung, die im darauffolgenden Kapitel stattfinden wird.

### **1. Personenbezogene Daten**

Datenschutz ist vornehmlich der Schutz personenbezogener Angaben. Personenbezogene Daten sind etwa im Sinne von Art. 2 lit. a der Datenschutzrichtlinie 95/46/EG alle Informationen über eine bestimmte oder bestimmbare natürliche Person. Die durch die Vorratsdatenspeicherung erhobenen Kommunikationsdaten fallen eindeutig in den Bereich solcher Informationen.

### **2. Datenschutzgrundsätze**

Wichtig für die datenschutzrechtliche Bewertung sind vor allem die den Bestimmungen zu Grunde liegenden Grundsätze des Datenschutzes. In Art. 7 der Richtlinie werden die für die Vorratsdatenspeicherung geltenden Datenschutzrichtlinien mit Bezug auf die Richtlinien 95/46/EG und 2002/58/EG formuliert.<sup>22</sup> Diese bestimmen insbesondere, dass die Datensicherheit gewährleistet sein muss und die Daten nach der vorgeschriebenen Speicherdauer zu löschen sind. Diese sehr allgemeinen Bestimmungen finden sich in § 113a X und XI TKG wieder.

#### **a. Datensparsamkeit**

In § 3a BDSG wird der Grundsatz der Datenvermeidung und Datensparsamkeit normiert, der sich an der Datenschutzrichtlinie 95/46/EG orientiert.<sup>23</sup> Er stellt den Ausgangspunkt datenschutzrechtlicher Grundsätze dar. Ihm wird die Vorratsdatenspeicherung

---

<sup>22</sup> Vgl. hierzu GITTER/SCHNABEL, MMR 2007, S. 411 (412).

<sup>23</sup> Vgl. BIZER in SIMITIS, BDSG, § 3a Rn. 32f.

in keiner Weise gerecht. Selbst Möglichkeiten, wie etwa die Filterung bestimmter Nummern und Kennungen zum besonderen Schutz hochsensibler Kommunikationsdaten (von Ärzten, Journalisten etc.) sind nicht vorgesehen.<sup>24</sup> Die umfassende Erhebung von Daten aller Menschen entspricht wohl am wenigsten dem Prinzip der Datensparsamkeit.

### **b. Datensicherheit**

Die massenhafte Speicherung von Verkehrsdaten und Standortdaten erhöht die Risiken eines Datenmissbrauchs erheblich. Gerade die Speicherung dieser sensiblen Daten über längere Zeiträume durch private Dienstleistungsanbieter birgt die große Gefahr, dass diese Daten entgegen den gesetzlichen Bestimmungen etwa für die Auswertung von Kundenprofilen oder etwa gezieltes Scoring missbraucht werden.<sup>25</sup> Die Erfahrungen der vergangenen Monate und Jahre – etwa aus Italien, Großbritannien oder Deutschland – zeigen, dass selbst hohe interne Sicherheitsmaßnahmen den Missbrauch und die Weitergabe von Daten nicht verhindern konnten. Besondere gesetzliche Maßnahmen zur Datensicherheit bestehen für die Vorratsdatenspeicherung nicht.

### **c. Zweckbindung**

In den meisten Regelungen zum Schutz des Einzelnen vor einer missbräuchlichen oder exzessiven Verwendung ist zudem anerkannt, dass jede Erhebung oder Verarbeitung personenbezogener Daten voraussetzt, dass die verantwortliche Stelle mit ihr bestimmte, legitime und nicht missbräuchliche Zwecke verfolgt, die jeweils im Vorfeld festzulegen sind.<sup>26</sup> Dies ist in Anbetracht des sehr unpräzise gehaltenen § 113b Nr. 1 TKG schwerlich zu erkennen. Auch die Auskunftsbefugnis aus § 100g StPO entbehrt einer eindeutig bestimmten Zweckbindung.

---

<sup>24</sup> Vgl. GOLA/KLUG/REIF, NJW 2007, S. 2599 (2601).

<sup>25</sup> BIZER, DuD 2007, S. 586 (588).

<sup>26</sup> BREYER, Vorratsdatenspeicherung, S. 68f.

## V. Verfassungsrechtliche Beurteilung

Die datenschutzrechtliche Bewertung eines Vorhabens wie der Vorratsdatenspeicherung kann nur im verfassungsrechtlichen Kontext gesehen werden. Die umfassende Speicherung nahezu aller Telekommunikationsdaten könnte wie schon angedeutet ein Eingriff in zahlreiche Grundrechte und rechtstaatliche Grundsätze darstellen, der einer entsprechenden Rechtfertigung bedarf.

### 1. Eingriffe in Verfassungsgüter

Neben der möglichen Verletzung von Grundrechten und rechtsstaatlichen Grundsätzen aus dem Grundgesetz könnten die Speicherung gemäß § 113a TKG und die Nutzung gemäß § 113b TKG auch in Bestimmungen der EMRK eingreifen.

#### a. Grundgesetz

Bereits durch die Datenerfassung der Verkehrsdaten eines individuellen Kommunikationsvorgangs liegt ein Eingriff in das Fernmeldegeheimnis aus Art. 10 I Alt. 3 GG vor<sup>27</sup>, der sich mit der Speicherung fortsetzt und durch den später gegebenenfalls erfolgenden Datenzugriff noch intensiviert wird.<sup>28</sup> Die Vorratsdatenspeicherung berührt fundamentale Grundsätze des Datenschutzes und führt zu empfindlichen Beeinträchtigungen des selbstbestimmten Umgangs mit persönlichen Daten.<sup>29</sup> Auch die Pressefreiheit aus Art. 5 I S. 2 Alt. 1 GG wird durch die Vorratsdatenspeicherung beeinträchtigt. Die Rückverfolgbarkeit jeder Kontaktaufnahme kann zur Einschüchterung von Informationsquellen und damit zu einer nur noch stark eingeschränkten Kontrolle durch unabhängige Presseorgane führen.<sup>30</sup> Zudem wird auch in die durch Art. 12 I und 14 I GG geschützte Berufs- und Gewerbefrei-

---

<sup>27</sup> BVerfG, NJW 2000, S. 55 (59); JARASS/PIEROOTH, Grundgesetz, Art. 10 Rn. 9; HOEREN, JZ 2008, S. 668 (669).

<sup>28</sup> Vgl. GOLA/KLUG/REIF, NJW 2007, S. 2599.

<sup>29</sup> GITTER/SCHNABEL, MMR 2007, S. 411 (413); BREYER, Vorratsdatenspeicherung, S. 53ff.; ROßNAGEL, EuZ 2006, S. 30 (34f.).

<sup>30</sup> GOLA/KLUG/REIF, NJW 2007, S. 2599 (2600f.).

heit der TK-Diensteanbieter eingegriffen, da die zu erwartenden Kosten der Vorratsdatenspeicherung in mindestens dreistelliger Millionenhöhe allein den Betreibern aufgebürdet wird.<sup>31</sup>

## **b. EMRK und Grundrechtecharta**

Das Fernmeldegeheimnis wird auch europarechtlich durch Art. 8 EMRK ausdrücklich geschützt. Wenn auch noch nicht verbindlich, so schützt die EU-Grundrechtecharta zudem in Art. 7 das Recht der Bürger auf Achtung ihres Privatlebens und enthält in Art. 8 ein Grundrecht auf Datenschutz. Auch in diese Rechte wird durch die TK-Datenspeicherung eingegriffen.<sup>32</sup>

Durch Art. 6 II EMRK wird zudem die Unschuldsvermutung im Strafverfahren ausdrücklich geschützt. Die Vorratsdatenspeicherung könnte als Maßnahme der so genannten Strafverfolgungsvorsorge zur Beweisbeschaffung für ein eventuell einzuleitendes Ermittlungsverfahren – sprich als Teil des gerichtlichen Verfahrens zur Strafverfolgung – gegen die Unschuldsvermutung verstoßen.<sup>33</sup> So verlangten bisherige Eingriffe im Bereich der Strafverfolgungsvorsorge einen konkreten Verdacht. Eine anlasslose und verdachtsunabhängige Vorratsdatenspeicherung der Kommunikationsdaten aller Teilnehmer stellt damit den bislang massivsten Ausdruck eines grundlegenden Wandels dar, bei dem ein Generalverdacht Eingriffe zu rechtfertigen droht.<sup>34</sup>

## **2. Verfassungsmäßige Rechtfertigung**

Diese Eingriffe können nur dann verfassungsgemäß sein, wenn sie wesentlichen Voraussetzungen wie dem Bestimmtheitsgrundsatz und dem Verhältnismäßigkeitsprinzip entsprechen. Aus datenschutzrechtlicher Sicht ist hier vor allem der Eingriff in das Recht auf informationelle Selbstbestimmung in seiner Ausprägung

---

<sup>31</sup> BREYER, StV 2007, S. 214 (216).

<sup>32</sup> Vgl. ROßNAGEL, EuZ 2006, S. 30 (33).

<sup>33</sup> PUSCHKE/SINGELNSTEIN, NJW 2008, S. 113 (118).

<sup>34</sup> So auch BIZER, DuD 2007, S. 586 (589).

des Fernmeldegeheimnisses beachtlich. In dieses darf nur insoweit eingegriffen werden, wie es zum Schutz öffentlicher Interessen unerlässlich ist.<sup>35</sup> Nach dem Volkszählungsurteil setzt ein Zwang zur Abgabe personenbezogener Daten voraus, dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt.<sup>36</sup> Das Bundesverfassungsgericht hat mehrfach (zuletzt bei der Rasterfahndung) festgestellt, dass eine Speicherung „nicht anonymisierter Daten auf Vorrat zu unbestimmten Zwecken oder nicht bestimmbar Zwecken“ unzulässig ist.<sup>37</sup> Die Vorratsdatenspeicherung stellt aber gerade nicht auf eine konkrete Bedrohung ab, sondern beinhaltet die verdachtslose Speicherung der Verkehrsdaten aller Kommunikationsteilnehmer. Die sehr pauschale Formulierung des § 113b Nr. 1 TKG in Verbindung mit § 100g StPO entspricht den Erfordernissen der Zweckbestimmtheit nicht.<sup>38</sup> Diese fehlende Zweckbindung und das frühe Ansetzen der Vorratsdatenspeicherung erhöhen die Anforderungen an die Verhältnismäßigkeit enorm.<sup>39</sup> Denn je früher und unabhängiger von konkreten Anhaltspunkten ein Eingriff erfolgt, umso bestimmter muss die Regelung und umso gewichtiger müssen die Gründe hierfür sein.<sup>40</sup>

Deshalb wird die Frage nach der Verhältnismäßigkeit weitgehend verneint.<sup>41</sup> Schon die Eignung der Vorratsdatenspeicherung zur Terrorismusbekämpfung ist umstritten. Bei dem vom Industrieverband BITKOM erwarteten Datenvolumen von bis zu 40.000 Terabyte pro Jahr wird allein die Dauer des Suchlaufs eine Hürde für wirksame Terrorismusbekämpfung sein.<sup>42</sup> Potenzielle Täter haben außerdem zahlreiche Möglichkeiten, um einer Entde-

---

<sup>35</sup> JARASS/PIEROTH, Grundgesetz, Art. 10 Rn. 18.

<sup>36</sup> BVerfG, NJW 1984, S. 419.

<sup>37</sup> St. Rspr. seit BVerfG, NJW 1984, S. 419.

<sup>38</sup> Vgl. dazu ausführlich BREYER, StV 2007, S. 214 (217).

<sup>39</sup> GITTER/SCHNABEL, MMR 2007, S. 411 (414).

<sup>40</sup> PUSCKE/SINGELNSTEIN, NJW 2008, S. 113 (118).

<sup>41</sup> Umfassende Darstellung in BREYER, Vorratsdatenspeicherung.

<sup>42</sup> BIZER, DuD 2007, S. 586 (588); GITTER/SCHNABEL, MMR 2007, S. 411 (414).

ckung mittels der Vorratsdatenspeicherung zu entgehen – insbesondere wenn die Tat gut geplant ist, was sicher vor allem auf die organisierte Kriminalität und den Terrorismus zutrifft.<sup>43</sup> Zumal in Hinblick auf § 113b Nr. 2 TKG anzumerken ist, dass die Vorratsdatenspeicherung im Bereich der Gefahrenabwehr ohnehin keine große Wirkung haben kann, da sie sich nur auf Vorgänge bezieht, die in der Vergangenheit stattgefunden haben.<sup>44</sup>

Auch die Erforderlichkeit einer solchen lückenlosen Erfassung aller Telekommunikationsdaten ist äußerst fraglich. Mit dem so genannten „Quick Freeze“-Verfahren existiert ein erheblich milderer Mittel, das es zulässt, bei Vorliegen eines konkreten Tatverdachts die Datenlöschung auf behördliche Anordnung zu blockieren und die Daten im Anschluss auf richterliche Anordnung hin auszuwerten.<sup>45</sup> In Hinblick auf die bestehenden Befugnisse könnte die Vorratsdatenspeicherung gar kontraproduktiv wirken, weil sie den Einsatz immer komplexerer Anonymisierungstechniken durch Kriminelle fördert und dadurch den Ermittlungsbehörden in vielen Fällen eine Gefahrenabwehr unmöglich macht.<sup>46</sup>

In mehreren Entscheidungen hat das Bundesverfassungsgericht Grundrechtseingriffe „ins blaue hinein“ – wie hier bei der verdachtsunabhängigen Datenerhebung und -speicherung auf Vorrat – für unzulässig erklärt und die Anforderungen für Eingriffe mit großer Streubreite hochgesetzt.<sup>47</sup> Zudem hat es sich als eindeutig herausgestellt, dass eine unbefangene Mitwirkung und somit auch Kommunikation der Bürger für die Wahrnehmung ihrer

---

<sup>43</sup> GOLA/KLUG/REIF, NJW 2007, S. 2599.

<sup>44</sup> LEUTHEUSER-SCHNARRENBERGER, ZRP 2007, S. 9 (11).

<sup>45</sup> Vgl. GOLA/KLUG/REIF, NJW 2007, S. 2599 (2600); Siehe auch GITTER/SCHNABEL, MMR 2007, S. 411 (414), die darauf verweisen, dass selbst das BKA in einem eigenen Gutachten keine klare Antwort auf die Frage hat, ob weitergehende Maßnahmen als das Quick-Freeze“-Verfahren erforderlich seien.

<sup>46</sup> So etwa BREYER, StV 2007, S. 214 (219) mit dem Verweis auf entsprechende Äußerungen der Vorsitzenden vom Europäischen Verband der Polizei und dem Bund Deutscher Kriminalbeamter zu dieser Entwicklung.

<sup>47</sup> BVerfG, NJW 2005, S. 2603 (2609); BVerfG, NJW 2006, S. 1939 (1946).

demokratischer Rechte konstitutiv ist und allein das Gefühl des ständigen Überwachtseins bereits geeignet ist, dies nachhaltig zu beeinträchtigen.<sup>48</sup> Dies gilt insbesondere angesichts des rasanten Wachstums elektronischer Kommunikationsmittel und ihrer Bedeutung im Alltagsleben. Mithilfe der durch die Vorratsdatenspeicherung erhobenen hoch sensiblen Daten werden erhebliche Rückschlüsse auf Kommunikations- und Bewegungsverhalten sowie auf Art und Intensität von Beziehungen ermöglicht.<sup>49</sup>

Angesichts der wenigen Daten, die tatsächlich im Rahmen der Strafverfolgung „benötigt“ werden (weniger als 0,001% der jährlich 6,4 Mio. begangenen Straftaten, noch weniger wären es bei nur schweren Straftaten), fehlt es damit an einer Zweck-Mittel-Relation.<sup>50</sup> Diese Unverhältnismäßigkeit wird zudem durch die über die Bestimmungen der Richtlinie hinausgehenden Zugriffsmöglichkeiten aus § 113b Nr. 2 und 3 TKG noch gesteigert.<sup>51</sup> Die Einbeziehung präventiver polizeilicher und geheimdienstlicher Aufgaben ist mit den europarechtlichen Vorgaben und dem Grundgesetz nicht vereinbar.<sup>52</sup> Insbesondere die Betroffenheit von Journalisten, Ärzten, Rechtsanwälten, Beratungsstellen und Abgeordneten ohne Möglichkeiten des besonderen Schutzes birgt hohes Missbrauchspotential.<sup>53</sup> Als "Verdachtsschöpfungsinstrument" erhöht eine Vorratsspeicherung das Risiko, zu Unrecht einer Straftat verdächtigt zu werden.<sup>54</sup> Alles in allem fällt eine verfassungsrechtliche Rechtfertigung der Vorratsdatenspeicherung – selbst noch bei einer abgeschwächten Form sehr schwer.<sup>55</sup>

---

<sup>48</sup> BVerfG, NJW 2003, S. 1787 (1793); BVerfG, NJW 1984, S. 419 (422).

<sup>49</sup> PUSCHKE/SINGELNSTEIN, NJW 2008, S. 113 (118).

<sup>50</sup> Vgl. hierzu ausführlich GITTER/SCHNABEL, MMR 2007, S. 411 (414) m.w.N.

<sup>51</sup> GOLA/KLUG/REIF, NJW 2007, S. 2599 (2600); mit noch weitergehender Einschätzung auch BREYER, StV 2007, S. 204 (220).

<sup>52</sup> ROBNAGEL, EuZ 2006, S. 30 (33); GITTER/SCHNABEL, MMR 2007, S. 411 (415).

<sup>53</sup> BIZER, DuD 2007, S. 586 (589).

<sup>54</sup> BREYER, StV 2007, S. 204 (219).

<sup>55</sup> So auch GITTER/SCHNABEL, MMR 2007, S. 411 (413) m.w.N.

## VI. Eilbeschlüsse des BVerfG

Das Bundesverfassungsgericht hat im Verlauf des Jahres 2008 durch zwei Eilbeschlüsse über den Antrag auf einstweilige Anordnung entschieden und diesem teilweise stattgegeben.

### 1. Einstweilige Anordnung

Mit dem Beschluss vom 11.3.2008 hat das Bundesverfassungsgericht Teile der Vorratsdatenspeicherung vorläufig außer Kraft gesetzt.<sup>56</sup> Dies betrifft allerdings nicht die grundsätzliche Speicherpflicht nach § 113a TKG, sondern die Verwendung der nach dieser Vorschrift gespeicherten Daten.<sup>57</sup> Die Zweckbindung des § 113b TKG ging dem Bundesverfassungsgericht nicht weit genug. Bis zur Entscheidung der Hauptsache dürfen die aufgrund § 113a TKG gespeicherten Daten nur zur Verfolgung von schweren Straftaten übermittelt werden, solange sie nicht auch auf Grund der §§ 96 ff. TKG gespeichert werden könnten.<sup>58</sup> Damit wird die Eingriffsintensität des § 100g StPO allerdings nur leicht geschmälert, schließlich gibt er den Strafverfolgungsbehörden durch die erhobenen Vorratsdaten ein Zugriffsrecht von nun sechs Monaten rückwirkend und lässt die Abfrage in Echtzeit zu.<sup>59</sup> Nunmehr dürfen Diensteanbieter einem Auskunftersuchen der Ermittlungsbehörden nach § 100g StPO nur nachkommen, wenn Gegenstand des Ermittlungsverfahrens eine Katalogtat nach § 100a II StPO ist und darüber hinaus die Voraussetzungen des § 100a I StPO vorliegen.<sup>60</sup>

Der Beschluss hat somit im Rahmen der Folgenabschätzung des § 32 BVerfGG – insbesondere bei den über die Richtlinie hinausgehenden Bestimmungen – eine starke Beschränkung des Umsetzungsgesetzes für die Zeit bis zur Entscheidung der Haupt-

---

<sup>56</sup> BVerfG, MMR 2008, S. 303.

<sup>57</sup> Vgl. HOEREN, JZ 2008, S. 668 (672).

<sup>58</sup> BVerfG, MMR 2008, S. 303.

<sup>59</sup> Vgl. hierzu PUSCHKE/SINGELNSTEIN, NJW 2008, S. 113 (114).

<sup>60</sup> BVerfG, MMR 2008, S. 303.

sache zur Folge. Zu besonderer Klarheit bei der Abgrenzung zwischen den verschiedenen Zweckbestimmungen der von den Diensteanbietern erhobenen Kommunikationsdaten hat dies allerdings nicht geführt.<sup>61</sup> Es ist deutlich erkennbar, dass das Bundesverfassungsgericht das Problem des Verhältnisses zwischen seiner eigenen Prüfungskompetenz und dem Gemeinschaftsrecht klar umschiffte, was sicher den strengen Anforderungen an eine einstweilige Anordnung bei Gesetzen geschuldet ist.<sup>62</sup>

## 2. Verlängerungsbeschluss und Erweiterung

Da die einstweilige Anordnung auf sechs Monate befristet war (wie es § 32 VI BVerfGG vorschreibt), erließ das Bundesverfassungsgericht am 1.9.2008 einen Verlängerungsbeschluss für weitere sechs Monate. Mit einem weiteren Beschluss vom 28.10.2008 gab das Bundesverfassungsgericht einem Ergänzungsantrag der Beschwerdeführer auf einstweilige Anordnung statt.<sup>63</sup> Es erweiterte die einstweilige Anordnung dahingehend, dass die nach § 113a TKG auf Vorrat gespeicherten Daten für die Gefahrenabwehr (§ 113b Satz 1 Nr. 2 TKG) von den TK-Diensteanbietern nur dann an die ersuchende Behörde übermittelt werden dürfen, wenn der Abruf der Daten zur Abwehr einer dringenden Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr erforderlich ist.<sup>64</sup> Für Aufgaben des Verfassungsschutzes (§ 113b Satz 1 Nr. 3 TKG) dürfen die Daten zudem nur dann übermittelt werden dürfen, wenn auch die Voraussetzungen von § 1 Abs. 1, § 3 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Art. 10-Gesetz) vorliegen.<sup>65</sup>

---

<sup>61</sup> Siehe hierzu ausführlich GRAULICH, NVwZ 2008, S. 485 (491f.).

<sup>62</sup> Vgl. GIETL, DuD 2008, 317 (320f.).

<sup>63</sup> BVerfG, MMR 2009, S. 29.

<sup>64</sup> BVerfG, MMR 2009, S. 29.

<sup>65</sup> BVerfG, MMR 2009, S. 29.

## VII. Ausblick zur Entscheidung

Mit den Beschlüssen vom März und Oktober hat das Bundesverfassungsgericht den im Falle einer einstweiligen Anordnung gegen Gesetze gegebenen (relativ engen) Rahmen weitestgehend ausgeschöpft. Ein Termin für die endgültige Entscheidung im Hauptsacheverfahren über das Gesetz zur Umsetzung der Richtlinie 2006/24/EG steht derzeit noch nicht fest. Es ist aber zu erwarten, dass sich das Bundesverfassungsgericht nach der Entscheidung des EuGH über die Nichtigkeitsklage Irlands gegen die Richtlinie mit einer materiellen Prüfung des Gesetzes umfassend auseinandersetzen wird. Je nach Ergebnis der Nichtigkeitsklage vor dem EuGH ist die Situation mehr oder weniger problematisch.<sup>66</sup>

Sollte die Richtlinie für nichtig erklärt werden, so stünde es dem Bundesverfassungsgericht nach eigener Rechtsprechung (Solange) frei, über alle Teile der Regelung zu urteilen. Blicke die Richtlinie hingegen gültig, so entstünde die problematische Situation, dass eine grundrechtliche Beurteilung gemeinschaftsrechtlicher Regelungen zwar wegen der Solange-Rechtsprechung<sup>67</sup> beschränkt wäre, das Bundesverfassungsgericht in diesem Fall aber dennoch zu der Einschätzung kommen könnte, dass die Regelung zumindest in Teilen verfassungswidrig ist.<sup>68</sup> Ob hier das Ende der Solange-Rechtsprechung, eine erneute Vorlage (zur materiellen Prüfung) an den EuGH, ein Teilurteil des Bundesverfassungsgerichtes oder schlicht ein politisches Einlenken ins Haus stünde, muss zum Zeitpunkt dieser Arbeit als offene Frage stehen bleiben.

Nach dem Voranstehenden wird das Bundesverfassungsgericht mit hoher Wahrscheinlichkeit zumindest die über die Richtlinie hinauschießenden Regelungen der §§ 113a und 113b TKG für unzulässig erklären und mit Blick auf die besondere Intensität von

---

<sup>66</sup> Vgl. LEUTHEUSER-SCHNARRENBERGER, ZRP 2007, S. 9 (13).

<sup>67</sup> Siehe BVerfG NJW 2000, 3124 ff.

<sup>68</sup> Hierzu ausführlich bei GIETL, DuD 2008, 317 (321ff.).

technikbasierten verdachtslosen Grundrechtseingriffen mit großer Streubreite eine besondere verfahrensrechtliche Grundrechtssicherung einfordern.<sup>69</sup> Angesichts der Tatsache allerdings, dass der Schwerpunkt des Eingriffs in die unbefangene Telekommunikation aller Bürger bereits bei der Erhebung und Speicherung der Daten über Abrechnungszwecke hinaus liegt, ist jedoch sogar davon auszugehen, dass das Gericht keine „Ja, aber...“ Entscheidung – wie bei der einstweiligen Anordnung geschehen – treffen kann.<sup>70</sup> Denn eine solche Entscheidung würde das Vertrauen der Bürger in moderne Telekommunikationsmittel wohl kaum wiederherstellen.

## VIII. Schluss

Es bleibt festzuhalten, dass die überwiegende Mehrheit zu dem klaren Ergebnis einer verfassungsrechtlich und datenschutzrechtlich höchst bedenklichen Vorschrift kommt und die bisherige – datenschutzfreundliche – Rechtsprechung des Bundesverfassungsgerichts klar gegen die Gültigkeit einer solchen Norm spricht. Insgesamt drängt sich der Eindruck auf, dass hier mit heißer Nadel im bisher schnellsten EU-Gesetzgebungsverfahren eine Regelung geschaffen wurde, dessen Ausmaße und Folgen vielen auf Grund der technisch hochkomplexen Materie nicht bewusst gewesen ist.

Ohne zu zögern wird die Bedeutung der Grundrechte hier auf den Kopf gestellt, indem nicht der staatliche Eingriff in die Grundrechte, sondern vielmehr die die Begrenzung staatlicher Ermittlungstätigkeit einer Rechtfertigung bedürfe.<sup>71</sup> Hier zeigt sich musterhaft die Bedeutung unabhängiger – nicht bloß gerichtlicher – Kontrollen bei grundrechtsrelevanten Maßnahmen. In Zeiten der rasant voranschreitenden Informationsgesellschaft gilt dies vor allem beim Schutz personenbezogener Daten.

---

<sup>69</sup> GOLA/KLUG/REIF, NJW 2007, S. 2599 (2602); GRAULICH, NVwZ 2008, S. 485 (486).

<sup>70</sup> Siehe auch GIETL, DuD 2008, 317 (322).

<sup>71</sup> So aber klingt es deutlich in der Begründung des deutschen Umsetzungsgesetzes durch den Bundestag in BT-Drucks. 16/5846, S. 22.

Rechtspolitisch ist es daher ein Problem, dass es auf Ebene der Europäischen Union kein umfassendes Individualbeschwerderecht vor dem EuGH und damit kein Äquivalent zum Bundesverfassungsgericht gibt.<sup>72</sup> Der Fall der Vorratsdatenspeicherung zeigt damit nicht nur beim Schutz datenschutzrechtlicher Standards, sondern vor allem bei der Wahrung des Gleichgewichts zwischen staatlichen Sicherheitsinteressen und persönlichen Freiheitsrechte massive Regelungslücken im bestehenden Verfassungsverbund der Europäischen Union auf. Zumal sich angesichts der Umstände und Debatte um die Vorratsdatenspeicherung der Verdacht aufdrängt, dass die Regelung weniger für die Ermittlungsbehörden zur Terrorbekämpfung, sondern vielmehr für namhafte Medienkonzerne zur Durchsetzung ihrer geistigen Eigentumsrechte als notwendig erscheint.<sup>73</sup> Ganz gleich welche Beweggründe tatsächlich im Raum stehen, so ist der Verlust eines ausgeglichenen Verhältnisses zwischen individueller Freiheit und staatlicher Intervention für einen Rechtsstaat nicht tragbar.

Und so möchte ich mit den Worten schließen, die BURKHARD HIRSCH jüngst in einer Erwiderung an Bundesinnenminister WOLFGANG SCHÄUBLE richtete: „Die Bürger haben Anspruch auf ein Parlament und eine Regierung, die dieselbe Nervenstärke, dasselbe Rechtsbewusstsein, den gleichen selbstbewussten Stolz auf unsere Rechtsordnung und den ebenso festen Willen zu ihrer Verteidigung haben, wie die Richter in Karlsruhe.“<sup>74</sup>

Und wenn ich mir eine persönliche Anmerkung zu diesem Zitat erlauben darf: Es wird Zeit, dass sie ihn durchsetzen.

---

<sup>72</sup> Zur Frage des lückenhaften individuellen Rechtsschutzes vor dem EuGH siehe MEYER, DVBI 2004, S. 606f.

<sup>73</sup> So ergab eine Studie des Freiburger Max Planck Institut für ausländisches und internationales Strafrecht, dass sich die allermeisten Fälle eines Datenabrufs durch Strafverfolgungsbehörden auf Betrugs- und Urheberrechtsdelikte beziehen: [http://www.vorratsdatenspeicherung.de/images/mp\\_i-gutachten.pdf](http://www.vorratsdatenspeicherung.de/images/mp_i-gutachten.pdf)

<sup>74</sup> HIRSCH, ZRP 2008, S. 24, der selbst Verfassungsbeschwerde gegen das Gesetz zur Vorratsdatenspeicherung eingelegt hat.