

# Meinhard Starostik

Rechtsanwalt

RA Starostik, Schillstraße 9, 10785 Berlin

An das  
Bundesverfassungsgericht  
Schloßbezirk 3  
76131 Karlsruhe

**Rechtsanwaltskanzlei:**

Schillstr. 9 ♦ 10785 Berlin  
Tel.: 030 - 88 000 345  
Fax: 030 - 88 000 346  
email: Kanzlei@Starostik.de  
USt-ID-Nr. DE165877648

**Kanzlei vereidigter Buchprüfer:**

Schwarzenberger Str. 7 ♦ 08280 Aue  
Tel.: 03771-290 999

Berlin, den 22. September 2009

**AZ: 82/06**

(bitte stets angeben)

In den Verfahren

**Verfassungsbeschwerden und Anträge auf Erlass einer einstweiligen Anordnung gegen die §§ 113a, 113b des Telekommunikationsgesetzes in der Fassung des Gesetzes zur Neuregelung der Telekommunikationsüberwachung der anderen verdeckten Ermittlungsverfahren sowie zur Umsetzung der Richtlinie 2006/24/EG**  
**1 BvR 256/08 und 1 BvR 508/08**

nehme ich zu den Stellungnahmen auf den Fragenkatalog des Bundesverfassungsgerichts wie folgt Stellung:

**A. Vorlage an den Europäischen Gerichtshof**

Ich **beantrage** weiterhin, noch vor mündlicher Verhandlung des Verfahrens

dem Europäischen Gerichtshof die Frage **vorzulegen**, ob die Richtlinie 2006/24/EG gültig ist.

**I. Vorlagepflicht**

Dass die beantragte Vorlage zulässig und geboten ist, ist bereits ausführlich dargelegt worden.<sup>1</sup> Dass die Vorlage begründet ist und **zur Ungültigerklärung** der Richtlinie 2006/24/EG führen wird, ist ebenfalls ausgeführt worden.<sup>2</sup>

Vor dem Hintergrund des **Lissabon-Urteils** des Bundesverfassungsgerichts<sup>3</sup> ist die Vorlage an den EuGH noch dringlicher geworden.<sup>4</sup> In Öffentlichkeit und Wissenschaft ist weithin kritisiert worden, dass sich das Bundesverfassungsgericht einerseits – richtigerweise – die Prüfung von Europarecht am Maßstab des Grundgesetzes

<sup>1</sup> Schriftsatz vom 13.08.2008, 21 ff.; Schriftsatz vom 23.02.2009, 2; Schriftsatz vom 26.03.2009.

<sup>2</sup> Beschwerdeschrift, 23 ff.; Schriftsatz vom 23.02.2009, 2 ff.

<sup>3</sup> BVerfG, 2 BvE 2/08 vom 30.6.2009.

<sup>4</sup> Caliess, FAZ 198/2009, 8.

vorbehält, andererseits jedoch – insoweit abzulehnen – keine Bereitschaft signalisiert, eine Vorlage an den EuGH zuvor wenigstens zu versuchen. In anderen Staaten, deren Verfassungsgericht sich die Letztentscheidungskompetenz gegenüber EU-Recht vorbehält, ist anerkannt, dass ein Übergehen von Europarecht erst in Betracht kommt, wenn der EuGH auf eine Vorlage hin keine Abhilfe schafft.<sup>5</sup> Das Bundesverfassungsgericht erkennt nun zwar nominell den Vorrang von „Rechtsschutz auf Unionsebene“ an,<sup>6</sup> hat selbst aber noch nie ein Vorabentscheidungsersuchen an den EuGH gerichtet. Sollte das Bundesverfassungsgericht in Fällen verfassungswidrigen sekundären Europarechts nicht wenigstens versuchen, eine Aufhebung des Rechtsakts durch Vorlage der Frage an den EuGH zu erreichen, so würde sein Ansehen in der nationalen und internationalen Öffentlichkeit untergraben und die Akzeptanz seiner Wächterrolle geschwächt.

Die Kritik an dem durch Vorlageverweigerung „**drohenden Justizkonflikt**“ reicht so weit, dass namhafte Europarechtler inzwischen unter Bezugnahme auf das vorliegende Verfahren eine Änderung des Bundesverfassungsgerichtsgesetzes fordern.<sup>7</sup> Eingefügt werden soll danach der folgende § 13a BVerfGG:

„Ist in einem Verfahren vor dem Bundesverfassungsgericht die Auslegung der vertraglichen Grundlagen der Europäischen Union oder die Gültigkeit und die Auslegung der Handlungen der Organe, Einrichtungen oder sonstigen Stellen der Europäischen Union entscheidungserheblich, **ist das Bundesverfassungsgericht zur Vorlage** dieser Frage an den Gerichtshof der Europäischen Union verpflichtet.“

Eine solche Änderung ist indes unnötig, weil sich diese **Vorlagepflicht bereits heute** aus Art. 234 EG ergibt. Eine Vorlage des Bundesverfassungsgerichts an den EuGH im vorliegenden Verfahren würde deutlich machen, dass das Hohe Gericht seine Vorlagepflicht anerkennt, Justizkonflikte europafreundlich zu vermeiden sucht und zu einer echten Kooperation mit dem EuGH bereit ist.

Das Hohe Gericht hat mit Urteil vom 30.06.2009 ausdrücklich ausgesprochen:<sup>8</sup>

**Wenn Rechtsschutz auf Unionsebene nicht zu erlangen ist**, prüft das Bundesverfassungsgericht, ob Rechtsakte der europäischen Organe und Einrichtungen sich [...] in den Grenzen der ihnen im Wege der begrenzten Einzelermächtigung eingeräumten Hoheitsrechte halten [...]. Darüber hinaus prüft das Bundesverfassungsgericht, ob der unantastbare Kerngehalt der Verfassungsidentität des Grundgesetzes nach Art. 23 Abs. 1 Satz 3 in Verbindung mit Art. 79 Abs. 3 GG gewahrt ist [...].

---

<sup>5</sup> Mayer, Kompetenzüberschreitung und Letztentscheidung (2000), 280: Dänemark (EuGRZ 1999, 49), Schweden, Österreich.

<sup>6</sup> BVerfG, 2 BvE 2/08 vom 30.6.2009, Absatz-Nr. 240.

<sup>7</sup> Bergmann u.a., Auswege aus dem drohenden Justizkonflikt, <http://whi-berlin.de/documents/whi-material0109.pdf>; vgl. auch Mayer, EUA-Drs. 16(21)916, 12; Streinz, EUA-Drs. 16(21)911, 2 und 10.

<sup>8</sup> BVerfG, 2 BvE 2/08 vom 30.6.2009, Absatz-Nr. 240.

Die beantragte Vorlage an den EuGH ist danach geboten, um feststellen, ob auf Unionsebene Rechtsschutz gegen die Richtlinie 2006/24/EG zu erlangen ist und um andernfalls nationalen Rechtsschutz nach Maßgabe der genannten Grundsätze des Bundesverfassungsgerichts gewähren zu können.

## II. Kompetenzüberschreitung

In der Beschwerdeschrift ist ausgeführt worden, dass die Richtlinie 2006/24/EG der Zulässigkeit der Verfassungsbeschwerde nicht entgegen steht.<sup>9</sup> Unter anderem ist dargelegt worden, dass sich die EG-Richtlinie 2006/24 nicht in den Grenzen der Hoheitsrechte, welche der EG eingeräumt worden sind, hält, weil der EG-Vertrag keine **Rechtsgrundlage für die Richtlinie** darstellt.<sup>10</sup> Daran ist trotz der abweichenden Entscheidung des EuGH,<sup>11</sup> die von der herrschenden Literatur zu Recht abgelehnt wird,<sup>12</sup> festzuhalten. Die Richtlinie dient hauptsächlich der Erleichterung der Strafverfolgung (vgl. Art. 1 Abs.1 RiL 2006/24/EG),<sup>13</sup> indem sie eine Verpflichtung zur Vorratsdatenspeicherung begründet und Mindestvorgaben macht. Ein solches Instrument dient nicht der „Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten, welche die Errichtung und das Funktionieren des Binnenmarktes zum Gegenstand haben“ (Art. 95 EG). Entsprechend der Entscheidung des EuGH zur Fluggastdatenübermittlung rechtfertigt Art. 95 EG nur die Regelung von Tätigkeiten, die „für die Erbringung einer Dienstleistung erforderlich“ sind, was bei einer Vorratsdatenspeicherung nicht der Fall ist. Die Argumente, mit denen der EuGH von der Entscheidung zur Fluggastdatenübermittlung abgewichen ist, überzeugen nicht.<sup>14</sup> Art. 95 EG setzt einen empirisch überprüfbaren Beitrag der Maßnahme zur Beseitigung von Hemmnissen für den freien Verkehr von Dienstleistungen sowie von Wettbewerbsverzerrungen voraus.<sup>15</sup> Zur Harmonisierung des Binnenmarktes ist die Richtlinie 2006/24/EG schon deshalb nicht geeignet, weil sie hinsichtlich Speicherfrist, zu speichernder Datentypen und Datennutzung nur Mindestvorgaben macht.<sup>16</sup> Wo vor Inkrafttreten der Richtlinie in wenigen Mitgliedsstaaten unterschiedliche Speicherpflichten bestanden und im Übrigen das einheitliche Lösungsgebot des Art. 6 RiL 2002/58/EG galt, hat die Richtlinie dazu geführt, dass nunmehr unterschiedliche Speicherpflichten in allen Mitgliedsstaaten bestehen.<sup>17</sup> Die Richtlinie hat das Gegenteil einer Harmonisierung bewirkt. Entsprechend früherer Entscheidungen des EuGH bildet Art. 95 EG keine Rechtsgrundlage für Maßnahmen, die einen negativen Binnenmarkteffekt haben, indem sie bestimmte Wirtschaftstätigkeiten behindern, wie es bei einer Pflicht zur Vorratsdatenspeicherung der Fall ist.<sup>18</sup> Entsprechend früherer Entscheidungen des EuGH rechtfertigt Art. 95 EG auch nicht die Schaffung neuer europäischer Rechtsinstitute, die Überlagerung

---

<sup>9</sup> Beschwerdeschrift, 20 ff.

<sup>10</sup> Beschwerdeschrift, 22.

<sup>11</sup> EuGH, NJW 2009, 1801.

<sup>12</sup> Petri, EuZW 2009, 214; Ambos, JZ 2009, 468; Braum, ZRP 2009, 174; Kleszczewski, HRRS 2009, 250; Terhechte, EuZW 2009, 199; Rossi, ZJS 2009, 298; Simitis, NJW 2009, 1782; vgl. auch Kleszczewski in: Weßlau/Wohlers, Festschrift Fezer (2008), 19.

<sup>13</sup> Rossi, ZJS 2009, 298 (299); Petri, EuZW 2009, 214 (214); Braum, ZRP 2009, 174 (175); Ambos, JZ 2009, 468 (470); Simitis, NJW 2009, 1782 (1783 f.); Kleszczewski in: Weßlau/Wohlers, Festschrift Fezer (2008), 19.

<sup>14</sup> Rossi, ZJS 2009, 298 (299); Braum, ZRP 2009, 174 (177); Kleszczewski, HRRS 2009, 250 (251); Petri, EuZW 2009, 214 (215); Simitis, NJW 2009, 1782 (1784); Kleszczewski in: Weßlau/Wohlers, Festschrift Fezer (2008), 19.

<sup>15</sup> Vgl. etwa EuGH, NJW 2000, 3701 (3703).

<sup>16</sup> Kleszczewski in: Weßlau/Wohlers, Festschrift Fezer (2008), 19.

<sup>17</sup> Terhechte, EuZW 2009, 199 (200).

<sup>18</sup> Kleszczewski, HRRS 2009, 251.

nationaler Rechtsinstitute oder die Einführung europäischer neben nationaler Rechtsinstitute,<sup>19</sup> wie es bei der Richtlinie zur Vorratsdatenspeicherung im Hinblick auf die allermeisten Mitgliedsstaaten der Fall ist. Die Vorratsdatenspeicherung stellt auch keinen Annex zur Datenschutzrichtlinie 2002/58/EG dar,<sup>20</sup> die schon vorher in Art. 15 eine Öffnungsklausel für Abweichungen zu staatlichen Zwecken enthielt und keiner Änderung bedurft hätte.

Bereits im Maastricht-Urteil hat das Bundesverfassungsgericht ausgesprochen:<sup>21</sup>

Dementsprechend prüft das Bundesverfassungsgericht, ob Rechtsakte der europäischen Einrichtungen und Organe sich in den **Grenzen der ihnen eingeräumten Hoheitsrechte** halten oder aus ihnen ausbrechen (vgl. BVerfGE 58, 1 [30 f.]; 75, 223 [235, 242]).

Das Hohe Gericht hat mit Urteil vom 30.06.2009 bekräftigt:<sup>22</sup>

Wenn Rechtsschutz auf Unionsebene nicht zu erlangen ist, **prüft das Bundesverfassungsgericht**, ob Rechtsakte der europäischen Organe und Einrichtungen sich unter Wahrung des gemeinschafts- und unionsrechtlichen Subsidiaritätsprinzips [...] in den Grenzen der ihnen im Wege der begrenzten Einzelermächtigung eingeräumten Hoheitsrechte halten (vgl. BVerfGE 58, 1 <30 f.>; 75, 223 <235, 242>; 89, 155 <188>: dort zum sogenannten ausbrechenden Rechtsakt).

Wie gezeigt, hält sich die EG-Richtlinie 2006/24 nicht in den Grenzen der Hoheitsrechte, welche die Bundesrepublik der EG vertraglich im Wege der begrenzten Einzelermächtigung eingeräumt hat. Dem lässt sich nicht entgegen halten, dass eine Pflicht zur Vorratsdatenspeicherung **im Wege eines EU-Rahmenbeschlusses** hätte eingeführt werden können und die Wahl des Rechtsrahmens aus Sicht des Grundgesetzes keinen Unterschied mache. Die Wahl zwischen Richtlinie und Rahmenbeschluss macht aus Sicht des Grundgesetzes einen fundamentalen Unterschied. Erstens war die Verabschiedung eines Rahmenbeschlusses zur Vorratsdatenspeicherung unter Geltung des Einstimmigkeitsprinzips politisch unmöglich, weil mehrere Mitgliedsstaaten einen entsprechenden Entwurf ablehnten und auch die Richtlinie 2006/24/EG nur gegen die Stimmen zweier Mitgliedsstaaten im Ministerrat verabschiedet werden konnte. Zweitens wäre der Deutsche Bundestag, der die Einführung einer flächendeckenden Vorratsdatenspeicherung zuvor mehrfach abgelehnt hatte, frei gewesen, die Umsetzung eines entsprechenden Rahmenbeschlusses im Einklang mit den Grundrechten abzulehnen.<sup>23</sup> Drittens wäre das Bundesverfassungsgericht zur uneingeschränkten Prüfung der Vereinbarkeit eines Rahmenbeschlusses am Maßstab der Grundrechte befugt gewesen.<sup>24</sup>

---

<sup>19</sup> Terhechte, EuZW 2009, 199 (203) m.w.N.

<sup>20</sup> Braum, ZRP 2009, 174 (176).

<sup>21</sup> BVerfGE 89, 155 (188).

<sup>22</sup> BVerfG, 2 BvE 2/08 vom 30.6.2009, Absatz-Nr. 240.

<sup>23</sup> BVerfGE 113, 273 (301).

<sup>24</sup> BVerfGE 89, 155 (177).

Schließlich wäre die EU zur Verpflichtung aller Telekommunikationsanbieter zur Vorratsdatenspeicherung **auch im Rahmen des EU-Vertrages nicht** kompetent gewesen. Wie der EuGH in diesem Zusammenhang zutreffend ausführt, betrifft die Vorratsdatenspeicherung weder die grenzüberschreitende Zusammenarbeit von Polizei- noch von Justizbehörden (Art. 29-31 EU). Vielmehr ist die Vorratsdatenspeicherung dem Strafverfahrensrecht zuzurechnen,<sup>25</sup> für dessen Harmonisierung es bislang an einer Kompetenz der EU fehlt. Erst der Vertrag von Lissabon sieht Kompetenzen in diesem Bereich vor (Art. 82 Abs. 2 UAbs. 1 und UAbs. 2 sowie Art. 84 AEUV), welche eine Vorratsdatenspeicherung zur Erleichterung der Strafverfolgung jedoch ebenfalls nicht abdecken. Deswegen kann auch nicht argumentiert werden, durch den Vertrag von Lissabon erledige sich die Kompetenzfrage. Zum hier maßgeblichen Zeitpunkt war der Vertrag von Lissabon nicht in Kraft. Ob er zukünftig in Kraft tritt, bleibt abzuwarten. Soweit der Rahmenbeschlussskizzenentwurf argumentierte, die Verfügbarkeit von Telekommunikationsdaten sei Voraussetzung für ihre grenzüberschreitende Übermittlung,<sup>26</sup> vermag dies eine Kompetenz der EU nicht zu begründen. Mit diesem Argument könnten weite Teile des strafrechtlichen Ermittlungsverfahrens ohne Bezug zur grenzüberschreitenden Zusammenarbeit harmonisiert werden, was den Zweck der Art. 29-31 EU offenkundig überschreitet. Das Straf- und Strafverfahrensrecht in seinem Kernbestand dient nicht als rechtstechnisches Instrument zur Effektuierung einer internationalen Zusammenarbeit, sondern steht für die besonders sensible demokratische Entscheidung über das rechtsethische Minimum.<sup>27</sup>

Für die Verwerfung der Richtlinie 2006/24/EG als kompetenzwidrig spricht ferner, dass die Richtlinie die **Grundrechte** der Betroffenen zutiefst verletzt. Je intensiver grundrechtlich geschützte Positionen betroffen sind, desto strengere Anforderungen sind auch an die Wahl und Bestimmung der exakten Kompetenzgrundlage zu stellen. Denn gerade in so grundrechtssensiblen Bereichen wie der Vorratsdatenspeicherung muss die Regelungsbefugnis mit dem Grundrechtsschutz und auch die Verantwortung für etwaige Grundrechtseingriffe und -verletzungen mit der demokratischen Legitimation der grundrechtsbeeinträchtigenden Regelung einhergehen.<sup>28</sup>

Außerdem stellt die Richtlinie einen **Präzedenzfall** dar, dessen Bestand weitere Kompetenzüberschreitungen nach sich zu ziehen droht. Auf Grundlage der Auslegung des Art. 95 EG durch den EuGH könnten Wirtschaftsunternehmen künftig – auch gegen die Stimme Deutschlands – jegliche Verpflichtungen zur Strafverfolgungs- und Gefahrenabwehrvorsorge auferlegt werden,<sup>29</sup> etwa Verpflichtungen zur Erhebung und Vorhaltung beliebiger personenbezogener Informationen, Verpflichtungen zur Identitätsfeststellung, zur Abnahme von Fingerabdrücken, zur Aufnahme von Fotos oder Videoaufzeichnungen oder zum Abgleich von Daten. Braum sieht eine drohende Vereinheitlichung von Aspekten des Strafvollzugs unter Berufung auf Art. 95 EG, „weil verschiedene Industrienormen des zu Vollzugszwecken verwendeten Stahls die europäische Stahlindustrie in ihrem grenzüberschreitenden

---

<sup>25</sup> Braum, ZRP 2009, 174 (176).

<sup>26</sup> Erwägungsgrund 9 und Art. 1 Abs. 1 des Entwurfs, BR-Drs. 406/04, 6 und 8.

<sup>27</sup> Vgl. BVerfG, 2 BvE 2/08 vom 30.6.2009, Absatz-Nr. 358.

<sup>28</sup> Rossi, ZJS 2009, 298 (299).

<sup>29</sup> Vgl. Ambos, JZ 2009, 468 (471); Petri, EuZW 2009, 214 (215).

Verkehr gefährden könnten.“<sup>30</sup> Eine so extensive Auslegung der Binnenmarktkompetenz untergräbt die fehlende Strafrechtskompetenz der Gemeinschaft (vgl. Art. 280 Abs. 4 Satz 2 EGV) und das Prinzip der begrenzten Einzelermächtigung,<sup>31</sup> welches gerade auch dem Schutz der Grundrechte in sensiblen Bereichen wie dem Strafrecht dient.

Die EG-Richtlinie 2006/24 ist folglich als kompetenzwidrig zu verwerfen und in Deutschland für unanwendbar zu erklären,<sup>32</sup> wenn der EuGH der Kompetenzüberschreitung nicht abhilft.<sup>33</sup> **Abhilfe durch den EuGH** ist noch nicht endgültig gescheitert. Obwohl der EuGH die formelle Rechtmäßigkeit der EG-Richtlinie 2006/24 angenommen hat,<sup>34</sup> kann er im Ergebnis noch abhelfen, indem er die Richtlinie wegen Verletzung der Gemeinschaftsgrundrechte für ungültig erklärt. Die Vereinbarkeit der Richtlinie mit den Gemeinschaftsgrundrechten hat der EuGH bisher ausdrücklich offen gelassen. Nach Art. 234 EG und kraft seiner Rechtsprechung<sup>35</sup> muss das Bundesverfassungsgericht dem EuGH folglich durch ein Vorabentscheidungsersuchen Gelegenheit geben, die Vereinbarkeit der EG-Richtlinie 2006/24 mit den Gemeinschaftsgrundrechten zu prüfen.

### III. Gebot des effektiven Rechtsschutzes

Dass auch die Garantie des effektiven Rechtsschutzes gegen die Vorratsdatenspeicherung ein Vorabentscheidungsersuchen gebietet, weil ein anderer Rechtsweg zum EuGH nicht in zumutbarer Weise offen steht, ist bereits ausgeführt worden.<sup>36</sup> Eine **Verweisung auf die Fachgerichte** widerspräche § 90 Abs. 2 S. 1 i.V.m. § 93 Abs. 3 BVerfGG und gewährleistete auch von Qualität und Gewicht der Vorlageentscheidung her keinen effektiven Rechtsschutz, wie die Vorlageentscheidung des VG Wiesbaden zeigt.<sup>37</sup> Im Übrigen ist darauf hinzuweisen, dass die ordentlichen Gerichte eine Vorlage an den EuGH gerade mit Blick auf das vorliegende Verfahren ablehnen.<sup>38</sup> Nachdem die Bürgerinnen und Bürger in Deutschland nun schon seit über einem Jahr die anlasslose Erfassung ihres Kommunikations- und Bewegungsverhaltens hinnehmen müssen, würde auch die mit einer Verweisung auf die Fachgerichtsbarkeit verbundene Verzögerung dem Gebot effektiven Rechtsschutzes nicht mehr gerecht.

### IV. Weiteres Verfahren nach der Entscheidung des EuGH

Auf die Vorlage des Bundesverfassungsgerichts wird der EuGH **aller Wahrscheinlichkeit nach** unter Bezug auf die Vorlageentscheidung des Hohen Gerichts und auf die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte die Richtlinie 2006/24/EG wegen Verletzung der Grundrechte der Millionen betroffener Bürgerinnen und Bürger aufheben. Der Verfassungsbeschwerde gegen die §§ 113a, 113b TKG kann das Hohe Gericht dann vollumfänglich

---

<sup>30</sup> Braum, ZRP 2009, 174 (175).

<sup>31</sup> Ambos, JZ 2009, 468 (471).

<sup>32</sup> Vgl. BVerfG, 2 BvE 2/08 vom 30.6.2009, Absatz-Nr. 241.

<sup>33</sup> Vgl. BVerfG, 2 BvE 2/08 vom 30.6.2009, Absatz-Nr. 240.

<sup>34</sup> EuGH, NJW 2009, 1801.

<sup>35</sup> Vgl. BVerfG, 2 BvE 2/08 vom 30.6.2009, Absatz-Nr. 240.

<sup>36</sup> Beschwerdeschrift, 19 und 30; Schriftsatz vom 13.08.2008, 21 ff.

<sup>37</sup> Näher Schriftsatz vom 26.03.2009, 2 f.

<sup>38</sup> OLG Frankfurt vom 22.04.2009, 13 U 105/07 – unveröff.

stattgeben – nicht nur wegen der mit § 113a TKG verbundenen Grundrechtsverletzung, sondern im Einklang mit dem Demokratieprinzip schon wegen der mangelnden Entscheidungsfreiheit des Deutschen Bundestags bei der Verabschiedung dieser Regelung.<sup>39</sup>

Dass der EuGH trotz der Vorlage des Bundesverfassungsgerichts und trotz der Entscheidung des EGMR im Sachen S. und Marper die Richtlinie 2006/24/EG **aufrecht erhält**, ist äußerst unwahrscheinlich. Sollte dies gleichwohl geschehen, wird die Richtlinie 2006/24/EG wegen der Kompetenzüberschreitung für in Deutschland unanwendbar zu erklären sein und werden die §§ 113a, 113b TKG wegen Verletzung der Grundrechte des Grundgesetzes zu verwerfen sein. Die Kompetenzkontrolle durch das Bundesverfassungsgericht setzt nach dessen ständiger Rechtsprechung nicht voraus, dass die Europäische Gemeinschaft die Grenzen der ihr übertragenen Hoheitsrechte „generell“ oder „systematisch“ überschreitet.<sup>40</sup> Vielmehr ist in jedem Einzelfall zu prüfen, ob eine „ersichtliche Grenzüberschreitung bei Inanspruchnahme von Zuständigkeiten“ der europäischen Organe vorliegt.<sup>41</sup> Dass die Überschreitung der Hoheitsrechte im Fall der Richtlinie 2006/24/EG nicht nur ersichtlich, sondern sogar offensichtlich ist, ist in der Beschwerdeschrift ausgeführt worden.<sup>42</sup> Im Übrigen ist die Richtlinie 2006/24/EG keineswegs ein Einzelfall. Die Europäischen Institutionen und insbesondere der EuGH weiten immer wieder ihre Kompetenzen über die Grenzen der Verträge hinaus aus.<sup>43</sup> In der Literatur als Beispiele genannt werden etwa auch die Komplexe Altersdiskriminierung (Mangold), Staatshaftung (Francovich), Tabakwerbeverbot, Strafrechtskompetenz und Diskriminierungsverbot (Gattoussi).<sup>44</sup>

## **B. Begründetheit der Verfassungsbeschwerde**

### **I. Empirische Erkenntnisse**

In den vorangegangenen Schriftsätzen ist mehrfach der Stand der Forschung hinsichtlich der Verwendbarkeit von Telekommunikationsdaten wiedergegeben worden.<sup>45</sup> Vor kurzem hat IBM eine **Software zur Auswertung von Verkehrsdaten** durch Telekommunikationsunternehmen vorgestellt. Zur Arbeitsweise der Software schreibt IBM:<sup>46</sup>

„In der Gruppenaufspürphase werden die **unterschiedlichen strukturellen Gruppen** anhand von Sprach- und Textverbindungen (SMS) ermittelt. Zu diesen Strukturen gehören Cliquen (in denen jedes Gruppenmitglied mit jedem anderen Gruppenmitglied kommuniziert), Stars (wo eine Person im Zentrum mit verschiedenen Randfiguren kommuniziert, welche untereinander fast nie kommunizieren) und verschiedene Arten dichter Unterdarstellungen innerhalb der Darstellung. Mitglieder struktureller Anrufgruppen, die andere Telekommunikationsnetze verwenden, werden identifiziert [...]“

---

<sup>39</sup> Näher Schriftsatz vom 13.08.2008, 30 f.

<sup>40</sup> So aber Calies, FAZ 198/2009, 8.

<sup>41</sup> BVerfG, 2 BvE 2/08 vom 30.6.2009, Absatz-Nr. 240.

<sup>42</sup> Beschwerdeschrift, 29.

<sup>43</sup> Bergmann u.a., Auswege aus dem drohenden Justizkonflikt, <http://whi-berlin.de/documents/whi-material0109.pdf>: „Anlässe gibt es genug“.

<sup>44</sup> Herzog/Gerken, FAZ 210/2008, 8.

<sup>45</sup> Beschwerdeschrift, 83; Schriftsatz vom 17.03.2008, 11; Schriftsatz vom 13.08.2008, 24 f.

<sup>46</sup> [http://domino.research.ibm.com/comm/research\\_projects.nsf/pages/snazzy.index.html](http://domino.research.ibm.com/comm/research_projects.nsf/pages/snazzy.index.html).

An dieser Darstellung wird deutlich, dass Verkehrsdaten das perfekte Instrument für eine gesellschaftliche und politische Kontrolle bilden.

In einem Hintergrundpapier<sup>47</sup> weisen die Forscher darauf hin, dass die Auswertung von Kommunikationsinformationen dabei helfen könne, die „**Struktur und Entwicklung sozialer Netzwerke**“ aufzudecken. Anhand solcher Informationen ließen sich im echten Leben zu beobachtende Phänomene wie die Effizienz von Organisationen, die Weiterverbreitung von Informationen oder die Verbreitung von Krankheiten erklären.

Für ihre Untersuchung stellte „einer der größten Mobiltelefonanbieter der Welt“ sämtliche Kommunikationsdaten des Monats März 2007 zur Verfügung. Die Datenmenge liege bei 60 GB, was in ausgedruckter Form 6 Mio. Aktenordnern entspräche. Den Daten entnahmen die Forscher über **9 Mio. wechselseitige Kommunikationsbeziehungen** zwischen Personen. Dabei nahmen die Forscher an, gegenseitige Kontakte längerer Dauer oder höherer Häufigkeit wiesen auf eine soziale Beziehung zwischen zwei Personen hin.

## I. Verletzung des Art. 10 GG

### 1. Eingriff in den Schutzbereich

Die Beschwerdeschrift führt aus, dass die **Übertragung der Vorratsdatenspeicherung auf Private** an dem staatlichen Eingriff in das Fernmeldegeheimnis nichts ändert.<sup>48</sup> Die Unternehmen speichern die Kommunikationsdaten nicht „als Private“, sondern als Beliehene in staatlichem Auftrag und aus staatlichem, nicht aus eigenem Recht. Insoweit ist der Distanzgedanke – die gespeicherten Datenvorräte seien ja nicht staatlich gespeichert und daher staatlichem Zugriff grundsätzlich nicht zugänglich – nur eingeschränkt richtig. Vielmehr wird durch die Speicherung ein Datenpool geschaffen bei privaten Unternehmen, welche – als solche – keine unmittelbaren Grundrechtsadressaten des Art. 10 Abs. 1 GG sind. Solche können sie allenfalls durch die Tatsache ihrer Beleihung werden. In beiden Fällen jedoch kann den Grundrechtsschutz bei den Unternehmen allein die öffentliche Hand sicherstellen: entweder durch die Aktualisierung von Schutzpflichten oder durch die Ausgestaltung und Durchsetzung der Grundrechtsbindung bei – nicht-staatlichen – Beliehenen. In beiden Fällen entsteht Grundrechtsdurchsetzung erst durch Regulierung von außen und muss eine globale und pauschale Erfassung sämtlicher Kommunikationsvorgänge untersagt werden. Die sonst „übliche“ Grundrechtsaktualisierung durch gerichtliche Klagen Betroffener scheidet bei der Vorratsdatenspeicherung weitgehend aus, da die Betroffenen von möglichen (Folge-)Eingriffen nicht zuverlässig erfahren: Sie können weder die Erhebung noch die Verwendung der erhobenen Daten selbst kontrollieren.

Ist ein Datenvorrat erst einmal angelegt, so steht er grundsätzlich zur Nutzung technisch offen. Rechtliche Verwendungsregeln sind nur eingeschränkt in der Lage, die Nutzung zweckentsprechend zu kanalisieren und zu regulieren. Diesem Effekt versucht die Grundrechtsdogmatik in der jüngeren Zeit mit dem **Grundsatz der**

---

<sup>47</sup> Dasgupta u.a., Social ties and their relevance to churn in mobile telecom networks, <http://portal.acm.org/citation.cfm?id=1353424>.

<sup>48</sup> Beschwerdeschrift, 41 f.



**Datensparsamkeit** zu begegnen, dem verfassungsrechtliche Relevanz zukommt. Ob der Datenvorrat unmittelbar beim Staat oder bei (beliebigen) Privaten angelegt wird, ändert daran grundsätzlich nichts.<sup>49</sup> Im Gegenteil ist bei Privaten die Grundrechtsdurchsetzung vielfach sogar schwieriger als beim Staat.

**Voßkuhle** und Kauser führen aus, das Verhalten Privater begründe einen Grundrechtseingriff, wenn es dem Staat zurechenbar sei. Ziele der Staat gerade auf das beeinträchtigende Verhalten des Privaten ab, sei die Zurechnung „ohne Weiteres“ zu bejahen („intentionaler Eingriff“).<sup>50</sup> § 113a TKG stellt einen solchen intentionalen Grundrechtseingriff dar, weil der Gesetzgeber das grundrechtsbeeinträchtigende Speicherverhalten der privaten Telekommunikationsanbieter gezielt anordnet, um etwaige Zugriffe zu einem späteren Zeitpunkt zu ermöglichen. In der Rechtsprechung ist anerkannt, dass ein absichtliches Verhalten auch dann vorliegt, wenn ein Ziel als Mittel zu einem anderen Zweck angestrebt wird (Zwischenziel).<sup>51</sup>

Eine aktuelle Entscheidung des **Hessischen Verwaltungsgerichtshofs** stützt die Auffassung, wonach § 113a TKG in Art. 10 GG eingreift. Zu Maßnahmen eines privaten Arbeitgebers führt das Gericht aus, dem Fernmeldegeheimnis dürften auch solche Maßnahmen unterliegen, die darauf ausgerichtet sind, Daten aus dem laufenden Kommunikations- oder Übertragungsvorgang zum Zwecke der nachträglichen Auswertung oder zur Ermittlung von Straftaten, zu erheben. Dazu gehöre hauptsächlich die Aufzeichnung von Verbindungsdaten.<sup>52</sup> § 113a TKG verpflichtet Private zu einer Maßnahme, die darauf ausgerichtet ist, Daten aus dem laufenden Kommunikations- oder Übertragungsvorgang zur Strafverfolgungsvorsorge zu erheben. Folglich greift die Vorschrift in das Fernmeldegeheimnis ein.

---

<sup>49</sup> BVerfGE 115, 320 (350): „die bei öffentlichen und privaten Stellen vorhandenen Daten ...“

<sup>50</sup> Voßkuhle/Kauser, JuS 2009, 313 (313).

<sup>51</sup> BGHSt 4, 109; BGHSt 18, 151; BGHSt 18, 246.

<sup>52</sup> VGH Kassel, NJW 2009, 2470 (2471).

## 2. Verfassungsmäßige Rechtfertigung

### a) Nutzen einer Vorratsspeicherung von Telekommunikationsdaten

Die **Bundesregierung** schreibt in ihrer Stellungnahme vom 02.06.2009, eine Vielzahl von Straftaten werde unter Nutzung von Telekommunikation begangen und könne ohne Rückgriff auf Verkehrsdaten nicht aufgeklärt werden. Abrechnungsdaten genügen zur Aufklärung nicht mehr, weil die Nutzung von Pauschaltarifen zugenommen habe. Die Bundesregierung führt verschiedene Fallgruppen und Beispiele mittels Telekommunikation begangener Straftaten an, welche ohne Rückgriff auf die nach § 113a TKG zu speichernden Daten nicht aufgeklärt werden könnten.

Dass die nach § 113a TKG zu speichernden Daten mitunter die Aufklärung einer Straftat erst ermöglichen, ist unstreitig.<sup>53</sup> Dass dieser Umstand gleichwohl **keine allgemeine Protokollierung** des Kommunikations- und Bewegungsverhaltens der gesamten Bevölkerung rechtfertigt, ist in den vorausgegangenen Schriftsätzen umfassend ausgeführt worden. Zur Vermeidung von Wiederholungen fasse ich die wesentlichen Gründe nur wie folgt zusammen:

1. Das Risiko der Unaufklärbarkeit mittels Telekommunikation begangener Straftaten ist auch ohne Vorratsdatenspeicherung **nicht höher als bei Straftaten**, die unter Verwendung anderer Kommunikationsmittel oder sonst begangen werden.<sup>54</sup> Denn auch bei anderen Kommunikations- und Handlungsformen hinterlassen wir regelmäßig keine identifizierbaren Spuren. In einer freiheitlichen Gesellschaft ist es normal, dass unser zurückliegendes Kommunikations-, Bewegungs- und Informationsverhalten nicht nachvollziehbar ist.<sup>55</sup> Es ist nicht gerechtfertigt, die Nutzung von Telekommunikationsnetzen nachvollziehbarer zu gestalten als vergleichbare Tätigkeiten außerhalb der Telekommunikationsnetze.<sup>56</sup>
2. Die durchschnittliche polizeiliche Aufklärungsrate liegt bei 55%.<sup>57</sup> Diese Aufklärungsrate wird erzielt, ohne dass systematisch das Kommunikations-, Bewegungs- und Informationsverhalten der gesamten Bevölkerung aufgezeichnet wird. Ausgehend von dieser Aufklärungsrate ist es **normal**, dass die Identifizierung und Überführung von Straftätern in vielen Fällen (zu 45%) scheitert.
3. Eine Aufklärungsrate von 55% lässt sich auch bei mittels Telekommunikation begangenen Straftaten erzielen, und zwar **auch ohne Vorratsdatenspeicherung**. Es stehen dazu betrieblich gespeicherte Daten, Speichieranordnungen im Einzelfall und eine Vielzahl anderer Mittel zur Verfügung.<sup>58</sup>
4. Die **Aufklärungsrate im Bereich mittels Internet begangener Straftaten** ist ohne Vorratsdatenspeicherung mit über 80% sogar sehr viel höher gewesen als im Bereich anderer Straftaten.<sup>59</sup>

---

<sup>53</sup> Schriftsatz vom 17.03.2008, 8.

<sup>54</sup> Beschwerdeschrift, 126 f.

<sup>55</sup> Beschwerdeschrift, 126 f.; Schriftsatz vom 17.03.2008, 4 ff.

<sup>56</sup> Beschwerdeschrift, 124 ff.

<sup>57</sup> Bundeskriminalamt, Polizeiliche Kriminalstatistik 2008, 65.

<sup>58</sup> Näher Schriftsatz vom 13.08.2008, 33 f.

<sup>59</sup> Näher Schriftsatz vom 09.06.2009, 7.

5. Die **zunehmend pauschale Abrechnung** von Internetzugängen, die sich in Deutschland schon vor Inkrafttreten der Vorratsdatenspeicherung ereignet hat (2005: 18% Flatrates, 2007: 69%), hatte keinerlei negative Auswirkung auf diese Aufklärungsrate.<sup>60</sup> Der Umfang der zu betrieblichen Zwecken gespeicherten Verkehrsdaten wie auch das Ausmaß ihrer staatlichen Nutzung hat vor Einführung des § 113a TKG nicht ab-, sondern rasant zugenommen.<sup>61</sup>
6. Es gibt keine Straftatbestände oder typische Fallgruppen solcher Straftaten, die ohne Vorratsdatenspeicherung **im Wesentlichen leer liefen**. Dies beweist die Praxis der Strafverfolgung sowohl in Deutschland vor Inkrafttreten der Vorratsdatenspeicherung wie auch in anderen Staaten, in denen bis heute das Verbot der Aufzeichnung unnötiger Kommunikationsinformationen gilt.<sup>62</sup> Niemand kann ernsthaft behaupten, dass in Staaten wie Österreich oder Kanada bestimmte Straftatbestände oder Fallgruppen solcher Straftaten im Wesentlichen leer liefen. Die Aufklärungsrate ist in Staaten ohne Vorratsdatenspeicherung nicht gefallen und in Staaten mit Vorratsdatenspeicherung nicht gestiegen. Von einer Vorratsdatenspeicherung gehen umgekehrt sogar kontraproduktive Wirkungen auf die Strafverfolgung aus.<sup>63</sup>
7. Weder im zeitlichen Vergleich innerhalb Deutschlands noch im Vergleich mit ausländischen Staaten ohne Vorratsdatenspeicherung lässt sich irgend ein statistisch relevanter **Einfluss des § 113a TKG auf die Aufklärungsrate** oder gar die Kriminalitätsrate zeigen, auch nicht im Bereich einzelner Straftatbestände.
8. Gemessen an der Gesamtheit der Ermittlungsverfahren kann die Vorratsdatenspeicherung in weniger als 0,01% der Fälle überhaupt von Nutzen sein.<sup>64</sup> Für 99,99% der registrierten Straftaten ist **§ 113a TKG von vornherein ohne jede Bedeutung**.

Die Vorratsdatenspeicherung ist danach in einem demokratischen Rechtsstaat **problemlos verzichtbar**. Eine wirksame Strafverfolgung ist auch ohne Vorratsdatenspeicherung möglich.

**Einzelne Fallbeispiele**, wie sie die Bundesregierung anführt, lassen von vornherein nicht auf einen verfassungsrechtlich relevanten Bedarf nach Vorratsdaten schließen. Zur Vermeidung von Wiederholungen der voran gegangenen Schriftsätze fasse ich die wesentlichen Gründe nur wie folgt zusammen:

1. Die Bundesregierung nennt Einzelfälle **ohne Angabe ihrer statistischen Relevanz**. Dies geht an der Frage des Bundesverfassungsgerichts vorbei. Das Hohe Gericht hatte gefragt, ob die Aufklärung mittels Telekommunikation zu verwirklichender Straftatbestände oder typischer Fallgruppen solcher Straftaten ohne § 113a TKG weitgehend leer laufe. Die Nennung von Einzelfällen ist von vornherein ungeeignet, ein Leerlaufen bestimmter Straftatbestände oder typischer Fallgruppen von Straftaten darzutun. Es ist bis heute nicht ersichtlich oder gar belegt, dass § 113a TKG die Aufklärungsrate irgend eines mittels Telekommunikation zu verwirklichenden Straftatbestandes oder einer einzigen

---

<sup>60</sup> Näher Schriftsatz vom 17.03.2008, 3 f. Auch im Jahr 2008 hat die Aufklärungsrate von Internetstraftaten bei 80% gelegen: Bundeskriminalamt, Polizeiliche Kriminalstatistik 2008, 243.

<sup>61</sup> Schriftsatz vom 17.03.2008, 6.

<sup>62</sup> Vgl. EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 115 f.

<sup>63</sup> Beschwerdeschrift, 100 f.; Schriftsatz vom 17.03.2008, 7.

<sup>64</sup> Schriftsatz vom 17.03.2008, 1 ff.; Schriftsatz vom 09.06.2009, 7.

Fallgruppe solcher Straftaten auch nur statistisch signifikant erhöht hätte. Noch weiter entfernt ist die Bundesregierung von der Darlegung, dass ohne § 113a TKG gar das Leerlaufen eines Straftatbestandes oder einer Fallgruppe von Straftaten drohe.

2. In mehreren der von der Bundesregierung genannten Fälle handelt es sich **nicht um mittels Telekommunikation** begangene Straftaten, nach denen das Hohe Gericht gefragt hatte. Im Bereich allgemeiner Kriminalität bilden Verkehrsdaten nur einen möglichen Ermittlungsansatz unter vielen und sind besonders häufig ersetzbar.
3. In den meisten der von der Bundesregierung genannten Fälle ist nicht dargetan, dass Vorratsdaten zur Identifizierung und Überführung des Täters **erforderlich** gewesen wären und nicht die Nutzung ohnehin gespeicherter Abrechnungsdaten, eine Fangschaltung oder eine Speicheranordnung im Einzelfall ausgereicht hätten.
4. In den meisten der übrigen von der Bundesregierung genannten Fälle ist nicht dargetan, dass die gewünschten Vorratsdaten die Identifizierung und Überführung des Täters **ermöglichen** würden oder ermöglicht hätten. Die Bundesregierung lässt außer Acht, dass Verkehrsdaten in vielen Fällen nicht zur Identifizierung oder Überführung des Täters führen, etwa wegen der Vielzahl von Verschleierungs- und Anonymisierungsmöglichkeiten.
5. Die Bundesregierung hat nicht dargetan, ob und in wie vielen der Fälle Vorratsdaten einen Einfluss auf den **Verfahrensausgang** gehabt hätten. Viele Strafverfahren werden auch bei vorhandenen Verkehrsdaten eingestellt, wie die Untersuchung des Max-Planck-Instituts zeigt.
6. Die verbleibenden der von der Bundesregierung angeführten Beispielfälle wären auch bei **Begehung der Straftat durch unmittelbare oder schriftliche Kommunikation** nicht nachvollziehbar gewesen.
7. Das Aufklärungsinteresse, welches sich aus den angeführten Einzelfällen ergibt, besteht **unverhältnismäßig selten** gemessen an der Reichweite und Eingriffstiefe der flächendeckenden und anlasslosen Vorratsdatenspeicherung.<sup>65</sup>

Die von der Bundesregierung angeführten Fälle mittels Telekommunikation begangener Straftaten lassen sich zweckmäßigerweise in **zwei Fallgruppen** unterscheiden: In der ersten Fallgruppe nutzt der Täter elektronische Kommunikationsmedien, um seine Identität zu verbergen oder darüber zu täuschen (z.B. Stalking, Beleidigung/Verleumdung, Bedrohung, Betrug, Vortäuschen einer Straftat, Phishing). In der zweiten Fallgruppe nutzt der Täter die Telekommunikation, um verbotene Informationen einverständlich mit einem anderen auszutauschen (z.B. Kinderpornografie, Volksverhetzung, Werben für terroristische Vereinigung, Verletzung des Dienstgeheimnisses). Dass sich Telekommunikationsnetze zu diesen Zwecken einsetzen lassen, ist unbestreitbar. Es ist aber schon ausführlich aufgezeigt worden, dass man auch im unmittelbaren Kontakt miteinander weitgehend anonym ist<sup>66</sup> und dass ein konspirativer Informationsaustausch auch im unmittelbaren Kontakt miteinander möglich ist (z.B. Gespräche, Übergabe von Aufzeichnungen oder Datenträgern). Erst recht gilt dies für die Möglichkeit postalischer Kommunikation.<sup>67</sup> Eine einmalige Kontaktaufnahme mit Unbekannten lässt sich in all diesen Fällen nur schwer nachvollziehen; es handelt sich um keine Besonderheit der elektronischen

---

<sup>65</sup> Umfassend Beschwerdeschrift, 50 ff.

<sup>66</sup> Beschwerdeschrift, 126 f.

<sup>67</sup> Beschwerdeschrift, 132 f.

Kommunikation. Im Fall wiederholter Kontaktaufnahme ist eine Rückverfolgung im Bereich elektronischer Kommunikation durch die Möglichkeit einer Fangschaltung sogar einfacher möglich als eine Rückverfolgung anonymer Briefe. Wegen der Einzelheiten nehme ich auf das Parallelverfahren Bezug, in welchem die Vor- und Nachteile anonymer Kommunikation bereits umfassend behandelt worden sind.<sup>68</sup>

Was das Argument der **Terrorismusbekämpfung** oder des Vorgehens gegen schwere Straftaten angeht, so ist nicht ersichtlich, dass wirksame Gefahrenabwehr oder die Aufklärung von Straftaten gerade durch die Vorratsdatenspeicherung hätte ermöglicht werden können. Wesentliche Aufklärungserfolge – etwa nach dem Attentat von Madrid – wurden gerade ohne die Vorratsdatenspeicherung erzielt.

Die schon vor Einführung der Vorratsdatenspeicherung **weit überdurchschnittliche Aufklärungsrate im Bereich von Netzkriminalität** belegt, dass sich elektronische Kommunikation insgesamt gesehen leichter nachvollziehen lässt als mündliche oder schriftliche Kommunikation.<sup>69</sup> Einer anlasslosen Aufzeichnung sämtlicher Kontakte bedarf es folglich im Bereich elektronischer Kommunikation ebenso wenig wie im Bereich mündlicher oder schriftlicher Kommunikation.

## **b) Eingriffstiefe**

Die Beschwerdeschrift führt aus, dass § 113a TKG einer **Antastung des Wesensgehaltes** des Fernmeldegeheimnisses zumindest nahe kommt.<sup>70</sup> Art. 10 GG enthält die Grundentscheidung für eine freie, unbeobachtete und unkontrollierte, technisch vermittelte Kommunikation per Distanz. Diese Grundentscheidung des Grundgesetzes – ebenso wie diejenige des Art. 8 EMRK – betrifft nicht nur die Inhalte, sondern auch die Kommunikationsvorgänge, Kommunikationspartner und Kommunikationsumstände. Eben jene Grundentscheidung des Grundgesetzes wird durch die Vorratsdatenspeicherung in ihr Gegenteil verkehrt. Die Entscheidung für die technisch vermittelte Kommunikation soll nunmehr die Entscheidung für den registrierten Kommunikationsvorgang sein. Dies steht mit Art. 10 GG nicht im Einklang.

Die Aufzeichnung der eigenen Telekommunikation kann im Schutz- und Anwendungsbereich des Art. 10 GG **nicht mehr auf legale Weise vermieden werden**. Eine Vermeidung ist ausschließlich durch die Entscheidung für die unmittelbare Kommunikation – ohne technische Vermittlung und damit außerhalb des Schutzbereichs des Art. 10 GG –, für die schriftliche Kommunikation per Post – ohne technische Vermittlung und damit außerhalb des Schutzbereichs des Fernmeldegeheimnisses – oder durch Unterlassung der Kommunikation möglich. Alle drei Alternativen sind mit dem Schutzgedanken des Fernmeldegeheimnisses unvereinbar: Dieses soll gerade verhindern, dass elektronische Kommunikation per Distanz allein wegen der Registrierung oder Überwachung unterbleibt.

Tatsächlich gibt es im Grundgesetz **kein anderes Freiheitsgrundrecht, welches so weit eingeschränkt ist** wie das Fernmeldegeheimnis. Keine andere grundrechtlich geschützte Freiheit steht generell unter dem Vorbehalt, dass jedes Gebrauchmachen von dem Grundrecht zwangsweise registriert wird. Wenn man darin nicht schon eine

---

<sup>68</sup> Etwa Schriftsatz vom 05.05.2009, 8 ff. im Parallelverfahren 1 BvR 1299/05.

<sup>69</sup> Beschwerdeschrift, 127.

<sup>70</sup> Beschwerdeschrift, 51.

Verletzung der Wesensgehaltsgarantie des Art. 19 Abs. 2 GG sieht, so verletzt § 113a TKG jedenfalls das Übermaßverbot.

### c) Negative Auswirkungen der Vorratsdatenspeicherung

In der Beschwerdeschrift ist ausgeführt worden, dass § 113a TKG die Gefahr begründet, **zu Unrecht in den Verdacht einer Straftat** zu geraten oder sonstige Nachteile wegen des eigenen Kommunikationsverhaltens zu erleiden.<sup>71</sup> In der Anlage zum Schriftsatz vom 23.02.2008 wurden nur exemplarisch einige wenige Fälle genannt, in denen Kommunikationsdaten unberechtigte Wohnungsdurchsuchungen nach sich gezogen haben. Eine empirische Untersuchung über das Ausmaß des Fehlerrisikos in Deutschland fehlt.

In Großbritannien besteht dagegen eine Meldepflicht für Fehler, „die dazu geführt haben, dass [eine Behörde] die falschen Kommunikationsdaten erhalten hat und dies zu einem Eingriff in die Privatsphäre eines unschuldigen Dritten geführt hat.“<sup>72</sup> Allein im Jahr 2008 zeigten britische Behörden und Telekommunikationsunternehmen **hunderter solcher Fehler** bei dem staatlichen Zugriff auf Telekommunikationsdaten an (2008: 595 Fehler). Die berichteten Fehler beruhten beispielsweise auf der fehlerhaften Eingabe von Telefonnummern.

Diese Statistik zeigt, dass **jährlich hunderte von unschuldigen** Telekommunikationsnutzern befürchten müssen, zu Unrecht staatlichen Eingriffsmaßnahmen ausgesetzt zu werden. Nur wenn schon eine Speicherung der irrtumsanfälligen Telekommunikationsdaten unterbleibt, lässt sich dieses Risiko zuverlässig ausschließen. Der britische Kommunikationsüberwachungsbeauftragte weist in seinem Bericht zu Recht darauf hin, dass der „menschliche Irrtum natürlich nie vollständig eliminiert werden kann.“ Eben aus diesem Grund darf die fehleranfällige Erfassung von Telekommunikationsdaten nach Art. 10 GG stets nur aus triftigem Grund und im Einzelfall angeordnet werden und niemals anlasslos und flächendeckend.

Die Anlegung eines Datenvorrates hat gegenüber verfassungsgemäßer Verwendungsregeln einen überschießenden Eingriffsgehalt. Aus der prinzipiellen Möglichkeit des Zugriffs auf Datenvorräte bei nur **eingeschränkter rechtlicher Steuerungs- und Begrenzungskapazität** hinsichtlich solcher Zugriffe resultiert eine Minderung des grundrechtlichen Schutzniveaus durch angelegte Datenvorräte. Die eingeschränkte Kontrollierbarkeit ergibt sich dabei insbesondere aus:

- faktischen Möglichkeiten des Zugriffs an rechtlichen Grenzen vorbei, dessen Aufklärung, Entdeckung und Verhinderung umso schwieriger ist, wenn der Zugriff heimlich und für Betroffene unkontrollierbar erfolgt (Stichwort: Datenskandale oder Missbrauch durch Unternehmen, deren Mitarbeiter, Behörden oder deren Mitarbeiter),
- Umsetzungs- und Vollzugsdefiziten bei der Zweckbindung und -begrenzung der Datenvorräte von außerhalb der speichernden Stelle und
- der Gefahr von Daten- und Ermittlungsspannen (z.B. falscher Verdacht), welche schwerste Nachteile für die Betroffenen nach sich ziehen können.

---

<sup>71</sup> Beschwerdeschrift, 85 f.

<sup>72</sup> Zum Folgenden: Kennedy, Report of the Interception of Communications Commissioner for 2008, <http://www.official-documents.gov.uk/document/hc0809/hc09/0901/0901.pdf>.

In der Beschwerdeschrift ist ausgeführt worden, dass die engen Voraussetzungen, unter denen eine Vorratsdatenspeicherung **ausnahmsweise für zulässig** gehalten worden ist, im Fall des § 113a TKG nicht erfüllt sind.<sup>73</sup>

## II. Verletzung des Art. 5 GG

Die Beschwerdeschrift führt aus, dass § 113a TKG **die Meinungs- und Informationsfreiheit unverhältnismäßig weitgehend einschränkt**.<sup>74</sup> Mit Schriftsatz vom 23.02.2009 ist darauf hingewiesen worden, dass das Grundrecht auf freie Meinungsäußerung nach der Rechtsprechung des Obersten Gerichtshofes der USA auch das Recht auf anonyme Meinungsäußerung schützt.<sup>75</sup>

Inzwischen hat erstmals auch der **Bundesgerichtshof** entschieden, die anonyme Nutzung sei „dem Internet immanent“. Eine Beschränkung der Meinungsäußerungsfreiheit auf Äußerungen, die einem bestimmten Individuum zugeordnet werden können, sei mit Art. 5 Abs. 1 Satz 1 GG nicht vereinbar.<sup>76</sup> Die Verpflichtung, sich namentlich zu einer bestimmten Meinung zu bekennen, würde die Gefahr begründen, dass der Einzelne aus Furcht vor Repressalien oder sonstigen negativen Auswirkungen sich dahingehend entscheide, seine Meinung nicht zu äußern. Dieser Gefahr der Selbstzensur solle das Grundrecht auf freie Meinungsäußerung gerade entgegen wirken.

Da **§ 113a TKG** eine anonyme Meinungsäußerung über Kommunikationsnetze generell unmöglich macht, verletzt die Vorschrift auch Art. 5 GG.

## III. Verletzung des Art. 12 GG

Die Beschwerdeschrift führt aus, dass die **entschädigungslose Inpflichtnahme** von Telekommunikationsunternehmen zur Vorratsdatenspeicherung die Berufsfreiheit der Anbieter unverhältnismäßig weit einschränkt<sup>77</sup> und auch das Gleichbehandlungsgebot verletzt.<sup>78</sup> Im Anschluss an die Verfassungsgerichte Frankreichs und Österreichs sowie den Vorlagebeschluss des VG Berlin zu § 110 TKG haben sich inzwischen auch Braun<sup>79</sup> und Kleszczewski<sup>80</sup> dieser Auffassung angeschlossen.

## IV. Verletzung des Art. 3 GG

In der Beschwerdeschrift ist ausgeführt worden, dass der Gesetzgeber das Gleichbehandlungsgebot verletzt, wenn er sich unter mehreren gleich wirksamen Mitteln nur für das tiefer in die Grundrechte eingreifende entscheidet.<sup>81</sup> Neben anderen Mitteln ist dort die Möglichkeit angesprochen worden, Sicherheitsbehörden zu ermächtigen, im Einzelfall die Aufbewahrung bereits gespeicherter

---

<sup>73</sup> Beschwerdeschrift, 73 ff.

<sup>74</sup> Beschwerdeschrift, 118 ff.

<sup>75</sup> Schriftsatz vom 23.02.2009, 6 f.

<sup>76</sup> BGH vom 23.06.2009, Az. VI ZR 196/08.

<sup>77</sup> Beschwerdeschrift, 106 ff.

<sup>78</sup> Beschwerdeschrift, 144 ff.

<sup>79</sup> K&R 2009, 386.

<sup>80</sup> In: Weßlau/Wohlers, Festschrift Fezer (2008), 19 ff.

<sup>81</sup> Beschwerdeschrift, 135.

Kommunikationsdaten anzuordnen (sog. „**Quick Freeze-Verfahren**“). Diese Möglichkeit ist in den Art. 16, 17 der Cybercrime-Konvention des Europarates vorgesehen. Sie hat sich in anderen Staaten anstelle einer globalen und pauschalen Vorratsdatenspeicherung bewährt (z.B. in den USA, Kanada, Japan).

Obwohl dieses Mittel eine Vorratsdatenspeicherung nicht in jedem Fall ersetzen kann, belegt eine neue **Entscheidung des Landgerichts Hamburg**, wie wirksam Aufbewahrungsanordnungen gerade im Bereich des Internet sind.<sup>82</sup> Aus dieser Entscheidung geht hervor, in welchem Verfahren die Unterhaltungsindustrie Urheberrechtsverletzer auch ohne Vorratsdatenspeicherung ermittelt. Stellt die Unterhaltungsindustrie fest, dass ihre Werke rechtswidrig in Internet-Tauschbörsen zum Abruf bereit gestellt werden, so bittet sie sofort – also noch während der fortbestehenden Internetverbindung des Nutzers – den genutzten Internet-Zugangsanbieter, die Identität des verdächtigen Nutzers für ein späteres Auskunftverlangen festzuhalten. Weil Internetnutzer üblicherweise einen Pauschaltarif („Flatrate“) nutzen und zunehmend den ganzen Tag lang mit dem Internet verbunden sind, lassen sich die meisten Verletzer auf diese Weise noch „auf frischer Tat“ anhand ihrer Kennung (IP-Adresse) ermitteln. Das Landgericht Hamburg hat entschieden, Internet-Zugangsanbieter müssten während der normalen Geschäftszeiten einem solchen Aufbewahrungsverlangen Folge leisten.<sup>83</sup>

Unabhängig von der Frage, ob diese Entscheidung mit dem geltenden Recht vereinbar ist, zeigt das Urteil doch, dass es **mit hohen Erfolgsaussichten** möglich ist, Internet-Flatratenutzer im Verdachtsfall mithilfe eines Aufbewahrungsverlangens auch ohne eine flächendeckende Vorratsdatenspeicherung zu identifizieren. Das Verfahren zum Erlass einer Aufbewahrungsanordnung könnte so ausgestaltet werden, dass die Staatsanwaltschaft oder die Polizei von Telekommunikationsanbietern rund um die Uhr telefonisch verlangen kann, die Identität eines bestimmten Internetnutzers für ein späteres Auskunftersuchen festzuhalten. Mit diesem Verfahren können sich einerseits die 99,99% unbescholtenen Internetnutzer darauf verlassen, dass ihre Verbindungsdaten nicht über das Verbindungsende hinaus aufbewahrt werden und ihnen folglich keine Nachteile infolge falschen Verdachts, Datenpannen oder Missbrauch drohen. Andererseits verfügten die Ermittlungsbehörden über ein Instrument, das ihnen – zusammen mit Speicheranordnungen nach § 100g StPO – eine hohe Aufklärungsrate auch im Bereich von Netzkriminalität sichern würde.

Die Bundesregierung wendet ein, dieses Verfahren **führe in weniger Fällen zum Erfolg** als eine globale und pauschale Vorratsspeicherung der Internetverbindungen der gesamten Bevölkerung. Dem ist erstens entgegen zu halten, dass nicht belegt ist, ob und in wie vielen Fällen eine Vorratsdatenspeicherung letztlich zur Aufklärung von Straftaten führt, die im Wege einer Aufbewahrungs- oder Speicheranordnung nicht aufgeklärt werden könnten. Weder im zeitlichen Vergleich innerhalb Deutschlands noch im internationalen Vergleich zu Staaten ohne Vorratsdatenspeicherung (z.B. Österreich) ist belegt, dass eine globale und pauschale Vorratsdatenspeicherung im Vergleich zu gezielten Aufbewahrungs- oder Speicheranordnungen die Aufklärungsrate erhöhe oder gar die Kriminalitätsrate senke. Dies mag darauf beruhen, dass auch im Fall einer Vorratsdatenspeicherung vielfältige Umgehungsmöglichkeiten zur Verfügung stehen, dass auch ohne

---

<sup>82</sup> LG Hamburg, MMR 2009, 570.

<sup>83</sup> LG Hamburg, MMR 2009, 570.



Vorratsdatenspeicherung andere Aufklärungsmöglichkeiten bestehen (z.B. bei Wiederholungstätern) und dass auch unter Geltung einer Vorratsdatenspeicherung die meisten Strafverfahren ohnehin eingestellt werden, zumal mittels Telekommunikation begangene Kriminalität ganz regelmäßig dem Bereich leichter Vergehen zuzuordnen ist. Zweitens ist dem Minderwertsargument entgegen zu halten, dass die allenfalls geringfügigen Vorteile einer Globalprotokollierung der Telekommunikation der gesamten Bevölkerung vollkommen außer Verhältnis zu ihren Nachteilen stehen. Dazu ist bereits umfassend vorgetragen worden.

Übrigens ist die Entscheidung des Landgerichts Hamburg gegen den Internet-Zugangsanbieter **Hansenet** ergangen, der sich bis heute weigert, die temporäre Internetkennung (dynamische IP-Adresse) seiner Nutzer ohne Anlass festzuhalten. Es ist nicht ersichtlich, dass Ermittlungsverfahren bei diesem Anbieter häufiger ohne Erfolg blieben als bei Anbietern, die sich § 113a TKG gebeugt haben.

Der **Oberste Gerichtshof Österreichs** hat erst jüngst bekräftigt, dass österreichische Internet-Zugangsanbieter die temporäre Internetkennung (dynamische IP-Adresse) ihrer Nutzer nicht protokollieren dürfen.<sup>84</sup> Es ist nicht ersichtlich, dass Ermittlungsverfahren in Österreich deswegen häufiger ohne Erfolg blieben als in Deutschland oder dass die Verfolgung von Netzkriminalität in Österreich dadurch gar „leer lief“.

## V. Auflösung datenschutzrechtlicher Grundsätze

Mit Schriftsatz vom 13.08.2009 ist darauf hingewiesen worden, dass eine auch nur teilweise Aufrechterhaltung des § 113a TKG einen **Dammbruch verfassungsrechtlicher Prinzipien** mit weitreichenden Konsequenzen nach sich ziehen würde.<sup>85</sup> Mit Schriftsatz vom 23.02.2009 ist berichtet worden, dass die EU bereits einen Rahmenbeschluss plant, der eine globale und pauschale Speicherung aller Flugreisedaten jedes Bürgers vorsieht.<sup>86</sup> Es ist darauf hingewiesen worden, dass Deutschland seine Zustimmung zu dem Vorhaben nur bis zur Entscheidung über die Verfassungsmäßigkeit des § 113a TKG zurückgestellt hat.

Die Gefahr, dass die anlasslose und flächendeckende Vorratsdatenspeicherung schrittweise auf andere Lebensbereiche ausgeweitet wird, hat sich inzwischen erstmals realisiert. Mit **§ 5 Abs. 1 BSIg n.F.**<sup>87</sup> hat der Deutsche Bundestag das BSI ermächtigt, ohne Anlass Informationen über unsere elektronische Kommunikation mit Bundesbehörden und über unsere Nutzung öffentlicher Internetportale von Bundesbehörden aufzuzeichnen, darunter wer sich wann für welche Internetseiten interessiert hat und nach welchen Worten er gesucht hat. Neben den näheren Umständen der Kommunikation sollen erstmals auch Inhalte (URLs) aufgezeichnet werden, was § 113a TKG noch ausschließt. Die nach § 5 Abs. 1 BSIg n.F. zu erhebenden Daten werden bis zur „unverzöglichen“ Auswertung auf Vorrat gespeichert. Im Anschluss sieht § 5 Abs. 2 BSIg n.F. eine dreimonatige

---

<sup>84</sup> OGH vom 14.7.2009, Az. 4 Ob 41/09x.

<sup>85</sup> Schriftsatz vom 13.08.2009, 34.

<sup>86</sup> Schriftsatz vom 23.02.2009, 9.

<sup>87</sup> BGBl. 2009 I 2821 (2823).

Vorratsspeicherung der Daten unter so geringen Voraussetzungen vor, dass die Speicherung – wie auch Bundesregierung und BSI zugestehen – in der Praxis permanent, global und pauschal erfolgen wird. Trotz schwerer Kritik des Bundesrats<sup>88</sup> und von Sachverständigen,<sup>89</sup> in deren Rahmen auch ausdrücklich auf die Unvereinbarkeit mit den Grundrechten hingewiesen wurde,<sup>90</sup> hat der Deutsche Bundestag § 5 Abs. 1 und 2 BSiG-E im Kern unverändert verabschiedet, ohne die darin vorgesehene globale Vorratsdatenspeicherung auch nur ansatzweise verfassungsrechtlich zu verteidigen.

§ 5 BSiG n.F. wird durch gesonderte Verfassungsbeschwerde angefochten werden müssen. Für die vorliegende Beschwerde ist entscheidend: Die Vorschrift bestätigt die Prognose, dass § 113a TKG einen Dambruch darstellt, der eine **Flut anlassloser Erfassungen unseres täglichen Lebens** nach sich ziehen wird, wenn ihm nicht durch Aufhebung des § 113a TKG Einhalt geboten wird. Die Zulässigkeit einer globalen und pauschalen Erfassung allein im Hinblick auf eine mögliche künftige staatliche Verwendung von Informationen droht allmählich alle Lebensbereiche zu erfassen, weil eine Globalspeicherung für den Staat stets und in allen Bereichen nützlich ist. Eine solche globale und pauschale Aufzeichnung des Verhaltens vollkommen unbescholtener Bürger war selbst unter totalitären Regimes wie der DDR undenkbar und widerspricht dem Menschenbild des Grundgesetzes zutiefst. Auch im Hinblick auf seine Präzedenzwirkung hinsichtlich der Zukunft des Datenschutzes muss § 113a TKG folglich aufgehoben werden.

Vier einfache Abschriften anbei.

Meinhard Starostik  
Rechtsanwalt

---

<sup>88</sup> BR-Drs. 62/09 (Beschluss), 5.

<sup>89</sup> BITKOM, Positionspapier vom 05.03.2009, 6; Deutscher Anwaltverein (DAV), Stellungnahme 2009-31 vom April 2009, INA-Drs. 16(4)588, 3; Breyer, Stellungnahme vom 07.05.2009, INA-Drs. 16(4)570 F, 14 ff.; Pfitzmann, Stellungnahme vom 07.05.2009, INA-Drs. 16(4)570 B, 1; Pohl (Präsident der Gesellschaft für Informatik e.V.), Stellungnahme vom 05.05.2009, INA-Drs. 16(4)570 C, 1 f.; Schaar, Stellungnahme vom 23.03.2009, INA-Drs. 16(4)570, 2.

<sup>90</sup> Deutscher Anwaltverein (DAV), Stellungnahme 2009-31 vom April 2009, 3; Breyer, Stellungnahme vom 07.05.2009, INA-Drs. 16(4)570 F, 18.