Meinhard Starostik

Rechtsanwalt/vereidigter Buchprüfer

Schlüterstr. 38 ◆ 10629 Berlin
Tel.: 030 - 88 000 345
Fax: 030 - 88 000 346
email: Kanzlei@Starostik.de
internet: www.Starostik.de

RA/vBP Starostik, Schlüterstr. 38, 10629 Berlin

An das
Bundesverfassungsgericht
Schloßbezirk 3

76131 Karlsruhe

Berlin, den 23. März 2007

AZ: 42/05
(bitte stets angeben)

Verfassungsbeschwerde

- 1 BvR 1299/05 -

In dem vorbezeichneten Verfahren nehme ich zu dem Schriftsatz des Bevollmächtigten der Bundesregierung vom 22.01.2007 wie folgt Stellung.

Inhalt

1 Zulässigkeit der Verfassungsbeschwerde

1.1 Wahrscheinlichkeit der Betroffenheit

Die Beschwerdeführer sind von den §§ 111, 95 Abs. 3 TKG sicher und von den §§ 112, 113 TKG jedenfalls mit einiger Wahrscheinlichkeit betroffen. Bei mehreren Millionen Abfragen jährlich liegt dies auf der Hand. Da Abfragen nach den §§ 112, 113 TKG offenbar bereits anhand aufgefundener Notizbücher und Einzelverbindungsnachweise erfolgen, ist es nicht unwahrscheinlich, dass einer der vielen privat oder geschäftlich mit den Beschwerdeführern bekannten Personen in ein Ermittlungsverfahren verwickelt wird und in diesem Zusammenhang eine Rufnummer der Beschwerdeführer nachgeprüft wird.

1.2 Gegenwärtige Betroffenheit von Ähnlichkeitssuche

Dass die Beschwerdeführer gegenwärtig von der gesetzlichen Ermächtigung zur Ähnlichkeitssuche betroffen sind, wird nicht dadurch in Frage gestellt, dass die Verordnung nach § 112 Abs. 3 TKG noch nicht erlassen sein und das Verfahren noch nicht praktiziert werden mag. Die entsprechende Rechtsverordnung kann jederzeit erlassen und das Verfahren jederzeit in Betrieb genommen werden. Im Fall eines Abwartens wäre die Beschwerdefrist des § 93 Abs. 3 BVerfGG im Hinblick auf § 112 TKG nicht mehr gewahrt.

1.3 Subsidiarität

Der Grundsatz der Subsidiarität der Verfassungsbeschwerde ist gewahrt. Der Rechtsweg zu den Fachgerichten steht den Beschwerdeführern bezüglich der §§ 112, 113 TKG nicht offen, weil sie von Abfragen keine Kenntnis erlangen. Auskünfte zur Datenschutzkontrolle (§ 112 Abs. 4 TKG) dürfen nur an die zuständige Kontrollstelle – die Datenschutzbeauftragten – erteilt werden, nicht aber an den Betroffenen (§ 112 Abs. 4 S. 4 TKG). Die Datenschutzbeauftragten wiederum sind, von vorgefundenen Datenschutzverstößen abgesehen, zur Verschwiegenheit verpflichtet (§ 23 Abs. 5 BDSG).

Eine Auskunft bei allen in den §§ 112, 113 TKG genannten Behörden einzuholen, um etwa erfolgte Bestandsdatenabfragen festzustellen, ist den Beschwerdeführern offensichtlich unzumutbar.[1] Durch die föderale Untergliederung Deutschlands handelt es sich um Hunderte verschiedener Stellen. Außerdem wüsste die Auskunft erteilende Person ohne Nennung eines bestimmten Verfahrens nicht, ob einer der Bediensteten der Behörde in irgend einem Verfahren einmal die Rufnummer der Beschwerdeführer abgefragt hat. Das Fachrecht sieht keine Zugriffsprotokollierung vor und gewährleistet nicht, dass entsprechende Anfragen beantwortet werden können. Das Fachrecht sieht zwar einen Auskunftsanspruch über gespeicherte Daten vor, nicht aber einen Auskunftsanspruch über in der Vergangenheit erfolgte Datenabfragen. Ohnehin unterliegt der Auskunftsanspruch so vielen Einschränkungen, dass die Auskunftserteilung oftmals rechtmäßig abgelehnt werden kann. Dies tun beispielsweise die Nachrichtendienste routinemäßig mit der Begründung, sie müssten eine „Ausforschung ihrer Arbeitsweise" verhindern.

Ferner gewährleistet die Möglichkeit der Anrufung von Fachgerichten keinen effektiven Rechtsschutz. Gegen die unmittelbar durch Gesetz erfolgte Grundrechtsverletzung ist der Rechtsweg nicht zulässig. Die Beschwerdeführer haben auch sonst keine andere Möglichkeit, um gegen die

1 Vgl. BVerfG, 1 BvR 2027/02 vom 23.10.2006, Abs. 44: „Zwar mag die Beschwerdeführerin zumindest gegenüber den meisten der genannten Personen und Stellen Ansprüche auf Auskunft über die bei ihnen vorhandenen Informationen über sie haben. Es ist aber weder realistisch noch zumutbar, von der Beschwerdeführerin zu erwarten, zur Durchsetzung ihres Rechts auf informationellen Selbstschutz von allen potentiell als Informanten in Betracht kommenden Stellen Auskunft zu verlangen."

Grundrechtsverletzung vorzugehen. Insbesondere ist es ihnen nicht zumutbar, vor den Fachgerichten gegen die Telekommunikationsunternehmen zu klagen. Die Fachgerichte können selbst keinen Rechtsschutz gegen die gesetzlich angeordnete Vorratsspeicherung gewähren. Eine fachgerichtliche Prüfung ist auch nicht zur Aufbereitung des Sachverhalts erforderlich, weil dieser klar auf der Hand liegt. Die Identifizierungs- und Vorratsspeicherungspflicht von Telekommunikationsdaten sowie der breite staatliche Zugriff darauf stellen ein so grundsätzliches Problem in einer freiheitlichen Gesellschaft dar, dass nur eine Entscheidung des Bundesverfassungsgerichts Rechtsfrieden schaffen kann.

1.4 Richtlinie 2006/24/EG

Die Richtlinie 2006/24/EG steht der Zulässigkeit der Beschwerde nicht entgegen.

Nach der Rechtsprechung des Bundesverfassungsgerichts sind zwar Verfassungsbeschwerden gegen europarechtlich zwingend vorgegebene deutsche Rechtsakte unzulässig, solange auf europäischer Ebene generell ein Grundrechtsschutz gewährleistet ist, welcher dem vom Grundgesetz unabdingbar gebotenen im Wesentlichen gleich kommt.[2] Die vorliegend angegriffenen Regelungen sind jedoch nicht zwingend europarechtlich vorgegeben (1.4.1 und 1.4.2) und könnten, selbst wenn man dies anders beurteilte, gleichwohl zulässig im Wege der Verfassungsbeschwerde angegriffen werden (1.4.3).

1.4.1 Fehlende Umsetzungspflicht nach Europarecht

Die angegriffenen Regelungen sind durch die Richtlinie 2006/24/EG jedenfalls insoweit nicht vorgegeben als sie über die Vorgaben der Richtlinie hinaus gehen.

Dies ist insbesondere bei § 111 TKG der Fall. Die Richtlinie 2006/24/EG sieht keine Identifizierungs- bzw. Datenerhebungspflicht vor. Sie schreibt lediglich vor, dass Daten zur Identifizierung von Kommunikationsteilnehmern, die ohnehin im Zuge der Bereitstellung von Telekommunikationsdiensten anfallen, auf Vorrat zu speichern sind. In Art. 3 Abs. 1 heißt es nämlich, „dass die in Artikel 5 der vorliegenden Richtlinie genannten Daten" nur zu speichern sind, „soweit sie [...] im Zuge der Bereitstellung der betreffenden Kommunikationsdienste von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes erzeugt oder verarbeitet werden". Bei vorausbezahlten oder kostenlosen Diensten fallen dagegen oft keine Bestandsdaten an. Dass die Richtlinie 2006/24/EG die anonyme Bereitstellung von Telekommunikation zulässt, ergibt sich auch aus Art. 5 Abs. 1 Buchst. e Nr. 2 vi. Nach dieser Bestimmung sollen „im Falle vorbezahlter anonymer Dienste: Datum und Uhrzeit der ersten Aktivierung des Dienstes und die Kennung des Standorts (Cell-ID), an dem der Dienst aktiviert wurde", auf Vorrat gespeichert werden. Diese Bestimmung setzt die Möglichkeit des Angebots anonymer Telekommunikationsdienste voraus. § 111 TKG verbietet folglich überschießend die anonyme Bereitstellung von Telekommunikationsdiensten.

Die §§ 112, 113 TKG sind von der Richtlinie nur insoweit vorgegeben, wie der Zugriff auf Bestandsdaten zur Aufklärung schwerer Straftaten zugelassen werden muss (Art. 1 Abs. 1 RiL 2006/46/EG). Die Vorratsspeicherungspflicht des § 95 Abs. 3 TKG ist von der Richtlinie nur teilweise vorgegeben, nämlich nur für die Dauer von sechs Monaten und nur für Namen und Anschrift der Teilnehmer. § 95 Abs. 4 TKG ist von der Richtlinie überhaupt nicht vorgegeben.

Ohnehin kann derzeit schon deshalb keine Pflicht zur Umsetzung der Richtlinie bestehen, weil die Umsetzungsfrist erst im September 2007 abläuft.

---

2 BVerfGE 102, 147, Ls. 1 und 2.

Vor allem aber ist Deutschland zur Umsetzung der Richtlinie 2006/24/EG nicht verpflichtet.

Nach der Rechtsprechung des Europäischen Gerichtshofs spricht für die Rechtsakte der Gemeinschaftsorgane grundsätzlich die Vermutung der Rechtmäßigkeit.[3] Rechtsakte entfalten dementsprechend Rechtswirkungen, solange sie nicht zurückgenommen, im Rahmen einer Nichtigkeitsklage für nichtig erklärt oder infolge eines Vorabentscheidungsersuchens oder einer Rechtswidrigkeitseinrede für ungültig erklärt worden sind.[4] Gegen eine Klage wegen Vertragsverletzung durch Nichtumsetzung einer Richtlinie kann ein Mitgliedsstaat die Nichtigkeit der Richtlinie nicht einwenden.[5] Der Mitgliedsstaat hat nur die Möglichkeit, die Richtlinie im Wege der Nichtigkeitsklage anzufechten und in diesem Rahmen einen Antrag auf einstweilige Befreiung von der Pflicht zur Umsetzung der angegriffenen Richtlinie zu stellen (Art. 230, 242 EG). Dies hat die Bundesregierung vorliegend unterlassen.

Von der grundsätzlichen Vermutung der Rechtmäßigkeit macht der Europäische Gerichtshof indes eine Ausnahme bei Rechtsakten, die mit einem Fehler behaftet sind, dessen Schwere so offensichtlich ist, dass er von der Gemeinschaftsrechtsordnung nicht geduldet werden kann.[6] In einem solchen, nur ausnahmsweise anzunehmenden Fall ist der Rechtsakt von vornherein „inexistent" und erzeugt keine Befolgungs- oder Umsetzungspflicht.

Die Richtlinie 2006/24/EG erfüllt diese Voraussetzungen und löst daher keine Umsetzungspflicht aus:

1.4.1.1 Formelle Rechtswidrigkeit

Die Richtlinie ist in formeller Hinsicht rechtswidrig, weil die Europäische Gemeinschaft über keine Kompetenz zum Erlass der in der Richtlinie 2006/24/EG vorgesehenen Regelungen verfügte.

Kommission, Europaparlament und Rat stützen die Richtlinie 2006/24/EG auf Art. 95 EG als Rechtsgrundlage. Sie begründen dies mit Rechtsgutachten, die im Auftrag der Kommission[7] und des Rates[8] erstellt wurden. Diesen Gutachten zufolge sei die Speicherung von Kommunikationsdaten in der Richtlinie 2002/58/EG bereits umfassend gemeinschaftsrechtlich geregelt. Die Einführung von Mindestspeicherfristen für solche Daten falle deswegen als Annex ebenfalls in die Kompetenz der Europäischen Gemeinschaft nach Art. 95 EG. Außerdem beeinträchtigten unterschiedliche nationale Vorschriften zur Vorratsdatenspeicherung den Binnenmarkt.

Einige Mitgliedsstaaten wie Irland und die Slowakei sowie der Deutsche Bundestag vertreten demgegenüber die Auffassung, dass die dritte Säule der EU die richtige Rechtsgrundlage gewesen wäre, weil Ziel der Datenspeicherung die Erleichterung der Strafverfolgung ist. Im Juli 2006 reichte Irland beim Europäischen Gerichtshof eine Nichtigkeitsklage gegen die Richtlinie zur Vorratsdatenspeicherung ein (Az. C-301/06). Stützen kann es sich dabei auf die zwischenzeitlich ergangene Entscheidung des EuGH zur Fluggastdatenübermittlung in die USA.[9] Auch in jenem Fall hatte die Kommission die Datenübermittlung auf der Grundlage der Binnenmarktkompetenz (Art. 95 EG) autorisiert. Sie argumentierte, Fluggastdaten würden von den Fluggesellschaften zur Erbringung einer Dienstleistung erhoben und fielen deshalb in den Anwendungsbereich des

3 EuGHE 1979, 623; EuGH, C-475/01 vom 05.10.2004, Abs.-Nr. 18.

4 EuGH, C-475/01 vom 05.10.2004, Abs.-Nr. 18.

5 EuGH, C-139/03 vom 15.07.2004, Abs.-Nr. 7.

6 EuGHE 1988, 3611; EuGHE I 1992, 5437; EuGH, C-475/01 vom 05.10.2004, Abs.-Nr. 19; st. Rspr.

7 Juristische Analyse vom 22.03.2005, SEC(2005)420, http://www.statewatch.org/news/2005/apr/Commission-legal-opinion-data-retention.pdf.

8 Rechtsgutachten des Juristischen Dienstes des Rates vom 05.04.2005, http://www.statewatch.org/news/2005/apr/Council-legal-opinion-data-retention.pdf.

9 EuGH, Urteil vom 30.05.2006, Az. C-317/04 und C-318/04.

Gemeinschaftsrechts. Zum Funktionieren des Binnenmarkts sei eine harmonisierte Regelung der Fluggastdatenübermittlung erforderlich, weil international agierende Unternehmen ansonsten in jedem Mitgliedsstaat unterschiedlichen Regelungen nachkommen müssten.

Der Europäische Gerichtshof verwarf diese Argumentation und erklärte die Rechtsakte mangels Kompetenz der Europäischen Gemeinschaft für nichtig. Die Binnenmarktkompetenz des Art. 95 EG sei nicht einschlägig. Die Fluggastdatenübermittlung sei „eine Datenverarbeitung, die nicht für die Erbringung einer Dienstleistung erforderlich ist, sondern zum Schutz der öffentlichen Sicherheit und zu Strafverfolgungszwecken als erforderlich angesehen wird."[10]

Auch die Vorratsspeicherung von Telekommunikationsdaten ist nicht für die Erbringung einer Dienstleistung der Telekommunikationsunternehmen erforderlich, sondern wird lediglich zu Strafverfolgungszwecken als erforderlich angesehen (vgl. Art. 1 RiL 2006/24/EG). Damit kommt Art. 95 EG als Rechtsgrundlage auch für die Vorratsdatenspeicherung nicht in Frage, so dass die Richtlinie zur Vorratsdatenspeicherung mangels Rechtsgrundlage nichtig ist.[11]

Übrigens hatte der Generalanwalt bereits in seinen Schlussanträgen zur Fluggastdatenübermittlung die fehlende Kompetenz der Europäischen Gemeinschaft abstrahiert auf alle Fälle, in denen „eine juristische Person zu einer solchen Datenverarbeitung und zur Übermittlung dieser Daten verpflichtet" wird.[12] Die Ausführungen waren also keineswegs auf den Einzelfall beschränkt. Der Generalanwalt hat sogar ausdrücklich auf die Vorratsdatenspeicherung Bezug genommen.[13]

1.4.1.2 Materielle Rechtswidrigkeit

Die Richtlinie 2006/24/EG ist auch materiell rechtswidrig, weil sie gegen mehrere Gemeinschaftsgrundrechte verstößt.

Einen Teil des primären Gemeinschaftsrechts stellen die Gemeinschaftsgrundrechte dar, die der Europäische Gerichtshof als „allgemeine Grundsätze des Gemeinschaftsrechts"[14] aus den Rechtstraditionen der Mitgliedstaaten entwickelt hat. Der Europäische Gerichtshof wendet dabei in der Regel die EMRK in ihrer Auslegung durch den Europäischen Gerichtshof für Menschenrechte an[15]. Entsprechend Art. 8 EMRK hat der Europäische Gerichtshof beispielsweise den Schutz der Privatsphäre als Gemeinschaftsgrundrecht anerkannt[16].

Die Gemeinschaftsgrundrechte gelten für Sachverhalte mit gemeinschaftsrechtlichem Bezug. Bei Handlungen oder Unterlassungen eines Organs der Europäischen Gemeinschaft ist ein solcher Bezug stets gegeben. Die Gemeinschaftsgrundrechte sind also anwendbar, wenn eine Vorratsspeicherung von Telekommunikationsdaten im Wege einer Richtlinie eingeführt wird.

Im Jahr 2000 wurde die Charta der Grundrechte der Europäischen Union[17] beschlossen. Die Grundrechtscharta kann als Fest- und Fortschreibung der richterrechtlich entwickelten Gemeinschaftsgrundrechte angesehen werden. In Artikel 7 der Charta wird ein Recht der Bürger auf Achtung ihrer „Kommunikation" garantiert. In Artikel 8 findet sich ein Grundrecht auf Schutz der eigenen personenbezogenen Daten, das auch die Aufsicht einer unabhängigen Stelle über jede Verarbeitung personenbezogener Daten vorsieht.

---

10 EuGH, Urteil vom 30.05.2006, Az. C-317/04 und C-318/04, Abs. 57.
11 Simitis, NJW 2006, 2011 (2013); Westphal, EuZW 2006, 555 (557).
12 Abs-Nr. 160 der Schlussanträge vom 22.11.2005.
13 a.a.O.
14 Schwarze-Stumpf, Art. 6 EUV, Rn. 19.
15 EuGH, Urteil vom 20.05.2003, Az. C-465/00, EuGRZ 2003, 232 (238), Abs. 69 und 73 ff.
16 EuGH, Urteil vom 20.05.2003, Az. C-465/00, EuGRZ 2003, 232 (238), Abs. 68 ff.
17 ABl. EG Nr. C 364 vom 18.12.2000, www.europarl.eu.int/charter/pdf/text_de.pdf.

1.4.1.2.1 Das Recht auf Achtung des Privatlebens und der Korrespondenz (Artikel 8 EMRK)

1.4.1.2.1.1 Eingriff in den Schutzbereich

Was den Schutz des Einzelnen vor der Verarbeitung seiner Telekommunikations-Verkehrsdaten durch die EMRK anbelangt, so kommt vor allem eine Anwendung des Art. 8 EMRK in Betracht. Diese Norm garantiert unter anderem das Recht auf Achtung des Privatlebens und der Korrespondenz. Fraglich ist, ob eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten einen Eingriff in Art. 8 EMRK darstellt. Der Europäische Gerichtshof für Menschenrechte (EGMR) hat wiederholt entschieden, dass auch Telefongespräche als „Korrespondenz" im Sinne des Art. 8 EMRK anzusehen sind[18]. Trotz des jedenfalls im Deutschen abweichenden Wortlauts ist diese Gleichstellung teleologisch geboten, weil sich der Bürger in beiden Fällen in einer vergleichbaren Gefährdungslage bezüglich seiner räumlich distanzierten Kommunikation befindet. Aus demselben Grund liegt es nahe, auch die näheren Umstände der Telekommunikation unter den Begriff der „Korrespondenz" zu fassen.

Die Subsumtion unter den Begriff des „Privatlebens" fällt leichter, weil der Gerichtshof unter Bezugnahme auf die Datenschutzkonvention allgemein anerkennt, dass die Sammlung und Speicherung personenbezogener Daten einen Eingriff in das Privatleben des Einzelnen darstellt[19], ebenso wie die Verwendung solcher Daten und die Verweigerung ihrer Löschung[20].

In vergangenen Urteilen hat der Gerichtshof wiederholt entschieden, dass die Erhebung von Verbindungsdaten ohne Einwilligung des Betroffenen einen Eingriff in dessen Rechte auf Achtung der Korrespondenz und des Privatlebens darstellt[21], weil Verbindungsdaten, „besonders die gewählten Nummern [...] integraler Bestandteil der Kommunikation" seien[22]. Entsprechend der in der Beschwerdeschrift zu Art. 10 Abs. 1 Var. 3 GG aufgeführten Argumentation[23] ist die Vorratsspeicherung von Verkehrsdaten daher als Eingriff in Art. 8 EMRK anzusehen, selbst wenn sie von Privaten durchgeführt wird[24]. Art. 8 EMRK schützt dabei sowohl geschäftliche als auch private Kommunikation[25].

1.4.1.2.1.2 Rechtfertigung des Eingriffs

Erfordernis einer gesetzlichen Grundlage

Eingriffe in den Schutzbereich des Art. 8 EMRK bedürfen der Rechtfertigung. Gemäß Art. 8 Abs. 2 EGMR ist zunächst eine gesetzliche Grundlage für Eingriffe erforderlich. Als „Gesetz" sieht das Gericht nicht nur verbindliche Rechtsnormen, sondern auch eine gefestigte innerstaatliche Rechtsprechung an[26]. Rechtlich unverbindliche Regulierungsmechanismen wie deutsche Verwaltungs-

18 Frowein/Peukert-Frowein, Art. 8, Rn. 34 m.w.N.

19 Frowein/Peukert-Frowein, Art. 8, Rn. 5 m.w.N.

20 EGMR, Leander-S (1987), Publications A116, Abs. 48; EGMR, Rotaru-ROM (2000), Decisions and Reports 2000-V, Abs. 46.

21 EGMR, Malone-GB (1984), EuGRZ 1985, 17 (23), Abs. 84; EGMR, Valenzuela Contreras-ES (1998), Decisions and Reports 1998-V, Abs. 47; EGMR, P.G. und J.H.-GB (2001), Decisions and Reports 2001-IX, Abs. 42.

22 EGMR, Malone-GB (1984), EuGRZ 1985, 17 (23), Abs. 84.

23 Beschwerdeschrift, 14 ff.

24 So auch Allitsch, CRi 2002, 161 (166); Covington & Burling, Memorandum (I), 3; ebenso die Verfasser des RSV-Entwurfs in dessen Erwägungsgrund 9.

25 EGMR, Niemietz-D (1992), Publications A251-B, Abs. 29, 31 und 33; EGMR, Rotaru-ROM (2000), Decisions and Reports 2000-V, Abs. 43; EGMR, Amann-CH (2000), Decisions and Reports 2000-II, Abs. 65.

26 EGMR, Huvig-F (1990), Publications A176-B, Abs. 28.

vorschriften oder eine bestimmte Praxis der zuständigen Organe genügen dagegen nicht[27]. Einen Parlamentsvorbehalt kennt das Gericht nicht.

Die Entscheidung, ob eine Einzelmaßnahme nach nationalem Recht rechtmäßig ist, überlässt der EGMR grundsätzlich den nationalen Gerichten[28], wobei deren Entscheidung nachvollziehbar sein muss[29]. Aus dem Erfordernis einer gesetzlichen Grundlage in Verbindung mit dem in der Präambel der EMRK erwähnten Rechtsstaatsprinzip leitet der EGMR zudem ab, dass das eingreifende innerstaatliche Recht hinreichend bestimmt und für den Bürger zugänglich sein muss[30]. Dem Einzelnen müsse es möglich sein, sein Verhalten den Vorschriften entsprechend einzurichten, was ein – gemessen an der Schwere des Eingriffs[31] – hinreichendes Maß an Vorhersehbarkeit voraussetze[32]. Ob diese Voraussetzungen gegeben sind, prüft der Gerichtshof selbst.

Aus dem Rechtsstaatsprinzip leitet der EGMR auch inhaltliche Anforderungen an das einzelstaatliche Recht ab. So muss das nationale Recht einen hinreichenden und effektiven Schutz vor willkürlichen Eingriffen und vor Missbrauch der eingeräumten Befugnisse gewährleisten, wobei der Gerichtshof betont, dass dieses Risiko gerade bei Maßnahmen ohne Wissen des Betroffenen „evident" sei[33]. Bei solchen Maßnahmen muss unter anderem eine effektive, rechtsstaatliche, unabhängige und unparteiische Kontrolle über eingreifende Maßnahmen gewährleistet sein, welche grundsätzlich, zumindest als nachträglicher Rechtsbehelf, durch die Justiz zu gewährleisten ist[34]. Welche rechtsstaatlichen Sicherungen von der EMRK gefordert werden, hängt vom Einzelfall ab, insbesondere von der Art, dem Umfang und der Dauer möglicher Maßnahmen, den Voraussetzungen für ihre Anordnung, den für die Anordnung, Durchführung und Kontrolle zuständigen Organen sowie den verfügbaren Rechtsbehelfen[35].

Räumt das nationale Recht der Exekutive oder dem zuständigen Richter ein Ermessen bei der Anordnung von Maßnahmen ein, dann verlangt das Bestimmtheitserfordernis – auch und gerade bei geheimen Maßnahmen –, dass der zulässige Zweck der Maßnahme, die Reichweite und Grenzen des Ermessens und die Kriterien, nach denen es auszuüben ist, hinreichend erkennbar sind, insbesondere, dass vorhersehbar ist, unter welchen Umständen und Bedingungen Eingriffe zulässig sind[36]. Die Anforderungen an die Vorhersehbarkeit im Einzelnen hängen von der Eingriffstiefe der jeweiligen Maßnahme ab, so dass schwerwiegende Eingriffe eine besonders präzise gesetzliche Regelung erforderlich machen[37].

Für den Fall einer Informationssammlung und -speicherung durch einen Geheimdienst wurde etwa entschieden, dass das nationale Recht detailliert festlegen muss, welche Arten von Informationen gespeichert werden dürfen, gegenüber welchen Personengruppen Überwachungsmaßnahmen ergriffen werden dürfen, unter welchen Umständen Informationen gesammelt werden dürfen, welches Verfahren dabei einzuhalten ist, nach welcher Zeitdauer erlangte Informationen

27 Vgl. EGMR, Khan-GB (2000), Decisions and Reports 2000-V, Abs. 27.
28 EGMR, Kruslin-F (1990), Publications A176-A, Abs. 29.
29 Vgl. EGMR, Craxi-IT (2003), hudoc.echr.coe.int/Hudoc1doc/HEJUD/200307/craxi%20-%2025337jv.chb1%2017072003e(sl).doc, Abs. 78 und 81.
30 EGMR, Sunday Times-GB (1979), EuGRZ 1979, 386 (387), Abs. 49; EGMR, Silver u.a.-GB (1983), EuGRZ 1984, 147 (150), Abs. 87 und 88; EGMR, Lambert-F (1998), Decisions and Reports 1998-V, Abs. 23.
31 EGMR, Kruslin-F (1990), Publications A176-A, Abs. 33.
32 EGMR, Silver u.a.-GB (1983), EuGRZ 1984, 147 (150), Abs. 88; EGMR, Malone-GB (1984), EuGRZ 1985, 17 (20), Abs. 66; EGMR, Amann-CH (2000), Decisions and Reports 2000-II, Abs. 56.
33 EGMR, Malone-GB (1984), EuGRZ 1985, 17 (20 und 22), Abs. 67 und 81.
34 EGMR, Klass u.a.-D (1978), EuGRZ 1979, 278 (286), Abs. 55; EGMR, Rotaru-ROM (2000), Decisions and Reports 2000-V, Abs. 59.
35 EGMR, Klass u.a.-D (1978), EuGRZ 1979, 278 (285), Abs. 50.
36 EGMR, Silver u.a.-GB (1983), EuGRZ 1984, 147 (150), Abs. 88; EGMR, Malone-GB (1984), EuGRZ 1985, 17 (20 f.), Abs. 67 und 68; EGMR, Leander-S (1987), Publications A116, Abs. 51; EGMR, Valenzuela Contreras-ES (1998), Decisions and Reports 1998-V, Abs. 60; EGMR, Khan-GB (2000), Decisions and Reports 2000-V, Abs. 26.
37 EGMR, Kopp-CH (1998), StV 1998, 683 (684), Abs. 72.

zu löschen sind, welche Personen auf den Datenbestand zugreifen dürfen, die Art und Weise der Speicherung, das Verfahren des Informationsabrufs sowie die zulässigen Verwendungszwecke für die abgerufenen Informationen[38].

Zum Schutz vor Missbrauch durch Telefonüberwachung ohne Wissen des Betroffenen hat der Gerichtshof die detaillierte Festlegung der folgenden Umstände durch das nationale Recht gefordert: gegen welche Personen und bei welchen Straftaten das Instrument der Telefonüberwachung eingesetzt werden darf, die maximale Dauer der Überwachungsmaßnahme, das Verfahren, in welchem Abhörprotokolle erstellt werden, die Sicherungsmaßnahmen dafür, dass die Originalbänder intakt und in ihrer Gesamtheit erhalten bleiben, damit sie vom Richter und dem Verteidiger des Beschuldigten untersucht werden können, sowie Fristen für die Löschung der erlangten Informationen[39]. Für den Fall, dass unbeteiligte Dritte von einer Überwachungsmaßnahme betroffen sind (z.B. als Gesprächspartner eines Verdächtigen), müssen Sicherungsvorkehrungen in Bezug auf deren Daten vorgesehen werden[40].

Auch wenn Strafverfolgungsorgane um die Herausgabe von Daten „bitten", ohne das Telekommunikationsunternehmen dazu zu verpflichten, ist erforderlich, dass die freiwillige Übermittlung der angeforderten Daten nach innerstaatlichem Recht rechtmäßig und dass die Befugnis der Strafverfolgungsorgane zur Anforderung solcher Daten im innerstaatlichen Recht detailliert geregelt ist[41]. In jedem Fall muss der Staat angemessene Maßnahmen ergreifen, um zu verhindern, dass Dritte unbefugt Kenntnis von überwachten Telekommunikationsinhalten erlangen[42].

Erforderlichkeit in einer demokratischen Gesellschaft

Liegt eine gesetzliche Grundlage der fraglichen Maßnahme nach den vorgenannten Kriterien vor, dann muss die Maßnahme nach Art. 8 Abs. 2 EMRK zusätzlich in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer erforderlich sein. Die einzelnen Staaten haben nach der Rechtsprechung des Gerichtshofs einen Beurteilungsspielraum bezüglich der Frage, ob eine Maßnahme zu einem der in Art. 8 Abs. 2 EMRK genannten Zwecke erforderlich ist[43]. Dabei behält sich der EGMR aber das Letztentscheidungsrecht vor, so dass er selbst vertretbare nationale Entscheidungen verwerfen kann[44]. Hinsichtlich des Ausmaßes des nationalen Beurteilungsspielraums schwankt das Gericht von Entscheidung zu Entscheidung[45].

In einer demokratischen Gesellschaft erforderlich ist eine Maßnahme nur, wenn ein in Anbetracht des Stellenwerts des garantierten Freiheitsrechts hinreichend dringendes soziales Bedürfnis nach ihr besteht, sie einen legitimen Zweck verfolgt und ihre Belastungsintensität nicht außer Verhältnis

38 EGMR, Rotaru-ROM (2000), Decisions and Reports 2000-V, Abs. 57.
39 EGMR, Kruslin-F (1990), Publications A176-A, Abs. 35; EGMR, Valenzuela Contreras-ES (1998), Decisions and Reports 1998-V, Abs. 46.
40 EGMR, Amann-CH (2000), Decisions and Reports 2000-II, Abs. 61.
41 EGMR, Malone-GB (1984), EuGRZ 1985, 17 (23), Abs. 87.
42 EGMR, Craxi-IT (2003), hudoc.echr.coe.int/Hudoc1doc/HEJUD/200307/craxi%20-%2025337jv.chb1%2017072003e(sl).doc, Abs. 74.
43 EGMR, Sunday Times-GB (1979), EuGRZ 1979, 386 (388 f.), Abs. 59; EGMR, Silver u.a.-GB (1983), EuGRZ 1984, 147 (152), Abs. 97; EGMR, Lambert-F (1998), Decisions and Reports 1998-V, Abs. 30; EGMR, Foxley-GB (2000), hudoc.echr.coe.int/Hudoc1doc2/HEJUD/200107/foxley%20-%2033274jv.chb3%2020062000e.doc, Abs. 43.
44 EGMR, Sunday Times-GB (1979), EuGRZ 1979, 386 (389), Abs. 59.
45 Van Dijk/van Hoof, Theory and Practise of the European Convention on Human Rights, 585 ff.

zu dem Gewicht des Zwecks steht[46]. Der EGMR hat dazu eindeutig erklärt, dass das Interesse des Staates gegenüber den Interessen des Einzelnen an der Achtung seiner Privatsphäre abgewogen werden müsse[47]. Eingriffe sind zwar nicht auf das unerlässliche Maß beschränkt, aber ein bloßes Nützlich- oder Wünschenswertsein genügt nicht[48]. Sind die genannten Kriterien erfüllt, dann liegt keine Verletzung von Art. 8 EMRK vor.

Ergebnis

In Bezug auf die Vorratsspeicherung von Telekommunikationsdaten wurde die Rechtsprechung des EGMR teilweise so interpretiert, dass jede Form einer groß angelegten, allgemeinen oder sondierenden elektronischen Überwachung unzulässig sei,[49] insbesondere, wenn nicht wegen einer bestimmten Tat oder Gefahr ermittelt wird, sondern nach möglichen Taten oder Gefahren erst gesucht werden soll.[50] Jedenfalls gelten die in der Beschwerdeschrift zum Grundgesetz gemachten Ausführungen analog, wonach eine generelle Telekommunikationsdatenspeicherung das Verhältnismäßigkeitsgebot verletzt. Eine generelle Vorratsspeicherung von Telekommunikationsdaten ist daher mit Art. 8 EMRK unvereinbar.

1.4.1.2.2 Die Freiheit der Meinungsäußerung (Artikel 10 EMRK)

Art. 10 Abs. 1 S. 1 und 2 EMRK bestimmt: „Jeder hat Anspruch auf freie Meinungsäußerung. Dieses Recht schließt die Freiheit der Meinung und die Freiheit zum Empfang und zur Mitteilung von Nachrichten oder Ideen ohne Eingriffe öffentlicher Behörden und ohne Rücksicht auf Landesgrenzen ein." Art. 10 EMRK schützt also unter anderem die Mitteilung und den Empfang von Tatsachen und Meinungen.[51] In technischer Hinsicht geschützt sind alle Kommunikationsformen,[52] also auch die Nutzung der Telekommunikationsnetze. Es kommt nicht darauf an, ob es sich um private oder um öffentliche, um individuelle oder um Massenkommunikation handelt.[53]

Wie bei Art. 5 GG stellt sich die Frage, ob eine vorbeugende, generelle Aufzeichnung der näheren Umstände der Telekommunikation einen Eingriff in die Meinungsfreiheit darstellt. Der Zweck des Art. 10 EMRK gebietet, dass dem Staat auch eine mittelbare Behinderung der freien Kommunikation als Eingriff zuzurechnen sein muss, wenn die Maßnahme typischerweise und vorhersehbar den Austausch von Meinungen und Tatsachenbehauptungen beeinträchtigt. Wie gezeigt, ist dies bei einer generellen Vorratsspeicherung von Telekommunikationsdaten der Fall. Eine Behinderung der Kommunikation erfolgt insoweit einerseits durch den Abschreckungseffekt, der mit einer generellen Vorratsdatenspeicherung verbunden ist. Die Einführung einer Vorratsspeicherung von Telekommunikationsdaten stellt damit einen Eingriff in Art. 10 EMRK dar.

---

46 EGMR, Sunday Times-GB (1979), EuGRZ 1979, 386 (389), Abs. 62; EGMR, Silver u.a.-GB (1983), EuGRZ 1984, 147 (152), Abs. 97; EGMR, Foxley-GB (2000),
hudoc.echr.coe.int/Hudoc1doc2/HEJUD/200107/foxley%20-%2033274jv.chb3%20200
62000e.doc, Abs. 43.

47 EGMR, Sunday Times-GB (1979), EuGRZ 1979, 386 (390 und 391), Abs. 65 und 67; EGMR, Leander-S (1987), Publications A116, Abs. 59.

48 EGMR, Silver u.a.-GB (1983), EuGRZ 1984, 147 (151), Abs. 97.

49 Empfehlung des Europäischen Parlaments zu der Strategie zur Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität (2001/2070(COS)) vom 06.09.2001, Dok.-Nr. T5-0452/2001; Ausschuss des Europäischen Parlaments für die Freiheiten und Rechte der Bürger, Justiz und innere Angelegenheiten: Zweiter Bericht betreffend den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, 24.10.2001, Dok.-Nr. A5-0374/2001, Abänderung 4; Artikel-29-Gruppe der EU, Überwachung, 5.

50 Allitsch, CRi 2002, 161 (167).

51 Frowein/Peukert-Frowein, Art. 10, Rn. 5; Kugelmann, EuGRZ 2003, 16 (20) m.w.N.

52 Frowein/Peukert-Frowein, Art. 10, Rn. 5; Kugelmann, EuGRZ 2003, 16 (19).

53 Vgl. Frowein/Peukert-Frowein, Art. 10, Rn. 15 ff.

Nach Art. 10 Abs. 2 EMRK kann die Ausübung der in Art. 10 Abs. 1 EMRK genannten Freiheiten eingeschränkt werden, und zwar unter anderem im Interesse der öffentlichen Sicherheit, der Verbrechensverhütung und des Schutzes der Rechte anderer. Hierbei gelten allerdings dieselben einschränkenden Voraussetzungen wie bei Eingriffen in Art. 8 EMRK[54], insbesondere das Verhältnismäßigkeitsprinzip. Wie an anderer Stelle zu Art. 5 GG gezeigt,[55] stehen die mit einer Vorratsspeicherung von Telekommunikationsdaten einher gehenden Einbußen für die freie Kommunikation in der Gesellschaft in einem deutlichen Missverhältnis zu den Vorteilen einer solchen Maßnahme. Eine generelle Vorratsspeicherung von Telekommunikationsdaten ist daher mit Art. 10 EMRK unvereinbar.

Soweit sich der Anwendungsbereich des Art. 10 EMRK mit dem des Art. 8 EMRK überschneidet, fragt es sich, ob ein Spezialitätsverhältnis anzunehmen ist oder ob beide Normen nebeneinander anzuwenden sind.[56] Wie bei den Grundrechten des Grundgesetzes[57] ist darauf abzustellen, dass beide Grundrechte verschiedene Schutzrichtungen haben und daher nebeneinander anwendbar sein müssen. Dies bedeutet im Ergebnis, dass sich die Anforderungen beider Grundrechte kumulieren.

1.4.1.3 Schwere der Fehler

Die vorbenannten Rechtsverletzungen stellen besonders schwere Fehler im Sinne der Rechtsprechung des Europäischen Gerichtshofs dar.

Wenn die Europäische Gemeinschaft einen Rechtsakt auf einem Gebiet erlässt, für das sie überhaupt nicht zuständig ist, also außerhalb ihrer begrenzten Einzelermächtigungen handelt, so liegt ein besonders schwerer Verstoß gegen die Gründungsverträge als Grundlage der Europäischen Gemeinschaft vor.

Wenn ein Rechtsakt der Europäischen Gemeinschaft mehrere Gemeinschaftsgrundrechte verletzt, weil er grob unverhältnismäßig ist, so liegt ebenfalls ein besonders schwerer Verstoß gegen primäres Gemeinschaftsrecht vor. Die Vorratsdatenspeicherung verkehrt das Regelungssystem der Grundrechte in ihr Gegenteil. Den Grundrechten zufolge ist das geschützte Verhalten grundsätzlich frei, und Einschränkungen sind nur dann und nur insoweit zulässig, wie dies tatsächlich erforderlich ist. Die Vorratsdatenspeicherung demgegenüber erklärt den Eingriff unabhängig von seiner Erforderlichkeit zum Regelfall und stellt so die Grundrechtsordnung auf den Kopf.

1.4.1.4 Offensichtlichkeit der Fehler

Die Verstöße sind auch offensichtlich.

Dass der Richtlinie 2006/24/EG eine Rechtsgrundlage fehlt und die EG außerhalb ihrer Kompetenz gehandelt hat, ergibt sich ohne Weiteres und evident aus dem Urteil des Europäischen Gerichtshofs zur Fluggastdatenübermittlung in die USA.[58] Die dortigen Erwägungen sind ohne Weiteres auf die Vorratsdatenspeicherung übertragbar. Die fehlende Rechtsgrundlage steht der Richtlinie 2006/24/EG „auf die Stirn geschrieben".

Auch der Verstoß gegen die vorbenannten Gemeinschaftsgrundrechte liegt auf der Hand. Der Europäische Gerichtshof für Menschenrechte hat staatliche Eingriffe in die Vertraulichkeit der Telekommunikation stets nur im Einzelfall zugelassen. Dass eine rein vorsorgliche Protokollierung

54 Seiten 7-10.
55 Breyer, Vorratsspeicherung (2005), 313 ff.
56 Zur Diskussion Kugelmann, EuGRZ 2003, 16 (20) m.w.N.
57 Breyer, Vorratsspeicherung (2005), 306 f.
58 EuGH, Urteil vom 30.05.2006, Az. C-317/04 und C-318/04.

des Telekommunikationsverhaltens aller Europäer in einer demokratischen Gesellschaft nicht erforderlich und verhältnismäßig ist, ist evident.

1.4.2 Fehlende Umsetzungspflicht nach Völkerrecht

Zur Umsetzung der Richtlinie 2006/24/EG wäre Deutschland auch dann nicht verpflichtet oder berechtigt, wenn man ihre Inexistenz im Sinne des Europarechts nicht annähme. Normen des sekundären Gemeinschaftsrechts, die gegen primäres Gemeinschaftsrecht verstoßen, sind vom deutschen Zustimmungsgesetz zum EG-Vertrag nämlich nicht gedeckt,[59] seien sie inexistent oder nicht. Die mit der Umsetzung befassten Staatsorgane sind aus verfassungsrechtlichen Gründen gehindert, diese Rechtsakte in Deutschland anzuwenden,[60] etwa durch Umsetzung einer Richtlinie. Die Reichweite des deutschen Zustimmungsgesetzes ist eine Frage des deutschen Rechts. Dementsprechend entscheidet letztverbindlich nicht der Europäische Gerichtshof, sondern das Bundesverfassungsgericht darüber, ob sich EG-Rechtsakte in den Grenzen der ihnen eingeräumten Hoheitsrechte halten oder aus ihnen ausbrechen.[61]

Dass die Richtlinie 2006/24/EG formell wie materiell gegen das primäre Gemeinschaftsrecht und damit gegen den EG-Vertrag verstößt, ist bereits dargelegt worden.[62] Unabhängig davon, wie das Europarecht bzw. der Europäische Gerichtshof die Frage der Umsetzungspflicht beurteilt, ist Deutschland völkerrechtlich zur Umsetzung der Richtlinie 2006/24/EG nicht verpflichtet. Würden europäische Organe eine Umsetzungspflicht für einen Rechtsakt annehmen, der vom Zustimmungsgesetz nicht gedeckt ist, so handelten sie selbst außerhalb des Zustimmungsgesetzes.

1.4.3 Zulässigkeit trotz Umsetzungspflicht

Selbst wenn man auch nach Völkerrecht eine Umsetzungspflicht annähme, geböte der effektive Rechtsschutz die Zulassung der vorliegenden Beschwerde, und zwar zum Zweck Vorlage der Frage der Wirksamkeit der Richtlinie 2006/24/EG an den Europäischen Gerichtshof. Außer der Verfassungsbeschwerde steht den Beschwerdeführern keine andere wirksame Möglichkeit zur Verfügung, Rechtsschutz gegen die Vorratsspeicherung ihrer Telekommunikationsdaten zu erlangen. Eine Nichtigkeitsklage gegen die Richtlinie 2006/24/EG können sie nicht erheben, weil sie von der Richtlinie nicht unmittelbar betroffen sind. Die von Irland eingereichte Nichtigkeitsklage hat die Frage der Grundrechtsverletzung nicht zum Gegenstand. Fachgerichtlicher Rechtsschutz wäre nicht wirksam. Ein deutsches Fachgericht könnte die Frage der Verfassungsmäßigkeit der angefochtenen Normen ebenfalls nur dem Bundesverfassungsgericht vorlegen; dieser Umweg ist wegen der Dringlichkeit und gesamtgesellschaftlichen Bedeutung der Angelegenheit nicht zumutbar.

1.4.4 Vorlage an den Europäischen Gerichtshof

Sollte sich das Gericht aufgrund der Richtlinie 2006/24/EG gehindert sehen, der Verfassungsbeschwerde stattzugeben, wird die Vorlage an den Europäischen Gerichtshof beantragt zur Entscheidung über die Wirksamkeit der Richtlinie in formeller und materieller Hinsicht. Die anhängige Nichtigkeitsklage (Az. C-301/06) macht die Vorlage nicht entbehrlich: Erstens kann Irland seine Klage jederzeit zurückziehen. Zweitens greift die Klage Irlands nur die formelle Rechtmäßigkeit der Richtlinie an, während gerade der Verstoß gegen die Gemeinschaftsgrundrechte die Beschwerdeführer belastet. Bei der Entscheidung über eine Nichtigkeitsklage berücksichtigt der Europäische Gerichtshof andere als die gerügten Nichtigkeitsgründe nur ausnahmsweise. Es besteht die Gefahr, dass der Europäische Gerichtshof die Richtlinie 2006/24/EG aus formellen

59 BVerfGE 89, 155 (188).
60 BVerfGE 89, 155 (188).
61 BVerfGE 89, 155 (188).
62 Seite 4 ff.

Gründen verwirft, sodann aber ein inhaltsgleicher EU-Rahmenbeschluss gefasst wird, der ebenso grundrechtswidrig ist. Auch um dies zu verhindern, ist es erforderlich, die Frage der Vereinbarkeit der Richtlinie mit den Gemeinschaftsgrundrechten dem Europäischen Gerichtshof vorzulegen.

Der Antrag auf Vorlage des Verfahrens an den Europäischen Gerichtshof gilt nur für den Fall, dass das Bundesverfassungsgericht die Richtlinie nicht bereits selbst in Anwendung der acte claire-Doktrin verwirft. Die Voraussetzungen dieser Doktrin sind gegeben, weil die Rechtswidrigkeit der Richtlinie offensichtlich und die maßgeblichen Fragen durch den Europäischen Gerichtshof bereits geklärt sind. Insoweit wird auf die obigen Ausführungen verwiesen.

Da die Vereinbarkeit mit der Richtlinie 2006/24/EG nur für die Beurteilung des § 95 Abs. 3 TKG eine Rolle spielt, wird im Fall einer Vorlage an den Europäischen Gerichtshof beantragt, über die übrige Verfassungsbeschwerde durch Teilurteil zu entscheiden.

2 Begründetheit der Verfassungsbeschwerde

2.1 Art. 10 GG

Dass das Fernmeldegeheimnis auch vor der Erhebung und Verwendung von Telekommunikations-Bestandsdaten schützt, erläutert die Beschwerdeschrift ausführlich.[63] Es gibt keinen Grund, weshalb das Fernmeldegeheimnis auf Inhalt und Umstände einzelner Kommunikationsvorgänge beschränkt sein sollte.

Den engen Bezug zur Telekommunikation verdeutlichen die vom Bevollmächtigten der Bundesregierung angeführten Fallbeispiele. Die Abfrage von Bestandsdaten anhand von bei Ermittlungen vorgefundenen Rufnummern gibt Aufschluss über eine Telekommunikationsbeziehung zwischen dem Beschuldigtem und dem Nummerninhaber und erlaubt die Annahme, dass die beiden Personen in der Vergangenheit miteinander telefoniert haben. Die Abfrage von Rufnummern, die durch Maßnahmen der Telekommunikationsüberwachung oder durch Verkehrsdatenauskünfte erlangt worden sind, vertieft den durch diese Maßnahmen erfolgten Eingriff in Art. 10 GG, weil die Bestandsdatenauskunft weitere Umstände der einzelnen Telekommunikationsvorgänge aufdeckt (Wie lauten die Namen der Kommunizierenden?).

Der Bevollmächtigte der Bundesregierung hält der Anwendbarkeit des Fernmeldegeheimnisses entgegen, die Beschlagnahme eines Schlüssels sei auch kein Eingriff in Art. 13 GG. Dieses Argument geht jedoch schon deswegen fehl, weil keineswegs geklärt ist, ob die Erlangung eines Wohnungsschlüssels nicht bereits einen Eingriff in die Unverletzlichkeit der Wohnung darstellt. Mithilfe eines Wohnungsschlüssels kann der Staat die Wohnung jederzeit öffnen. Abgesehen hiervon ist ein Wohnungsschlüssel allenfalls dann mit Bestandsdaten vergleichbar, wenn ihre Abfrage zur Vorbereitung einer Telekommunikationsüberwachungsmaßnahme erfolgt. Dies ist aber nach Abgaben des Bevollmächtigten der Bundesregierung eher selten der Fall.

Auch § 113 Abs. 1 S. 3 TKG[64] ändert nichts an dem Eingriff in Art. 10 GG. § 113 Abs. 1 S. 3 TKG zeigt lediglich, dass der Gesetzgeber – in Übereinstimmung mit der bislang vorherrschenden Meinung – fälschlich von einem zu engen Schutzbereich des Fernmeldegeheimnisses ausgegangen ist.

63 Beschwerdeschrift, 10 ff.

64 „Ein Zugriff auf Daten, die dem Fernmeldegeheimnis unterliegen, ist nur unter den Voraussetzungen der hierfür einschlägigen gesetzlichen Vorschriften zulässig."

Der Bevollmächtigte der Bundesregierung hält der Anwendbarkeit des Fernmeldegeheimnisses weiter entgegen, die Abfrage einer Adresse sei kein Eingriff in das Postgeheimnis, so dass die Abfrage einer Rufnummer auch kein Eingriff in das Fernmeldegeheimnis sein könne. Diese Argumentation verkennt, dass es in beiden Fällen darauf ankommt, bei wem die Kundendaten erhoben werden. Würde eine Anschrift, von welcher die Deutsche Post AG im Zusammenhang mit der Beförderung von Briefen Kenntnis erlangt hat, bei der Post erhoben, so läge durchaus ein Eingriff in das Postgeheimnis vor. Derzeit führt die Post kein Register mit Bestandsdaten derjenigen, die Briefe absenden oder empfangen. Würde sie dies tun, wären die entsprechenden Daten vom Postgeheimnis erfasst.

Der Bevollmächtigte der Bundesregierung beruft sich ferner auf die Entscheidung des Bundesverfassungsgerichts zu § 100i StPO.[65] Im Ausgangspunkt bestätigt die Entscheidung zunächst:

> „*Die Beteiligten sollen weitestgehend so gestellt werden wie sie bei einer Kommunikation unter Anwesenden stünden.*"[66]

Dass bei einer Kommunikation unter Anwesenden keine Bestandsdaten bei einem Kommunikationsmittler anfallen, mit deren Hilfe die Rekonstruktion des Kommunikationsverhaltens ohne Kenntnis der Beteiligten möglich ist, wurde bereits dargelegt. Auch bestätigt die Entscheidung:

> „*Die Nutzung des Kommunikationsmediums soll in allem vertraulich sein (BVerfGE 100, 313 <358>; Beschluss der 3. Kammer des Zweiten Senats des Bundesverfassungsgerichts vom 17. Juni 2006 – 2 BvR 1085/05, 2 BvR 1189/05 -).*"[67]

Soweit die Kammerentscheidung davon ausgeht, die Empfangsbereitschaft eines Mobiltelefons und dessen Positionsmeldungen unterfielen nicht dem Fernmeldegeheimnis, hat sie berechtigte Kritik erfahren.[68] Jede Telekommunikation setzt einen Sender und einen Empfänger voraus. Das Bereithalten einer Empfangsvorrichtung ist notwendiger Bestandteil von Telekommunikation und muss daher dem Schutz des Fernmeldegeheimnisses unterliegen. Der Erste Senat des Bundesverfassungsgerichts hat § 100i StPO zutreffend zu den Maßnahmen der „Überwachung der Telekommunikation zu Zwecken der Strafverfolgung" gezählt.[69]

Vor allem lässt die vom Bevollmächtigten der Bundesregierung gezogene Parallele zu den Entscheidungen über die Sicherstellung von Telekommunikations-Endgeräten[70] und zu § 100i StPO außer Acht, dass sich jene Maßnahmen – anders als die §§ 95, 111 ff. TKG – gerade nicht gegen den Kommunikationsmittler richten.[71] In ihnen hat sich nicht gleichermaßen die spezifische Gefahr der Telekommunikation verwirklicht wie in der Abfrage der Personalien von Kommunikationsteilnehmern bei dem Kommunikationsmittler. Auch bei unmittelbarer Kommunikation lassen sich Gesprächsnotizen sicherstellen und können technische Lokalisierungs- oder Beobachtungsgeräte eingesetzt werden. Das Fernmeldegeheimnis muss hingegen einschlägig sein, wo gerade die notwendige Beteiligung des Kommunikationsmittlers zur erleichterten Gewinnung von Kenntnissen über die Kommunizierenden genutzt, mithin die spezifische Verletzlichkeit von Kommunikationsmedien wie Telefon, Handy, E-Mail und Internet ausgenutzt wird. Eben dies ist der Fall, wenn

65 BVerfG, 2 BvR 1345/03 vom 22.8.2006, NJW 2007, 351.
66 BVerfG, 2 BvR 1345/03 vom 22.8.2006, NJW 2007, 351 (353), Abs. 51.
67 BVerfG, 2 BvR 1345/03 vom 22.8.2006, NJW 2007, 351 (353), Abs. 52; ebenso auch BVerfG, 2 BvR 2099/04 vom 2.3.2006, NJW 2006, 976 (978).
68 Nachbaur, NJW 2007, 335 (336 f.).
69 BVerfGE 113, 348 (372).
70 BVerfG, 2 BvR 2099/04 vom 2.3.2006, NJW 2006, 976.
71 Hierauf abstellend BVerfG, 2 BvR 2099/04 vom 2.3.2006, NJW 2006, 976 (978), Abs. 68 und 73: „Die spezifischen Gefahren der räumlich distanzierten Kommunikation bestehen im Herrschaftsbereich des Empfängers, der eigene Schutzvorkehrungen gegen den ungewollten Datenzugriff treffen kann, nicht."

der Staat die Identität von Nutzern dieser Medien bei dem Anbieter ohne das Wissen der Betroffenen abfragt (§§ 112, 113 TKG), nachdem er für die Erhebung und Vorhaltung der Daten bei dem Anbieter gesorgt hat (§§ 95, 111 TKG).

Die vom Bevollmächtigten der Bundesregierung angeführten Entscheidungen können außerdem nicht losgelöst von der praktischen Bedeutung ihres Gegenstandes gesehen werden. Zu § 100i StPO hat die Kammer etwa ausgeführt:

> „*Angesichts der engen Anwendungsvoraussetzungen und des infolge des erheblichen Aufwands – nach den vom Generalbundesanwalt und dem Bundeskriminalamt mitgeteilten Zahlen – eher seltenen Einsatzes des ‚IMSI-Catchers' ist auch nicht zu befürchten, dass die Regelung des § 100 i StPO die Bereitschaft zur Nutzung von Mobiltelefonen einschränkt.*"[72]

Ähnliches gilt für die Sicherstellung von Telekommunikations-Endgeräten anlässlich von Wohnungsdurchsuchungen.

Anders verhält es sich demgegenüber bei den §§ 95, 111 TKG, die praktisch die gesamte Bevölkerung betreffen, und bei den §§ 112-113 TKG, die jeden Tag tausendfach zur Anwendung kommen. Diese Normen führen dazu, dass eine anonyme Kommunikation kaum noch möglich ist und man sich stets der Nachvollziehbarkeit von Telekommunikation bewusst sein muss. Hierzu genügt es, dass die eigene Rufnummer, E-Mail-Adresse oder IP-Adresse bekannt wird. Durch diese Nachvollziehbarkeit sinkt die Bereitschaft zur Nutzung der Telekommunikation in bestimmten Situationen erheblich. Wer etwa kritische Meinungsäußerungen gegenüber dem Staat oder die Übermittlung staatsbezogener Informationen an die Presse plant, kann sich heute im Grunde nicht mehr seines Telefons oder Mobiltelefons bedienen, ohne Konsequenzen befürchten zu müssen. Will man das Risiko von (auch unberechtigten) Ermittlungsmaßnahmen vermeiden, muss man auf die Post oder den unmittelbaren Kontakt ausweichen oder auf die Kommunikation überhaupt verzichten. Regierungskritische Organisationen sowie der Presse setzen das Medium der Telekommunikation in solchen Situationen teilweise tatsächlich nicht mehr ein.

Der Schutzzweck des Fernmeldegeheimnisses ist im Fall von Bestandsdaten einschlägig. Hierzu hat das Bundesverfassungsgericht ausgeführt:

> „*Der spezielle Schutz des Fernmeldegeheimnisses durch Art. 10 GG schafft einen Ausgleich für den technisch bedingten Verlust an Beherrschbarkeit der Privatsphäre, der durch die Nutzung von Anlagen Dritter zwangsläufig entsteht, und errichtet eine besondere Hürde gegen den vergleichsweise wenig aufwändigen Zugriff auf Kommunikationsdaten, den die Nutzung der Fernmeldetechnik ermöglicht.*"[73]

Bestandsdaten fallen zwangsläufig an, wenn man per Telefon kommunizieren will, und der Zugriff auf diese Daten ist einfach und kostengünstig.

Nach der Rechtsprechung des Bundesverfassungsgerichts soll das Fernmeldegeheimnis gewährleisten, dass die Nutzung der Telekommunikation alles in allem vertraulich möglich ist.[74] Gewährleistet ist dies aber nur, wenn die Möglichkeit anonymer Telekommunikation gegeben ist und der Einzelne vor seiner Identifikation als Teilnehmer an – bekannten oder noch unbekannten – Kommunikationsvorgängen geschützt ist. Bestandsdaten als Daten über die Identität der Teil-

72 BVerfG, 2 BvR 1345/03 vom 22.8.2006, NJW 2007, 351 (356), Abs. 82.

73 BVerfG, 2 BvR 2099/04 vom 2.3.2006, NJW 2006, 976 (979), Abs. 80.

74 BVerfGE 100, 313 (358); BVerfG, 2 BvR 1085/05 vom 17.6.2006, NJW 2006, 3197 (3197), Abs. 4; BVerfG, 2 BvR 1345/03 vom 22.8.2006, NJW 2007, 351 (353), Abs. 52.

nehmer an Telekommunikationsvorgängen müssen deshalb den Schutz des Fernmeldegeheimnisses genießen.

2.2 Nutzen der §§ 95, 111-113 TKG, Fallbeispiele

Der Bevollmächtigte der Bundesregierung greift die Aussage in der Beschwerdeschrift an, eine intensivierte Strafverfolgung lasse keinen verbesserten Rechtsgüterschutz erwarten. Er bleibt aber einen empirischen Beleg des Gegenteils schuldig, während sich die Beschwerdeschrift mit dieser Frage und diesbezüglichen Untersuchungen eingehend auseinandersetzt.[75]

Die Strafrechtspflege wird in der Beschwerdeschrift keineswegs gering geschätzt. Der Nutzen der Strafverfolgung wird lediglich realistisch betrachtet. Die Beschwerdeschrift gesteht der Strafverfolgung eine generalpräventive Wirkung und mithin einen Beitrag zum Rechtsgüterschutz ausdrücklich zu.[76] In Frage steht nicht das Erfordernis einer wirksamen Strafverfolgung überhaupt, sondern die Frage, ob eine weitere Intensivierung der Strafverfolgung Grundrechtseingriffe auf breiter Ebene rechtfertigen kann. Problematisch ist dies insbesondere in Abwesenheit einer konkreten Gefahr und eines konkreten Tatverdachts (§§ 95 Abs. 3 und 4, 111 TKG), wenn sich Maßnahmen also „ins Blaue hinein" gegen vollkommen ungefährliche und unverdächtige Bürger richten, die keinen Anlass für ihre Beobachtung gegeben haben.

Richtig ist, dass das Bundesverfassungsgericht in der Vergangenheit oftmals das Ziel einer verbesserten Strafverfolgung zur Rechtfertigung von Grundrechtseingriffen hat genügen lassen, ohne den Nachweis zu verlangen, dass die jeweilige Norm tatsächlich den Rechtsgüterschutz verbessert, die Kriminalitätsquote senkt oder wenigstens die Aufklärungsquote erhöht. Nachdem der Gesetzgeber in den letzten Jahren aber zunehmend das Maß verliert und – trotz stabiler Kriminalitätslage – zum Zwecke der Gewährleistung möglichst totaler Sicherheit die Grundrechte immer weiter aushöhlt, wird der verfassungsrechtliche Maßstab enger angelegt werden müssen als mitunter in der Vergangenheit. Das Bundesverfassungsgericht trägt dieser Entwicklung durchaus Rechnung, wie etwa das Urteil zur Rasterfahndung mit seinen grundsätzlichen Ausführungen zum Verhältnis von Freiheit und Sicherheit zeigt.

Der Bevollmächtigte der Bundesregierung verkennt, dass die Beschwerde dem Staat nicht das Recht abspricht, zur Abwehr von Gefahren für Leib und Leben sowie zur Aufklärung schwerer Straftaten Bestandsdaten abzufragen, die aus betrieblichen Gründen ohnehin bei Telekommunikationanbietern gespeichert werden müssen. Soweit die §§ 95, 111-113 TKG aber weit hierüber hinaus gehen, ist nicht erkennbar, dass dies dem Rechtsgüterschutz besser dient, etwa die Kriminalitätsquote weiter senkt. Derartiges ist weder im zeitlichen Vergleich innerhalb Deutschlands noch im Vergleich zu ausländischen Staaten, die über entsprechende Vorschriften nicht verfügen, ersichtlich.

Die vom Bevollmächtigten der Bundesregierung einzig angeführten Einzelfälle, in denen die Abfrage von Bestandsdaten den Strafverfolgungsbehörden nützlich war, taugen nicht zur Rechtfertigung der vorbenannten Normen. Eingriffe in die Grundrechte einer Vielzahl unverdächtiger Bürger, im Grunde sogar praktisch der gesamten Bevölkerung, kann der Staat nicht mit Einzelerfolgen rechtfertigen. Erforderlich wäre zumindest der Nachweis eines verbesserten Rechtsgüterschutzes auf ebenso breiter Ebene, etwa einer erheblichen und dauerhaften Senkung der Kriminalitätsrate. Dass die §§ 95, 111 ff. TKG einen allgemein verbesserten Rechtsgüterschutz bewirkten, ist nicht ersichtlich. Außerdem überschreiten die vorbenannten Normen, wie noch zu zeigen sein wird, Verfassungsgrenzen, die unabhängig von dem möglichen Nutzen der Regelungen gelten.

---

75 Beschwerdeschrift, 139 ff.

76 Beschwerdeschrift, 143.

Zu den vom Bevollmächtigten der Bundesregierung angeführten zehn Einzelbeispielen[77] ist noch Folgendes anzumerken:

In den meisten Fällen handelt es sich nicht um schwere Straftaten, also um Straftaten im oberen Kriminalitätsbereich. Dies gilt etwa für die Fälle von Geldfälschung und nicht näher bezeichneter „Agententätigkeit". Hinsichtlich der Drogendelikte ist anzumerken, dass eine Strafverfolgung mit Mitteln, die über die Standardbefugnisse der Strafverfolgungsbehörden hinaus gehen, in diesem Bereich besonders wenig erfolgversprechend ist. Die internationale Praxis zeigt, dass es keinem demokratischen Staat – unabhängig von den Eingriffsbefugnissen seiner Behörden – gelingt, die Verfügbarkeit illegaler Substanzen nennenswert einzuschränken. Wer Drogen kaufen will, kann dies nach wie vor ohne größere Schwierigkeiten tun. Die Preise für Drogen sind in den letzten Jahren sogar noch gesunken. Hier stoßen die Möglichkeiten der Strafverfolgung offenkundig an ihre Grenzen. Ähnlich verhält es sich im Bereich der Kinderpornografie. Das erste angeführte Fallbeispiel unterscheidet nicht hinreichend zwischen der Verschaffung von kinderpornografischen Darstellungen – der Strafrahmen des § 184b StGB verdeutlicht, dass es sich hierbei um keine schwere Straftat handelt – und dem tatsächlichen Missbrauch von Kindern. Auch im Bereich der Kinderpornografie dürfte eine Strafverfolgung über die Standardbefugnisse im Verdachtsfall hinaus nicht geeignet sein, die Verfügbarkeit solchen Materials nennenswert weiter einzudämmen als es mithilfe der traditionellen Ermittlungsbefugnisse möglich ist. Erst recht gilt dies für die Verhinderung von Kindesmissbrauch selbst.

Kaum eines der Fallbeispiele zeigt auf, dass die Datenabfrage konkret den Schutz von Rechtsgütern bewirkt hätte. Eine intensivierte Strafverfolgung kann kein Selbstzweck sein.

Die Fallbeispiele zeigen nur Erfolge. In der Praxis wird die Abfrage von Bestandsdaten dagegen meistens nicht weiter führen. Selbst richterlich angeordnete Telekommunikationsüberwachungsmaßnahmen über Monate hinweg bringt nur in 17% der Fälle den gewünschten Erfolg, also in einem von sechs Fällen.[78] Bei Bestandsdaten wird die Erfolgsquote allenfalls im einstelligen Prozentbereich liegen, weil mit zunehmender Anzahl von Maßnahmen immer ungezielter vorgegangen wird und die Wahrscheinlichkeit von Erfolgen sinkt. Bei mehreren Millionen Abfragen jährlich muss die weitaus überwiegende Mehrzahl erfolglos bleiben.

Selbst wenn die zehn angeführten Straftaten durch Bestandsdaten aufgeklärt worden wären, würde dies in Anbetracht der über 6 Mio. jährlich registrierten Straftaten offensichtlich nicht ins Gewicht fallen und kann dies etwa das faktische Verbot anonymer Telekommunikation für die gesamte Bevölkerung (§ 111 TKG) nicht rechtfertigen.

Die Argumentation des Bevollmächtigten der Bundesregierung leidet darunter, dass Einzelfallbeispiele, eine „langjährige Praxis" und ein „bewährter Nutzen" allesamt keine belastbare Grundlage sind, um einen möglichen Zusatznutzen der §§ 95, 111-113 TKG festzustellen, soweit sie über die Bereitstellung ohnehin anfallender Bestandsdaten zur Verfolgung schwerer Straftaten hinaus gehen. Der Gesetzgeber hat es unterlassen, eine unabhängige wissenschaftliche Untersuchung über die Frage in Auftrag zu geben, ob die vorbenannten Normen den Rechtsgüterschutz fördern, ob also ohne die Normen etwa mehr Straftaten begangen würden als ohne die Vorschriften. Aufgrund der grundrechtlichen Freiheitsvermutung[79] gehen daraus resultierende Zweifel zulasten des eingreifenden Staates.

Zur Rechtfertigung der Identifizierungspflicht des § 111 TKG und der Vorratsspeicherung der §§ 95 Abs. 3, 111 Abs. 1 S. 4 TKG taugen die Fallbeispiele im Übrigen schon deswegen nicht, weil

77 Stellungnahme des Bevollmächtigte der Bundesregierung, 12 f.

78Albrecht/Arnold/Demko/Braun, Rechtswirklichkeit und Effizienz der Telekommunikationsüberwachung, 455 ff.

79 BVerfGE 6, 55 (72); BVerfGE 32, 54 (72); BVerfGE 55, 159 (165).

sie keinerlei Bezug zu den vorbenannten Regelungen aufweisen. Es ist nicht dargelegt, dass die beschriebenen Erfolge erst durch die Identifizierungs- und Vorratsspeicherungspflicht des TKG erzielt werden konnten. Zur Rechtfertigung der §§ 112, 113 TKG sind die Fallbeispiele jedenfalls insoweit von vornherein untauglich, als die §§ 112, 113 TKG weit über den – offenbar einzig praktisch bedeutsamen – Bereich der Strafverfolgung hinaus gehen.

2.3 Sensibilität von Bestandsdaten

Die Ansicht des Bevollmächtigten der Bundesregierung, Bestandsdaten seien von geringer Sensibilität, ist falsch. Die Beschwerdeschrift zeigt auf, dass Bestandsdaten schon für sich genommen sehr aussagekräftig sein und Details über das Privatleben, den Gesundheitszustand usw. wiedergeben können.[80] Entscheidend für die Bewertung der Sensibilität personenbezogener Daten ist nach der Rechtsprechung des Bundesverfassungsgerichts jedoch ihre Nutzbarkeit und Verwendungsmöglichkeiten unter Berücksichtigung der Möglichkeit ihrer Verknüpfung mit anderen Informationen.[81] So lässt erst die Kenntnis von Bestandsdaten den Schluss zu, mit wem jemand in Verbindung steht (z.B. bei Beschlagnahme eines Notizbuchs mit Telefonnummern). Wenn Inhalt oder nähere Umstände eines Kommunikationsvorgangs bekannt sind, erlauben es erst Bestandsdaten, die Beteiligten zu identifizieren.

Bestandsdaten geben insbesondere Aufschluss darüber, wer an bestimmten Telekommunikationsvorgängen beteiligt war, und ermöglichen die Erhebung von Kommunikationsinhalten (durch nachfolgende Überwachungsmaßnahmen oder – bei PINs und Passwörtern – durch unmittelbaren Zugriff). Die Identität der Kommunikationspartner ist integraler Bestandteil der Kommunikation selbst. Ohne die Kenntnis der Identität der Kommunikationsbeteiligten ist die Kenntnis der sonstigen Kommunikationsumstände und des Inhalts der Telekommunikation nutzlos. Dies verdeutlicht die besondere Sensibilität von Bestandsdaten.

Name, Anschrift, Geburtsdatum und Rufnummer mögen bei isolierter Betrachtung zwar wenig aussagekräftig erscheinen. Auch aus einem isolierten Verbindungsdatensatz lässt sich aber wenig ableiten, weil er keine Aussage über die Identität der Gesprächsteilnehmer enthält. Ebenso ist die isolierte Kenntnis eines Gesprächsinhalts wenig aufschlussreich, wenn die Gesprächsteilnehmer ihre Identität nicht offen gelegt haben. Nutzbarkeit und Verwendungsmöglichkeit eines isolierten Gesprächsinhalts oder eines isolierten Verbindungsdatensatzes sind also ebenso gering wie die bloße Kenntnis eines Bestandsdatensatzes.

Es ist deswegen falsch, den Aussagegehalt der einzelnen Datentypen isoliert zu bewerten. Stattdessen muss die Telekommunikationsnutzung als integraler Vorgang betrachtet werden. Das Führen von Telefongesprächen setzt ein Vertragsverhältnis voraus, bei dem regelmäßig Bestandsdaten anfallen. Die Identität der an den einzelnen Gesprächen Beteiligten (Name, Anschrift, Geburtsdatum der Anschlussinhaber) ist integraler Bestandteil der einzelnen Verbindungen. Ebenso wie Bestandsdaten, Verbindungsdaten und Inhalte nur in ihrer Kombination aussagekräftig sind, ist auch die Schutzwürdigkeit dieser Datentypen nur in ihrer Gesamtheit zutreffend erfasst.

Verfehlt ist es deswegen, Bestandsdaten eine geringere Sensibilität als Kommunikationinhalten oder Umständen einzelner Kommunikationsvorgänge zuzumessen. Bestandsdaten müssen als Bestandteil der einzelnen Kommunikationsvorgänge denselben Eingriffsgrenzen unterliegen. In dem Recht anderer Länder ist dies übrigens traditionell der Fall.

80 Beschwerdeschrift, 10 f.
81 BVerfGE 65, 1 (45).

Soweit der Bevollmächtigte der Bundesregierung anführt, Bestandsdaten würden oft ohne Bezug zu konkreten Verbindungen abgefragt, ändert dies an ihrer Schutzwürdigkeit nichts. Findet die Polizei Telefonnummern in einem Notizbuch oder in einem elektronischen Telefonbuch eines Mobiltelefons vor, dann lässt dies regelmäßig den Schluss zu, dass der Besitzer des Telefonbuchs mit den Rufnummerninhabern in Verbindung gestanden hat, auch per Telekommunikation. Kommunizieren Menschen außerhalb der Kommunikationsnetze unmittelbar miteinander, fallen solche Kommunikationsspuren nicht an, denn den Aufenthaltsort eines Bekannten braucht man sich nicht aufzuschreiben. Dass Telekommunikation regelmäßig das Aufschreiben oder Abspeichern der Rufnummer der Gegenseite voraussetzt, verdeutlicht erneut die technikbedingt erhöhte Verletzlichkeit distanzierter elektronischer Kommunikation und die entsprechend erhöhte Schutzwürdigkeit von Telekommunikations-Bestandsdaten.

Weiterhin darf nicht vergessen werden, dass der Begriff der Bestandsdaten weit über Name, Anschrift, Geburtsdatum und Rufnummer hinaus geht. Er erfasst sämtliche während des Vertragsverhältnisses angefallenen Kundendaten. Dazu zählen Kontoverbindung, PIN-Kennungen und Passwörter ebenso wie Partner- oder „Family&Friends"-Rufnummern. Mithilfe von PIN-Kennungen kann man auf die in Mobiltelefonen gespeicherten Daten sowie auf Kommunikationsinhalte zugreifen (z.B. elektronische Anrufbeantworter). Mithilfe von Passwörtern kann man die gesamte elektronische Post der Nutzer von E-Mail-Diensten einsehen („Webmail"). Aus Partner- und „Family&Friends"-Rufnummern kann man die kontaktintensivsten sozialen Beziehungen des Teilnehmers ablesen (z.B. zu Vorgesetzten, zu Familienmitgliedern, zum Lebenspartner). Denn bei diesen Tarifen kann der Anschlussinhaber einige von ihm benannte Rufnummern besonders günstig oder sogar kostenlos anwählen. Es liegt auf der Hand, dass hier die Rufnummern derjenigen Personen benannt werden, mit denen man am häufigsten kommuniziert. Da es sich hierbei um eine neue technische Entwicklung handelt – diese Tarife gibt es erst seit Ende der 90er Jahre –, hat der Gesetzgeber die Schutzwürdigkeit von Bestandsdaten unterschätzt, als er Speicherung von und Zugriff auf Bestandsdaten ursprünglich regelte.

Die Menge und Qualität von Bestandsdaten nimmt auch weiterhin zu. So fallen alle „Einstellungen" bei der Benutzung von E-Mail-Diensten im Internet („Webmail") unter den Begriff der Bestandsdaten. Darunter können sich Filterlisten mit erwünschten oder unerwünschten E-Mail-Adressen befinden, die Rückschlüsse auf das Kommunikationsnetzwerk des Nutzers erlauben. Ebenso sind elektronische Adressbücher mit E-Mail-Adressen von Kommunikationspartnern bei den Anbietern von E-Mail-Diensten gespeichert und gehören damit zu den Bestandsdaten. Es handelt sich dabei um kommunikationsspezifische Daten, die sich in anderen Wirtschaftszweigen nicht unter den Kundendaten finden. Auch dies verdeutlicht die besondere Sensibilität von Telekommunikations-Bestandsdaten.

2.4 Vergleiche

Der Bevollmächtigte der Bundesregierung bemüht in seiner Stellungnahme immer wieder Vergleiche der angegriffenen Normen mit anderen Regelungen und Sachverhalten, die zeigen sollen, dass die §§ 95, 111-113 TKG keine Besonderheit und nichts Ungewöhnliches seien, vielmehr Vergleichbares schon immer praktiziert worden sei und auch in anderen Bereichen praktiziert werde. Abgesehen davon, dass eine Verwaltungspraxis sowie Tätigkeiten des einfachen Gesetzgebers von vornherein nicht Maßstab einer verfassungsrechtlichen Prüfung sein können, sind die angeführten Vergleiche sachlich verfehlt.

2.4.1 Konto-Stammdaten

Befugnisse zur Übermittlung der Stammdaten von Bankkonten (§§ 93 AO, 24c KWG) können schon deswegen nicht zum Vergleich herangezogen werden, weil ihre Verfassungsmäßigkeit bislang ungeklärt ist. Das Bundesverfassungsgericht hat entschieden, im anhängigen Beschwer-

deverfahren werde „unter anderem zu prüfen sein, ob die angegriffenen Regelungen den Anforderungen der Gesetzesbestimmtheit und der Verhältnismäßigkeit gerecht werden."[82]

§ 24c KWG lässt die Übermittlung von Stammdaten auch nicht so uferlos zu wie die §§ 112, 113 TKG. Eine Übermittlung zur Gefahrenabwehr oder zur Verfolgung von Ordnungswidrigkeiten ist etwa nicht vorgesehen. Für Nachrichtendienste besteht nur eine Erhebungsbefugnis, nicht aber eine Auskunftspflicht (§ 8a BVerfSchG).

Zudem gewährleisten Bargeld und die Möglichkeit von Bareinzahlungen einen anonymen Zahlungsverkehr zumindest im Alltag, während § 111 TKG eine anonyme Telekommunikation selbst durch Privatpersonen in weiten Bereichen unmöglich macht. Die Möglichkeit eines anonymen unbaren Zahlungsverkehrs erscheint in einer demokratischen Gesellschaft ohnehin weniger wichtig als die Gewährleistung einer freien und unbefangenen Information und Kommunikation der Bürger. Nur die freie Information und Kommunikation der Bürger ist Grundvoraussetzung für die Ausübung mehrerer Grundrechte des Grundgesetzes (z.B. Art. 5, Art. 8 GG) und für die unbefangene Mitwirkung der Bürger in einem demokratischen Staat.

2.4.2 Luftfahrtunternehmen, Post

Dass die Nachrichtendienste von Luftfahrtunternehmen im Einzelfall Auskunft verlangen können, ist mit den §§ 95, 111 ff. TKG nicht vergleichbar. Es gibt für Luftfahrtunternehmen keine Identifizierungspflicht, kein automatisiertes Abrufverfahren für eine Vielzahl von Behörden und keine Pflicht zur Vorratsdatenspeicherung.

Dass staatliche Behörden teilweise Auskunftsansprüche gegen die Post haben, ändert nichts daran, dass anonyme Postfächer angeboten werden dürfen und dadurch eine vertrauliche Kommunikation ermöglicht werden darf. Auch im Bereich der Post gibt es keine Identifizierungspflicht, kein automatisiertes Abrufverfahren für eine Vielzahl von Behörden und keine Pflicht zur Vorratsdatenspeicherung.

2.4.3 Vorfeldbefugnisse der Polizei

Der Vergleich mit polizeilichen Befugnissen zum anlasslosen Anhalten, Kontrollieren und Durchsuchen von Personen geht fehl, weil von diesen Maßnahmen in der Praxis nur einzelfallbezogen Gebrauch gemacht wird, während die §§ 95, 111-113 TKG quasi die gesamte Bevölkerung permanent treffen, insbesondere die Regelungen über die Vorratsdatenerhebung und -speicherung. Auch ist die Streubreite der §§ 112, 113 TKG ungleich größer.

Im Übrigen ist die Verfassungsmäßigkeit der vorbenannten polizeilichen Regelungen höchst fragwürdig;[83] das Bundesverfassungsgericht hat hierüber jedenfalls bislang noch nicht zu entscheiden gehabt.

Die §§ 112, 113 TKG sind auch nicht mit „allgemeinen Auskunftsrechten" zur Gefahrenabwehr oder Strafverfolgung vergleichbar. Sie unterscheiden sich vielmehr dadurch, dass Privatunternehmen verpflichtet werden, Auskunft über Daten zu erteilen, die – zumal in Verbindung mit anderen Informationen – Rückschlüsse auf das Informations- und Kommunikationsverhalten der Betroffenen ermöglichen.

82 BVerfG, 1 BvR 2357/04 vom 22.3.2005, NJW 2005, 1179 (1180), Abs. 44.
83 Vgl. MVVerfG, LKV 2000, 149.

2.4.4 Zeugenpflicht, Beschlagnahme

Der Vergleich mit der Zeugenpflicht geht fehl, weil Zeugen nur über ihre Wahrnehmung zu berichten haben, nicht aber über bei ihnen gespeicherte Daten.[84]

Der Verweis auf die strafprozessuale Beschlagnahmebefugnis verkennt, dass eine Beschlagnahme nur zur Aufklärung von Straftaten zulässig ist und nicht zu all den Zwecken der §§ 112, 113 TKG. Außerdem würde eine Beschlagnahme von Bestandsdaten nur in einem Bruchteil der Fälle erfolgen, in denen von der automatisierten, regelmäßig kostenlosen Abfrage von Bestandsdaten Gebrauch gemacht wird. Die §§ 112, 113 TKG stellen ein millionenfaches Standardverfahren dar.

2.4.5 Einwohnermeldedaten / Anschrift

Der Vergleich der Rufnummer mit der Wohnanschrift einer Person zieht sich durch die gesamte Stellungnahme des Bevollmächtigten der Bundesregierung. Der Bevollmächtigte der Bundesregierung argumentiert, ebenso wie die Wohnanschrift stelle die Rufnummer die Erreichbarkeit des Betroffenen sicher und sei als „grundlegendes Ordnungsmerkmal" oder „Basisdatum" einer Person anzusehen. Aus Regelungen über die Anmeldepflicht und die Übermittlung von Meldedaten folgert der Bevollmächtigte der Bundesregierung dann, dass entsprechendes auch für Telekommunikations-Bestandsdaten zulässig sein müsse.

Diese Folgerung ist schon deshalb verfehlt, weil die Verfassungsmäßigkeit der Einwohnermelderegelungen ungeklärt ist. Deswegen kann auch die Ausgestaltung der Verarbeitungsregelungen nicht zur Rechtfertigung der vorliegend angegriffenen Normen heran gezogen werden (z.B. fehlende Eingriffsschwelle, automatisierter Abruf, fehlende Benachrichtigungspflicht). Es ist bekannt, dass Einwohnermeldedaten während des Dritten Reiches zu Massenverbrechen missbraucht worden sind. Nicht nur deshalb stellt sich die Frage, ob eine Meldepflicht erforderlich ist oder ob es – wie in vielen ausländischen Staaten ohne Probleme praktiziert – genügt, dass jede Behörde die zur Erfüllung ihrer jeweiligen Aufgaben aktuell erforderlichen Daten speichert. Übrigens plant die Bundesregierung derzeit die Einführung eines zentralen Bundeseinwohnermelderegisters.[85] Die §§ 111, 112 TKG nehmen dies praktisch vorweg.

Der Vergleich mit den Einwohnermelderegistern geht schon im Ansatz fehl. Zweck der Einwohnermelderegister ist es, die Erreichbarkeit des Bürgers für den Staat zu gewährleisten. Das Ziel der §§ 95, 111 ff. TKG ist hingegen die potenzielle Erleichterung der Strafverfolgung und der Gefahrenabwehr. Zweck dieser Regelungen ist also gerade nicht, die telefonische Erreichbarkeit der Bürger zu gewährleisten (obwohl die Nutzung der §§ 112, 113 TKG als Telefonbuch oder Adressregister nach dem Wortlaut der Regelungen in der Tat zulässig wäre). Sollen die Normen aber nicht die Erreichbarkeit der Anschlussinhaber gewährleisten, so kann sich der Gesetzgeber auch nicht darauf berufen, Rufnummern hätten eben diese Funktion. Nach dem Vortrag des Bevollmächtigten des Bundesregierung werden die §§ 112, 113 TKG angeblich auch in der Praxis nicht dazu benutzt, Personen telefonisch zu erreichen.

2.4.6 Kfz-Register

Der Bevollmächtigte der Bundesregierung vergleicht Bestandsdaten weiterhin mit den im Kraftfahrzeugregister gespeicherten Halterdaten (§§ 31 ff. StVG). Auch in diesem Bereich besteht eine Identifizierungspflicht (§ 34 Abs. 1 StVG) mit Übermittlungsregelungen (§§ 35 ff. StVG) einschließlich eines automatisierten Abrufverfahrens.

84 Ausführlich Breyer, Vorratsspeicherung (2005), 104 f.

85 Ramelsberger, Ein Zentralregister für alle Deutschen, Süddeutsche Zeitung vom 17.01.2007.

Zu beachten ist allerdings erstens, dass von der Verfassungsmäßigkeit der §§ 31 ff. StVG nicht ohne Weiteres ausgegangen werden kann, da eine verfassungsgerichtliche Entscheidung hierzu bislang nicht vorliegt.

Zweitens sind die beiden Regelungskomplexe nicht miteinander vergleichbar. Die im Kfz-Register gespeicherten Daten werden unter anderem zum Zweck der Besteuerung von Fahrzeughaltern erhoben (§ 32 Abs. 1 Nr. 3 StVG); es besteht insoweit ein ständiger Bedarf nach diesen Daten. Anders als nach den §§ 95, 111 TKG erfolgt keine Erhebung und Speicherung überflüssiger Daten alleine für den Fall, dass die Daten einmal zur Strafverfolgung oder sonstigen staatlichen Aufgabenwahrnehmung nützlich sein könnten.

Drittens ist das Kfz-Register auch vor dem Hintergrund zu sehen, dass der Straßenverkehr jährlich Tausende von Menschenleben kostet, also Leib und Leben konkret gefährdet (vgl. § 32 Abs. 2 StVG). Mittels Telekommunikation ist dagegen noch niemand in seiner körperlichen Unversehrtheit verletzt worden.

2.4.7 Ergebnis

Die §§ 95 Abs. 3 und 4, 111 TKG sind mithin aus mehreren Gründen mit Einwohnermelde- oder Fahrzeugregistern nicht vergleichbar: Jenes sind öffentliche Register, auf welche Strafverfolgungsbehörden und Gefahrenabwehrbehörden im Einzelfall Zugriff haben. Das TKG begründet dagegen

- private Register,
- deren Daten nicht ohnehin zu einem bestimmten Zweck gespeichert sind, sondern die besonders erhoben werden müssen für den Fall, dass sie dem Staat einmal von Nutzen sein könnten,
- deren Daten Aufschluss über das Kommunikationsverhalten geben,
- auf die nicht nur Polizei und Staatsanwaltschaft sondern eine Vielzahl anderer Behörden im automatisierten Verfahren Zugriff haben.

Der Vergleich mit der Übermittlung von Einwohnermelde- oder Fahrzeugregisterdaten verkennt insbesondere die besondere Sensibilität von Telekommunikations-Bestandsdaten. Nur im Telekommunikations- und Internetbereich werden standardmäßig Daten über das Verhalten der Betroffenen aufgezeichnet (z.B. Verbindungsdaten, Internet-Serverprotokolle über das Surfverhalten). Diese Protokollierung bringt die besondere Gefahr mit sich, dass die Protokolle mit Bestandsdaten kombiniert und dadurch das Informations- und Kommunikationsverhalten der Nutzer personenbezogen und minuziös nachvollzogen werden kann. Das Verhalten von Einwohnern und von Fahrzeugführern wird demgegenüber – bislang – nicht protokolliert. Die Nutzbarkeit und Verwendungsmöglichkeit letzterer Daten ist daher sehr viel geringer.

Die Bedeutung von Bestandsdaten und das Bedürfnis nach anonymer Kommunikation erhöht sich weiter in Anbetracht der Tatsache, dass inzwischen selbst die Vorratsspeicherung von Verkehrsdaten (Verbindungsdaten, Standortdaten, Internet-Nutzungskennung) in der EG-Richtlinie 2006/24/EG vorgesehen und von der Bundesregierung auch für Deutschland geplant ist. Im Fall einer Vorratsspeicherung von Verkehrsdaten ist die anonyme Nutzung von Mobiltelefon oder E-Mail das einzige Mittel, das Kommunikationsbeziehungen noch einigermaßen vor einer Kenntnisnahme des Staates oder Dritter schützen kann. Bekanntlich müssen Menschen in vielen Situationen Nachteile infolge einer staatlichen Kenntnisnahme ihres Kommunikationsverhaltens befürchten, obwohl ihr Verhalten vollkommen legal und in einer demokratischen Gesellschaft wichtig ist (z.B. Aktivitäten staatskritischer Organisationen wie Demonstrationen, Presseinformanten).

2.5 Art. 3 GG

Der Bevollmächtigte der Bundesregierung moniert, die Ausführungen in der Beschwerdeschrift zur Verletzung des Gleichbehandlungsgebots beträfen nur Verkehrsdaten. Der Grund hierfür liegt darin, dass ursprünglich mehrere Vorschriften über Verkehrsdaten Beschwerdegegenstand gewesen sind. Die diesbezüglichen Ausführungen gelten aber entsprechend für Bestandsdaten. Denn die weitgehende Erhebung, Speicherung und Beauskunftung von Daten über Telekommunikationsteilnehmer ist im Vergleich zu Kunden anderer Unternehmen nicht sachlich zu rechtfertigen. Jedenfalls existiert kein sachlicher Grund von solcher Art und solchem Gewicht, dass er es rechtfertigen würde, die Identität der Nutzer von Telekommunikation derart weitgehend erheben, vorratsspeichern und beauskunften zu lassen, wie es das TKG vorsieht. Vergleichbares ist bei räumlich-unmittelbarer Kommunikation, postalischer Kommunikation und der Inanspruchnahme sonstiger Leistungen nicht vorgeschrieben. Stellt man sich in diesen Bereichen eine zwangsweise Erhebung, Speicherung und Beauskunftung der Identität der Beteiligten vor, so wird deutlich, dass die §§ 95, 111 ff. TKG eines Überwachungsstaats wie der DDR würdig sind, nicht aber eines freiheitlichen Rechtsstaates.

2.6 § 111 TKG (Identifizierungspflicht)

§ 111 Abs. 1 TKG zufolge setzt die Nutzung eines Telefon- oder Handyanschlusses sowie künftig auch eines E-Mail-Postfachs[86] zwingend die Angabe von Name, Anschrift und Geburtsdatum voraus, und zwar selbst dann, wenn die Erhebung von Kundendaten zu betrieblichen Zwecken nicht erforderlich ist (z.B. bei vorausbezahlten Mobiltelefonkarten oder kostenlosen E-Mail-Diensten).

Das Grundgesetz lässt solche Grundrechtseingriffe nur aus überwiegenden Interessen der Allgemeinheit zu. Hiervon kann bei der Identifizierungspflicht für Telefon, Handy und E-Mail keine Rede sein. Wer eine politische Demonstration vorbereitet oder gegenüber der Presse vertraulich Missstände aufdecken will, hat ein berechtigtes Interesse an der Nutzung einer anonymen Mobiltelefonkarte. Es ist unverhältnismäßig, die anonyme Inanspruchnahme der Telekommunikation für die gesamte Bevölkerung zu verbieten, obwohl diese Möglichkeit nur in einem Bruchteil aller Fälle missbraucht wird. Wenn Menschen aus Furcht vor sozialer Stigmatisierung, vor Nachteilen am Arbeitsplatz, vor Strafverfolgungsmaßnahmen oder vor geheimdienstlicher Beobachtung auf Kommunikation mit anderen verzichten, schadet dies nicht nur ihnen, sondern der demokratischen Gesellschaft insgesamt. Die demokratische Gemeinschaft ist darauf angewiesen, dass die Bürgerinnen und Bürger unbefangen von ihren Grundrechten Gebrauch machen. Die vielfältigen Möglichkeiten zur Umgehung der Bestandsdatenerhebung, angefangen mit dem Tausch vorausbezahlter Telefonkarten, lassen den vermeintlichen Nutzen der Regelung weiter hinter den mit ihr verbundenen Schaden zurücktreten. Das Gewicht des Eingriffs vergrößert sich ferner durch die ausufernden gesetzlichen Zugriffsrechte (§§ 112, 113 TKG), zu denen in Kürze noch ein zivilrechtlicher Auskunftsanspruch wegen Urheberrechtsverletzungen hinzu treten soll.[87]

2.6.1 Aktuell geplante Änderungen

Es ist darauf hinzuweisen, dass der „Referentenentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG" vom November 2006 eine weitere Ausdehnung der Identifizierungspflicht des § 111 TKG vorsieht. So sollen künftig auch Anbieter von E-Mail-Postfächern von § 111 TKG erfasst werden, obgleich auch hier fiktive Daten angegeben oder ausländische Anbieter ohne Identifizierungspflicht genutzt werden können. Die Richtlinie 2006/24/EG schreibt

86 Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG.

87 Entwurf eines Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums.

eine Identifizierungspflicht für E-Mail-Konten nicht vor, sondern betrifft nur ohnehin zu betrieblichen Zwecken erhobene Bestandsdaten.

Die erneute Ausdehnung des § 111 TKG, vor allem aber die beabsichtigte Einführung einer allgemeinen Vorratsspeicherung von Verkehrsdaten verdeutlicht (§ 110a TKG-E), dass bei Zulassung einer Erhebung oder Speicherung personenbezogener Daten auf Vorrat „alle Dämme brechen" würden. Die Vorratsspeicherung von Bewegungen mit nur empfangsbereitem Handy, die Protokollierung von Internetnutzungsdaten und die Aufbewahrung von Inhaltsdaten (z.B. Betreffzeilen, SMS) auf Vorrat ist absehbar. Aber auch in anderen Bereichen würde das Beispiel der Vorratsdatenspeicherung Schule machen. Die verdachtsunabhängige Vorratsspeicherung von Flugreisen und Nahverkehrsfahrten, von Fahrzeugbewegungen auf Autobahnen, von Aufzeichnungen privater Überwachungskameras, von Einkäufen in Geschäften und Ausleihvorgängen in Büchereien sind Beispiele einer Vorratsspeicherung, die im Ausland geplant oder bereits realisiert sind. Ein Papier des Bundesinnenministeriums aus dem Jahr 2006 mit dem Titel „E-Government 2.0" sieht bereits vor, eine offizielle elektronische E-Mail-/Meldeadresse für jeden Bürger solle „die nicht-anonyme [...] Kommunikation zum Normalfall" machen.

Spektakuläre Straftaten, die zuvor Undenkbares als wünschenswert erscheinen lassen, werden auch in Deutschland immer wieder neue Forderungen laut werden lassen. Die vorsorgliche Erhebung und Protokollierung personenbezogener Daten ist für den Staat stets und in allen Bereichen nützlich. Aus jedem personenbezogenen Datum können sich im Einzelfall einmal Schlüsse bezüglich einer begangenen oder geplanten schweren Straftat ergeben. Das gesamte Datenschutzrecht beruht indes auf dem Gedanken, dass nicht bereits die bloße Möglichkeit, dass ein Datum irgendwann in der Zukunft einmal gebraucht werden könnte, dessen Speicherung rechtfertigt, weil ansonsten sämtliche personenbezogene Daten unbegrenzt auf Vorrat gespeichert werden dürften. Dies aber wäre eine unverhältnismäßige und unangemessene Beeinträchtigung des Persönlichkeitsrechts der Betroffenen, denen aus der Sammlung personenbezogener Daten schwere Nachteile entstehen können.

Es ist daher zum Schutz des freiheitlichen Rechtsstaats des Grundgesetzes unabdingbar, das verfassungsrechtliche Verbot der Erhebung und Speicherung personenbezogener Daten auf Vorrat in allen Bereichen zu verteidigen und durchzusetzen. Dieser Verfassungsgrundsatz muss eine rote Linie zum Schutz unbescholtener Bürger und der offenen Gesellschaft insgesamt darstellen, die der Staat in keinem Bereich überschreiten darf, auch nicht im vorliegenden Zusammenhang.

2.6.2 Konsequenzen aus dem Urteil zur Rasterfahndung

Mit Urteil vom 04.04.2006 hat das Bundesverfassungsgericht ausdrücklich ausgesprochen:

> *„Die Anforderungen an den Wahrscheinlichkeitsgrad und die Tatsachenbasis der Prognose dürfen allerdings nicht beliebig herabgesenkt werden, sondern müssen auch in angemessenem Verhältnis zur Art und Schwere der Grundrechtsbeeinträchtigung und zur Aussicht auf den Erfolg des beabsichtigten Rechtsgüterschutzes stehen. Selbst bei höchstem Gewicht der drohenden Rechtsgutbeeinträchtigung kann auf das Erfordernis einer hinreichenden Wahrscheinlichkeit nicht verzichtet werden."*[88] *„Der Grundsatz der Verhältnismäßigkeit führt dazu, dass der Gesetzgeber intensive Grundrechtseingriffe erst von bestimmten Verdachts- oder Gefahrenstufen an vorsehen darf [...] Verzichtet der Gesetzgeber auf begrenzende Anforderungen an die Wahrscheinlichkeit des Gefahreneintritts sowie an die Nähe der Betroffenen zur abzuwehrenden Bedrohung und*

88 BVerfG, 1 BvR 518/02 vom 04.04.2006, NJW 2006, 1939 (1946), Abs. 136.

sieht er gleichwohl eine Befugnis zu Eingriffen von erheblichem Gewicht vor, genügt dies dem Verfassungsrecht nicht."[89]

§ 111 TKG verzichtet auf jeden Verdachtsgrad und auf jede Nähe der Betroffenen zu einer Gefahr, stellt gleichzeitig aber einen schwerwiegenden Grundrechtseingriff dar, weil er die Grundlage für die personenbezogene Aufdeckung des Telekommunikationsverhaltens schafft. Dies ist mit dem Verfassungsrecht offensichtlich unvereinbar.

Dass die zwangsweise Erhebung und Vorratsspeicherung der Identität aller Telekommunizierenden einen schwerwiegenden Eingriff in deren Grundrechte darstellt, legt bereits die Beschwerdeschrift ausführlich dar.[90] Die Meinungs- und Versammlungsfreiheit ist gefährdet, wo Organisatoren staatskritischer Demonstrationen (z.B. gegen die Globalisierung, gegen Atomkraft oder gegen soziale Probleme) aus Furcht vor staatlichen Repressalien auf die Benutzung von Telekommunikation zur Koordinierung ihrer Aktivitäten verzichten. Die Pressefreiheit ist gefährdet, wo Informanten aus Furcht vor staatlicher Strafverfolgung nicht mehr zur Aufdeckung staatlicher Missstände per Telekommunikation bereit sind. Die Möglichkeit vertraulicher Kommunikation – und zwar auch gegenüber dem Staat vertraulicher Kommunikation – ist in vielen Bereichen konstitutiv für unsere demokratische Gesellschaft. Wo die Telekommunikation als Medium vertraulicher Kommunikation ausfällt, stehen oft keine praktikablen Alternativen zur Verfügung mit der Folge, dass auf den Informationsaustausch insgesamt verzichtet wird. Dies fügt nicht nur den Betroffenen, sondern auch unserem Gemeinwesen insgesamt schweren Schaden zu.

Ebenso wie § 111 TKG widerspricht der Bevollmächtigte der Bundesregierung den vom Bundesverfassungsgericht dargestellten verfassungsrechtlichen Vorgaben. Seine Ansicht, wonach der Staat Informationen überall dort erheben dürfe, wo er sie finden könne, selbst wenn die Betroffenen vollkommen unverdächtig, ungefährlich und unbeteiligt seien,[91] steht in diametralem Gegensatz zu Fernmeldegeheimnis und dem Grundrecht auf informationelle Selbstbestimmung. Diese Rechte garantieren das Recht des Bürgers, in Ruhe gelassen zu werden. Sie statuieren die Privatheit als Grundsatz, während staatlich veranlasste Informationseingriffe die rechtfertigungsbedürftige Ausnahme zu bleiben haben. Damit ist § 111 TKG unvereinbar.

Immerhin machen die diesbezüglichen Ausführungen des Bevollmächtigten der Bundesregierung noch einmal deutlich, welche Konsequenzen es hätte, eine allgemeine Identifizierungs- und Vorratsspeicherungspflicht vor den Grundrechten bestehen zu lassen. Denn dann wären in der Tat, wie der Bevollmächtigte der Bundesregierung bereits heute wahr wähnt,[92] die Kategorien „verdächtig – unverdächtig" und „Nähebeziehung – Unbeteiligter" obsolet. Dann könnte in allen Bereichen des öffentlichen Lebens ein Identifizierungszwang und eine Vorratsspeicherungspflicht eingeführt werden, um die lückenlose staatliche Überwachung der Bürger zu ermöglichen. Ein solcher Staat wäre aber nicht mehr der freiheitliche Rechtsstaat des Grundgesetzes, sondern ein Überwachungsstaat.

2.6.3 Frühere Rechtslage und frühere Praxis

Falsch ist die verharmlosende Formulierung des Bevollmächtigten der Bundesregierung in seiner Stellungnahme, die Norm sei „nichts wesensmäßig Neues". § 111 TKG hat mit dem traditionellem Zugriff auf ohnehin erforderliche Bestandsdaten nichts zu tun, sondern statuiert erstmals eine Pflicht zur Erhebung und Speicherung personenbezogener Daten auf Vorrat. Eine Vorratsdatenerhebung liegt vor, soweit von Anfang an nicht erforderliche Daten der Teilnehmer erhoben werden müssen (z.B. bei kostenlosen oder vorausbezahlten Produkten). Eine Vorratsdatenspeiche-

89 BVerfG, 1 BvR 518/02 vom 04.04.2006, NJW 2006, 1939 (1946), Abs. 137.

90 Beschwerdeschrift, 54.

91 Stellungnahme des Bevollmächtigten der Bundesregierung, 65.

92 Stellungnahme des Bevollmächtigten der Bundesregierung, 65 f. und 91 f.

rung liegt vor, soweit nach Vertragsende nicht mehr erforderliche Daten gleichwohl gespeichert bleiben müssen.

§ 111 TKG ist auch insofern eine Besonderheit als in den meisten ausländischen Staaten nach wie vor vorausbezahlte Mobiltelefonkarten (Prepaidkarten) anonym verkauft werden dürfen. Mit Ausnahme von Frankreich und der Schweiz ist kein Staat mit einer vergleichbaren Identifizierungspflicht bekannt. Auch die Richtlinie 2006/24/EG verzichtet auf eine solche.

Falsch ist ferner die Darstellung, dass § 111 TKG nur eine nach einer Entscheidung des Bundesverwaltungsgerichts entstandene „Lücke" geschlossen habe. Richtig ist, dass es bis zur Einführung des § 111 TKG nie eine Identifizierungspflicht gegeben hat und vorausbezahlte Mobiltelefonkarten auch tatsächlich verbreitet ohne Identifizierung des Käufers verkauft wurden. Erst recht wurden niemals Angaben wie das Geburtsdatum o.ä. erhoben, wie es § 111 TKG vorsieht. Diese Angabe dient besonders offensichtlich einzig der erleichterten staatlichen Überwachung der Bevölkerung.

2.6.4 Nutzen

Die Problematik des § 111 TKG ist nicht auf Prepaidprodukte beschränkt, sondern betrifft alle vorausbezahlten und kostenlosen Dienste. Bei all diesen Diensten eine Identifikation der Kunden nicht erforderlich. Die kostenlose Bereitstellung von Rufnummern wird etwa im Bereich der Internet-Telefonie von verschiedenen Anbietern bereits praktiziert. In Zukunft soll § 111 TKG, wie bereits erwähnt, auch auf E-Mail-Dienste Anwendung finden, die heute verbreitet anonym angeboten werden.

Die Behauptung, Bestandsdaten von Prepaidkunden seien in 90% der Fälle akkurat, wird entschieden bestritten. Als Quelle dieser Behauptung werden einzig nicht näher spezifizierte „Angaben von Sicherheitsbehörden" genannt. Es dürfte sich um die willkürliche Schätzung eines Kriminalbeamten handeln, der einen statistisch validen Überblick nicht haben kann.

In einem Papier des Bundeswirtschaftsministeriums aus dem Jahr 2002 heißt es noch:

> „*Derzeit werden Prepaid-Karten von Straftätern häufig unter Angabe falscher bzw. fiktiver Personalien oder unter dem Namen der Vertriebspartner (Händler) erworben und registriert, oder es werden nicht existente Anschriften angegeben. [...] Außerdem kommt es wegen der zum Teil falschen Angabe von Personalien unbeteiligter Dritter immer wieder zu [...] Ermittlungsmaßnahmen gegen Unschuldige. [...] Regelmäßig kommt es auch zu Schwierigkeiten bei der Telekommunikationsüberwachung (z.B. nach § 100a StPO), denn dort sind Anschlussinhaberfeststellungen von entscheidender Bedeutung. [...] Gegenwärtig sind lediglich in Frankreich die Anbieter von Prepaid-Karten verpflichtet, Kundendaten zu erheben. Es kommt vor, dass trotz Vorgaben von Regierungsseite völlig unzutreffende Angaben gemacht werden. In den anderen EU-Staaten, aus denen Informationen vorliegen, gibt es keine gesetzlichen Regelungen, die bei dem Verkauf von Prepaid-Karten zu beachten sind. [...] Etwa 50 % der Karten werde innerhalb eines Jahres verschenkt, größtenteils innerhalb der Familie.*"[93]

Wenn es noch vor wenigen Jahren derart große Probleme mit der Identifizierung der Inhaber von Prepaid-Karten gab und auch weiterhin das Anmelden unter falschen Namen oder Weitergeben vorausbezahlter Mobiltelefonkarten möglich ist, so ist nicht glaubhaft, dass sich dies nun plötzlich geändert haben soll. So ist bekannt, dass trotz § 111 TKG viele Mobilfunkhändler beim Verkauf einer vorausbezahlten Telefonkarte bereit sind, diese auf ihren eigenen Namen zu registrieren,

93 BMWi-Ressortarbeitsgruppe, Eckpunkte zur Anpassung der Regelungen des § 90 TKG vom 28.03.2002, www.almeprom.de/fiff/material/Eckpunkte_90_TKG_Prepaid.pdf, 7.

wenn der Kunde dies wünscht. Auch auf Flohmärkten usw. ist der identifizierungsfreie Erwerb freigeschalteter Karten weiterhin möglich.

Der Bevollmächtigte der Bundesregierung bleibt den Nachweis schuldig, dass § 111 TKG hieran irgend etwas geändert hätte. Vor allem ist nicht ersichtlich, dass die Verfolgung schwerer Straftaten verbessert worden wäre. Wenn § 111 TKG die Datenlage verbessert hat, dann allenfalls bei arglosen, ungefährlichen Bürgern und vielleicht unvorsichtigen Kleinkriminellen.

Wenn der Bevollmächtigte der Bundesregierung die angebliche Bedeutung des § 111 TKG hochstilisiert, vergisst er vor allem zu erwähnen, dass die Behörden bis vor wenigen Jahren stets ohne die Identifizierungspflicht ausgekommen sind und in den allermeisten ausländischen Staaten noch immer auskommen. Die Norm ist für staatliche Zwecke entbehrlich; auch ohne sie war und ist eine effektive Strafverfolgung und sonstige staatliche Aufgabenwahrnehmung möglich.

2.7 §§ 95 Abs. 3, 111 Abs. 1 S. 4 TKG (Vorratsspeicherung von Bestandsdaten)

Hinsichtlich der Pflichten zur Vorratsspeicherung von Bestandsdaten ist vorab nochmals darauf hinzuweisen, dass aktuell auch die Vorratsspeicherung von Verkehrsdaten geplant ist und eine weitere Ausdehnung von Pflichten zur Vorratsspeicherung personenbezogener Daten für den Fall, dass sie dem Staat nützlich sein könnten, absehbar ist.

2.7.1 Regelungsinhalt des § 95 Abs. 3 TKG; Mindestspeicherfrist

Zu § 95 Abs. 3 TKG ist vorab in Erinnerung zu rufen, dass die Norm über § 111 Abs. 1 S. 4 TKG hinaus die Vorratsspeicherung sämtlicher während des Vertragsverhältnisses angefallenen Kundendaten anordnet. Dazu zählen Kontoverbindung und PIN-Kennungen ebenso wie E-Mail-Adressbücher und Partner- oder „Family&Friends"-Rufnummern. Der hohe Aussagegehalt dieser unter § 95 Abs. 3 TKG fallenden Bestandsdaten ist bereits dargestellt worden;[94] er erhöht die Eingriffsintensität des § 95 Abs. 3 TKG weiter.

§ 95 Abs. 3 TKG begründet eine Mindest- und nicht nur eine Höchstspeicherfrist. Er statuiert eine Speicherpflicht und nicht nur ein Speicherungsrecht.

Dies ergibt sich zunächst aus dem Wortlaut der Regelung. Die von der Norm geforderte Datenlöschung „mit Ablauf des auf die Beendigung folgenden Kalenderjahres" ist schlichtweg nicht möglich, wenn die Löschung bereits zuvor erfolgt ist.

Dass eine Mindestspeicherfrist vorliegt, zeigt weiter die systematische Auslegung. § 97 Abs. 3 S. 3 TKG hat der Gesetzgeber bewusst anders formuliert: „Die Verkehrsdaten dürfen - vorbehaltlich des Absatzes 4 Satz 1 Nr. 2 - höchstens sechs Monate nach Versendung der Rechnung gespeichert werden." Demgegenüber fehlt in § 95 Abs. 3 TKG das Wort „höchstens". Zudem ist § 95 Abs. 3 praktisch wortgleich mit § 111 Abs. 1 S. 4 TKG: „Nach Ende des Vertragsverhältnisses sind die Daten mit Ablauf des auf die Beendigung folgenden Kalenderjahres zu löschen." Dass § 111 Abs. 1 S. 4 TKG eine Mindestspeicherfrist statuiert, ist unbestritten.

Historisch ist auf die Begründung des TKG-Gesetzentwurfs von 2004 zu verweisen, die zu § 111 TKG (damals: § 109 TKG) Folgendes ausführt: „Durch Satz 4 wird geregelt, dass der Verpflichtete die Daten nach Vertragsende für die Dauer von einem Jahr weiter vorzuhalten und dann mit Ablauf des auf den Vertragsablauf folgenden Kalenderjahres zu löschen hat; diese Aufbewahrungsfrist entspricht den Vorgaben des § 93 Abs. 3."[95] (§ 93 Abs. 3 TKG-E entspricht dem heuti-

94 Seite 18.
95 BT-Drs. 15/2316, 95.

gen § 95 Abs. 3 TKG.) Der Gesetzgeber wollte also sowohl mit § 95 Abs. 3 TKG wie mit § 111 Abs. 1 S. 4 TKG eine Mindestspeicherfrist begründen.

Dass § 95 Abs. 3 TKG eine Mindestspeicherfrist begründet, ergibt sich schließlich auch aus dem Zweck der Vorschrift. Sie soll nämlich die Verfügbarkeit auch anderer als der in § 111 TKG genannten Bestandsdaten für öffentliche Zwecke gewährleisten. Der Bevollmächtigte der Bundesregierung gesteht dies auf S. 5 seiner Stellungnahme selbst zu.

Eine Auslegung der Norm gegen Willen des Gesetzgebers ist nach der Rechtsprechung des Bundesverfassungsgerichts unzulässig und wäre auch mit dem Gebot der Normenklarheit nicht zu vereinbaren. Denn eine von Wortlaut, Systematik und Zweck abweichende Auslegung ist für die von § 95 Abs. 3 TKG betroffenen Bürger unvorhersehbar.

Dass auch das Bundesjustizministerium in § 95 Abs. 3 TKG eine Mindestspeicherfrist sieht, verdeutlicht der Gesetzentwurf zur Umsetzung der Richtlinie 2006/24/EG. Die Richtlinie sieht unter anderem vor, dass Name und Anschrift der an Kommunikationsvorgängen Beteiligten mindestens sechs Monate lang auf Vorrat zu speichern sind. Dies gilt auch für Dienste, die von § 111 TKG nicht erfasst sind (z.B. Internetzugang). Gleichwohl sieht der Gesetzentwurf zur Umsetzung der Richtlinie keine Änderung des § 95 Abs. 3 TKG vor. Dementsprechend geht das Bundesjustizministerium davon aus, dass § 95 Abs. 3 TKG bereits in seiner gegenwärtigen Fassung die in der Richtlinie vorgesehene Mindestspeicherpflicht umsetzt.

Nur hilfsweise erfolgt deshalb die Erwägung, dass § 95 Abs. 3 TKG auch in einer Auslegung als Recht zur Vorratsspeicherung (Höchstspeicherfrist) verfassungswidrig wäre.[96] Aus Fernmeldegeheimnis und Recht auf informationelle Selbstbestimmung folgt – entgegen der Ansicht des Bevollmächtigten der Bundesregierung[97] – durchaus eine Schutzpflicht des Staates, die private Datenverarbeitung auf das erforderliche Maß zu beschränken. Dies gilt insbesondere dann, wenn der Staat selbst Zugriff auf die gespeicherten Daten hat und deswegen bereits die private Datenspeicherung typischerweise ein Risiko staatlicher Eingriffe begründet.

Das Bundesverfassungsgericht hat in seiner Entscheidung vom 23.10.2006 deutlich auf diese staatliche Schutzpflicht hingewiesen:

> „*Das allgemeine Persönlichkeitsrecht gewährleistet, dass in der Rechtsordnung gegebenenfalls die Bedingungen geschaffen und erhalten werden, unter denen der Einzelne selbstbestimmt an Kommunikationsprozessen teilnehmen und so seine Persönlichkeit entfalten kann. Dazu muss dem Einzelnen ein informationeller Selbstschutz auch tatsächlich möglich und zumutbar sein. Ist das nicht der Fall, besteht eine staatliche Verantwortung, die Voraussetzungen selbstbestimmter Kommunikationsteilhabe zu gewährleisten. In einem solchen Fall kann dem Betroffenen staatlicher Schutz nicht unter Berufung auf eine nur scheinbare Freiwilligkeit der Preisgabe bestimmter Informationen versagt werden. Die aus dem allgemeinen Persönlichkeitsrecht folgende Schutzpflicht gebietet den zuständigen staatlichen Stellen vielmehr, die rechtlichen Voraussetzungen eines wirkungsvollen informationellen Selbstschutzes bereitzustellen.*“[98]

2.7.2 Verfassungsrechtliches Verbot der Vorratsdatenspeicherung

Das Bundesverfassungsgericht hat nunmehr das „außerhalb statistischer Zwecke bestehende strikte Verbot der Sammlung personenbezogener Daten auf Vorrat” ausdrücklich ausgesprochen.[99] Entgegen der Ansicht des Bevollmächtigten der Bundesregierung gilt dieses Verbot nicht

96 Vgl. Beschwerdeschrift, 219 ff.

97 Stellungnahme des Bevollmächtigten der Bundesregierung, 21.

98 BVerfG, 1 BvR 2027/02 vom 23.10.2006, Abs. 38.

99 BVerfG, 1 BvR 518/02 vom 04.04.2006, NJW 2006, 1939 (1943), Abs. 105.

nur für eine Vorratsdatenspeicherung „zu unbestimmten oder noch nicht bestimmbaren Zwecken". Diese Einschränkung hat das Bundesverfassungsgericht in seinem Urteil zur Rasterfahndung aufgegeben und nicht mehr genannt.[100] Stattdessen hat das Gericht präzisiert, dass eine Vorratsdatenspeicherung nur zu statistischen Zwecken zulässig ist.

Unabhängig davon sehen die §§ 95 Abs. 3, 111 Abs. 1 S. 4 TKG durchaus eine Datensammlung „zu unbestimmten oder noch nicht bestimmbaren Zwecken" im Sinne der Rechtsprechung des Bundesverfassungsgerichts vor. Eine allgemeine Aufgabenbeschreibung (z.B. „zu Strafverfolgungszwecken", „zu Zwecken der Gefahrenabwehr") stellt keine hinreichende Zweckbestimmung in diesem Sinne dar. Dies ergibt sich schon daraus, dass das Bundesverfassungsgericht die Datenspeicherung zu statistischen Zwecken gesondert zulässt, also auch die Zweckbestimmung „zu statistischen Zwecken" nicht hinreichend präzise wäre. Würde man schon eine allgemeine Aufgabenbeschreibung zur Rechtfertigung einer Sammlung personenbezogener Daten auf Vorrat genügen lassen, so wäre das vom Bundesverfassungsgericht ausgesprochene Verbot gegenstandslos. Eine allgemeine Beschreibung der denkbaren Verwendungszwecke ist stets möglich. So kann die Rechtsprechung des Bundesverfassungsgerichts nicht gemeint sein.

Abwegig ist die Auffassung des Bevollmächtigten der Bundesregierung, die „Gewährleistung der öffentlichen Sicherheit" stelle eine hinreichend präzise Zweckbestimmung für eine massenhafte Aufbewahrung personenbezogener Daten auf Vorrat dar.[101] Im Polizeirecht ist anerkannt, dass das „Rechtsgut" der öffentlichen Sicherheit die Funktionsfähigkeit des Staates und seiner Einrichtungen, die Rechtsordnung sowie Güter und Rechte des Einzelnen und der Allgemeinheit umfasse. Ist aber die Durchsetzung der gesamten Rechtsordnung von dem Begriff umfasst, so kann man ihn auch ersetzen durch die „pflichtgemäße Erfüllung staatlicher Aufgaben durch Eingriffsbehörden". Dass eine solche Zweckbestimmung den verfassungsrechtlichen Anforderungen bei weitem nicht genügt,[102] vielmehr eine bereichsspezifische und präzise Bestimmung der einzelnen Verwendungszwecke erforderlich ist, ergibt sich aus der ständigen Rechtsprechung des Bundesverfassungsgerichts.[103]

Eine Pflicht zur unverzüglichen Löschung von Bestandsdaten ist den Unternehmen zumutbar. Dies zeigen schon die unverzüglichen Löschungspflichten für Verkehrsdaten (§ 96 Abs. 2, § 97 Abs. 3 TKG). Durch die heutige automatisierte Datenverarbeitung ist eine unverzügliche Löschung ohne nennenswerten Aufwand machbar.

2.8 § 95 Abs. 4 TKG

Aus dem Antrag in der Beschwerdeschrift ergibt sich eindeutig, dass auch § 95 Abs. 4 TKG Gegenstand der Verfassungsbeschwerde ist und sein soll. Dass die Norm auf Seite 1 der Beschwerdeschrift nicht aufgeführt ist, beruht offenkundig auf einem Versehen.

Die Verfassungswidrigkeit der Norm ist in der Beschwerdeschrift auch begründet worden. Es heißt nämlich zutreffend, dass ein bloßes Recht zur Identifizierung von Kunden anhand von Ausweispapieren zur Erreichung der damit verfolgten öffentlichen Zwecke von vornherein untauglich ist.[104] Die Sätze 2 und 3 der Vorschrift sind im Zusammenhang mit den §§ 111 ff. TKG geschaffen worden; die Verfassungswidrigkeit jener Normen erstreckt sich deshalb auch auf § 95 Abs. 4 TKG.

---

100 Die frühere Rechtsprechung wird nur unter „vergleiche" zitiert: „*Dadurch entsteht ein Risiko, dass das außerhalb statistischer Zwecke bestehende strikte Verbot der Sammlung personenbezogener Daten auf Vorrat (vgl. BVerfGE 65, 1 <47>) umgangen wird.*"

101 Stellungnahme des Bevollmächtigten der Bundesregierung, 69 f.

102 BVerfGE 65, 1 (66 f.).

103 BVerfGE 100, 313 (360); BVerfGE 65, 1 (46).

104 Beschwerdeschrift, 53 f.

2.9 §§ 112, 113 TKG

2.9.1 Praxis und Ausmaß der Abfrage von Bestandsdaten

Die vom Bevollmächtigten der Bundesregierung diskutierte frühere Praxis des Zugriffs auf Bestandsdaten ist für die verfassungsrechtliche Prüfung unerheblich. Zu Zeiten der Bundespost gab es im Übrigen kein automatisiertes Abrufverfahren. Die Ausführungen des Bevollmächtigten der Bundesregierung verkennen, dass die Beschwerde das verfassungsmäßige Recht des Staates, zur Abwendung von Gefahren für Leib und Leben sowie zur Verfolgung schwerer Straftaten auf die Telekommunikation einschließlich Bestandsdaten zuzugreifen, nicht in Abrede stellt. Dass der Staat Bestandsdaten erheben darf, steht nicht in Frage. Die Frage ist lediglich, unter welchen Voraussetzungen und zu welchen Zwecken dies erfolgen darf.

Die Vielzahl der nach den §§ 112, 113 TKG auskunftsberechtigten Stellen lässt sich keineswegs mit zwischenzeitlich erfolgten Zuständigkeitsänderungen erklären; der Bevollmächtigte der Bundesregierung substanziiert diese Behauptung auch nicht. Vielmehr führt er zutreffend aus, dass zu Zeiten der Bundespost als Ermächtigungsgrundlage allenfalls § 161 StPO in Frage kam, also eine Datenabfrage durch Staatsanwaltschaft und Polizei zu Zwecken der Strafverfolgung.[105]

Der Bevollmächtigte der Bundesregierung legt dar, dass zu Beginn der 90er Jahre nur 30-40.000 Abfragen von Bestandsdaten pro Jahr erfolgten, 2001 bereits 1,5 Mio. Abfragen und 2005 schließlich 3,4 Mio. Abfragen. Damit liegt allein in den Jahren 2001-2005 ein Anstieg um über 20% pro Jahr vor. Dementsprechend ist auch zukünftig alle drei bis vier Jahre mit einer Verdoppelung der Anfragen zu rechnen, also mit einem weiteren sprunghaften Anstieg.

Diese Entwicklung lässt sich in Anbetracht der stabilen Kriminalitätslage nicht mit einer gestiegenen Anzahl von Straftaten zu erklären. Die Ursache ist vielmehr darin zu suchen, dass die Abfrage von Bestandsdaten kostenlos, mit geringem Aufwand, ohne richterliche Kontrolle und ohne nennenswerte Eingriffsschwelle möglich ist. Insbesondere das automatisierte Abrufverfahren nach § 112 TKG hat zu einem sprunghaften Anstieg der Abfragen geführt, ohne dass dies sachlich begründet wäre. Die vom Bevollmächtigten der Bundesregierung geschilderte Praxis von Ermittlungsbehörden, jegliche bei Beschuldigten aufgefundene Telefonnummern abzufragen,[106] offenbar auch ohne konkrete Anhaltspunkte dafür, dass die Abfrage zur Aufklärung einer Straftat erforderlich ist, verdeutlicht die Sorglosigkeit im Umgang mit den Abfragebefugnissen.

Wenn der Bevollmächtigte der Bundesregierung diesen Zahlen den Anstieg an Mobilfunkanschlüssen von 48 Mio. im Jahr 2000 auf 79 Mio. im Jahr 2005 gegenüber stellt, vergisst er zu erwähnen, dass diese Zahlen nur einer jährlichen Steigerung um 10% entsprechen. Würde man auch die Festnetzanschlüsse in die Berechnung einbeziehen, um die Vergleichbarkeit zu den Zahlen nach § 112 TKG herzustellen, ergäbe sich eine noch geringere Steigerungsrate.

Aus dem Bereich der Telekommunikationsüberwachung (§§ 100a, 100b StPO) ist bekannt, dass die Anzahl von Strafverfahren, in denen die Telekommunikationsüberwachung zum Einsatz kommt (nicht die Zahl der Anordnungen), von Jahr zu Jahr um 10% steigt.[107] Dieser Anstieg lässt sich gerade nicht damit erklären, dass Beschuldigte zunehmend mehrere Anschlüsse nutzten; jeder Umstand würde sich nicht in der Verfahrenszahl niederschlagen. Wenn die Abfrage von Bestandsdaten mehr und mehr zur Standardmaßnahme wird, ohne dass dies durch eine Änderung der Sachlage zu erklären wäre, kann die Ursache nur in der fehlenden Eingriffsschwelle liegen.

---

105 Stellungnahme des Bevollmächtigten der Bundesregierung, 3.

106 Stellungnahme des Bevollmächtigten der Bundesregierung, 12.

107 Breyer, Vorratsspeicherung (2005), 23 m.w.N.

Die Verteilung der – vom Bevollmächtigten der Bundesregierung leider nicht vollständig offen gelegten – Anzahl von Zugriffen auf die einzelnen nach § 112 TKG berechtigten Stellen belegt, dass anderen Zwecken die als der Strafverfolgung keine nennenswerte praktische Bedeutung zukommt und die entsprechenden Befugnisse ohne Beeinträchtigung gestrichen werden können, zumal die entsprechenden Behörden ihre Aufgaben früher auch ohne die Abfragebefugnis wirksam erfüllen konnten.

2.9.2 Auskunftspflicht und Datenerhebungsbefugnis, Verhältnis zum „Fachrecht"

Der Bevollmächtigte der Bundesregierung meint, die §§ 112, 113 TKG statuierten nur eine Auskunftspflicht der Anbieter, während die Datenerhebungsbefugnis der berechtigten Stellen und die Weiterverarbeitung der Daten im „Fachrecht" – also in anderen Gesetzen – geregelt oder jedenfalls zu regeln sei. Fachrechtliche Datenerhebungsbefugnisse nennt er dann allerdings nur für den Bereich der Strafverfolgung, der Abwehr von Gefahren und der Nachrichtendienste, nicht für die übrigen in § 112 TKG angesprochenen Stellen.

Richtig ist, dass etwaige die §§ 112, 113 TKG einschränkende Normen des Fachrechts zu beachten wären. Der Bevollmächtigte der Bundesregierung hat indes nicht eine Bestimmung darzulegen vermocht, die den Datenzugriff weiter gehenden Beschränkungen unterwirft als die §§ 112, 113 TKG. Umgekehrt nennt er mit Art. 31 Abs. 1 BayPAG eine Norm, die Datenerhebungen nicht nur zur Abwehr von Gefahren, sondern bereits für vorgelagerte Ermittlungen erlauben soll. Die vom Bevollmächtigten der Bundesregierung angeführten §§ 100a ff. StPO gelten, wie er selbst einräumt, für Bestandsdaten nicht.

Die §§ 112, 113 TKG würden selbst dann einen (eigenständigen) Grundrechtseingriff darstellen, wenn man in ihnen nur eine Auskunftspflicht sähe. Denn die Einführung einer Auskunftspflicht führt zahlenmäßig öfter zu staatlichen Kenntnisnahmen als wenn der Staat auf freiwillige Auskünfte angewiesen ist. Dies gilt auch unter Berücksichtigung der Zwangsbefugnisse nach der Strafprozessordnung (Beschlagnahme), weil von diesen viel seltener Gebrauch gemacht würde als vom kostenlosen, automatisierten Abrufverfahren nach § 112 TKG.

Tatsächlich begründen die §§ 112, 113 TKG nicht nur eine Auskunftspflicht der Anbieter, sondern auch eine Datenerhebungsbefugnis der dort aufgeführten berechtigten Stellen. Dies ergibt sich schon aus den Normen selbst. § 112 Abs. 2 TKG bestimmt etwa, dass Auskünfte an die bezeichneten Behörden erteilt werden, „soweit die Auskünfte zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind". Nachdem die Regulierungsbehörde diese Voraussetzung nicht kontrollieren darf (§ 112 Abs. 4 S. 2-3 TKG), muss sich diese Bestimmung an die berechtigten Stellen selbst richten und deren Datenerhebungsbefugnis regeln. Auch § 113 Abs. 1 TKG regelt die Datenerhebungsbefugnis, wenn er bestimmt, Auskünfte seien zu erteilen, „soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes erforderlich ist". Auch diese Anforderungen sind von den Verpflichteten nicht zu kontrollieren und müssen sich deswegen an die berechtigten Stellen richten.

Gegenüber dem Deutschen Bundestag hat der Bevollmächtigte der Bundesregierung dann auch selbst ausgeführt: „So sind im Telekommunikationsbereich z.B. Bestandsdateneingriffe (welche nicht Art. 10 GG, sondern allein das Recht auf informationelle Selbstbestimmung betreffen) aufgrund von §§ 112 f. TKG zulässig; Verkehrsdateneingriffe, die Art. 10 GG berühren, dagegen müssen auf eine – inhaltlich anspruchsvollere – Befugnisnorm z.B. nach §§ 100a ff. StPO bzw. auf eine polizeigesetzliche Grundlage gestützt werden."[108] Auch der Bevollmächtigte der Bundes-

108 Möstl, Schriftliche Stellungnahme zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages am 8.11.2006, http://www.bundestag.de/ausschuesse/a04/anhoerungen/Anhoerung03/Stellungnahmen/Stellungnahme_02.pdf.

regierung geht also davon aus, dass die Erhebung von Bestandsdaten bereits aufgrund der §§ 112, 113 TKG zulässig ist und keiner zusätzlichen Befugnisnorm bedarf.

Dass die §§ 112, 113 TKG den maßgeblichen Grundrechtseingriff darstellen, ergibt sich auch daraus, dass ohne diese Normen Bestandsdatenauskünfte an Behörden ausgeschlossen wären. § 95 Abs. 1 S. 2 TKG erlaubt die Übermittlung von Bestandsdaten an Dritte nämlich nur, wenn ein Gesetz sie zulässt oder der Teilnehmer eingewilligt hat. Eine fachrechtliche Datenerhebungsbefugnis (z.B. § 161a StPO) berechtigt Telekommunikationsanbieter aber noch nicht zur Übermittlung personenbezogener Daten unter Durchbrechung der Zweckbindung des § 95 Abs. 1 TKG. Hierzu bedarf es vielmehr einer normenklaren Übermittlungsbefugnis, wie sie etwa in § 14 Abs. 2 des Telemediengesetzes vorgesehen ist. In Bezug auf Telekommunikations-Bestandsdaten stellen die §§ 112, 113 TKG die einzige vorhandene Übermittlungsbefugnis dar.

Eine gesonderte Regelung von Auskunftspflicht und Datenerhebungsbefugnis würde auch dem Gebot der Normenklarheit widersprechen. Eine Auskunftspflicht von Privaten ohne korrespondierende Datenerhebungsbefugnis der Behörde macht keinen Sinn. Umgekehrt macht auch eine Datenerhebungsbefugnis der Behörde ohne Übermittlungsrecht des Privaten (vgl. § 95 Abs. 1 S. 2 TKG) keinen Sinn. Eine normenklare Regelung der Übermittlung von Bestandsdaten muss deswegen einheitlich erfolgen.

2.9.3 Bestandsdaten bei Anbietern von Chatrooms

Das in der Beschwerdeschrift genannte Beispiel einer geschlossenen Benutzergruppe von Mitgliedern einer Aids-Selbsthilfegruppe[109] ist keineswegs fernliegend. Die Beschwerdeschrift nennt das Beispiel eines von einer Selbsthilfegruppe eingerichteten Internet-Diskussionsraums (Chatroom). Die Einrichtung eines solchen Dienstes ist einer Selbsthilfegruppe heutzutage durchaus möglich. Bei der Anmeldung zur Teilnahme an einem Diskussionsraum werden verbreitet Bestandsdaten abgefragt, beispielsweise die E-Mail-Adresse des Nutzers. Mithilfe des § 113 TKG könnten also durchaus alle Nutzer des Chatrooms einer Aids-Selbsthilfegruppe ermittelt werden. Dazu ist die Kenntnis von Inhalts- oder Verkehrsdaten nicht erforderlich.

Behörden könnten auch etwa daran interessiert sein, welche Benutzer der Internet-Chatroom einer Drogenberatungsstelle hat. Auch hierbei würde es sich um eine Auskunft über Bestandsdaten (§ 113 TKG) handeln. Dieses Beispiel macht deutlich, wie verhängnisvoll es sich auswirkt, dass die §§ 112, 113 TKG nicht auf die Bestandsdaten Beschuldigter oder ihrer Nachrichtenmittler beschränkt sind (anders als die §§ 100a, 100g StPO).

Wenn der Bevollmächtigte der Bundesregierung darauf verweist, dass die Normen der Strafprozessordnung die Ermittlungen der Strafverfolgungsbehörden auf Verdachtsfälle beschränken, so gewährleistet dies in der Praxis keinen wirksamen Schutz. So hat die Staatsanwaltschaft Halle schon dem bloßen Angebot illegaler Inhalte im Internet den Verdacht entnommen, dass Deutsche das Angebot nutzten („Operation Mikado"). Nach diesem Maßstab begründet schon der Internet-Chatroom einer Drogenberatungsstelle den Verdacht, dass Konsumenten illegaler Substanzen an der Diskussion teilnehmen.

2.9.4 Zuordnung des Internet-Nutzungsverhaltens

Auf S. 36 seiner Stellungnahme diskutiert der Bevollmächtigte der Bundesregierung die Rechtsprechung, derzufolge das gesamte Internetnutzungsverhalten nach Inhalt und Umständen der Person des Nutzers zugeordnet werden kann, indem eine Auskunft nach § 113 TKG über die Person des Nutzers einer IP-Adresse zum maßgeblichen Zeitpunkt eingeholt wird („dynamisch vergebene IP-Adresse").

109 Beschwerdeschrift, 10.

Unzutreffend ist die Ansicht des Bevollmächtigten der Bundesregierung, die Zulässigkeit dieser Praxis sei lediglich eine Frage der Auslegung und Anwendung des einfachen Rechts; gegebenenfalls müsse auf § 100g StPO zurückgegriffen werden. Auf § 100g StPO kann schon deswegen nicht zurückgegriffen werden, weil die Norm – wie der Bevollmächtigte der Bundesregierung an anderer Stelle selbst ausführt – gerade keine Auskunft über Name, Anschrift und Geburtsdatum der Kommunikationsteilnehmer vorsieht. Liest man § 100g StPO im Zusammenhang mit den §§ 112, 113 TKG, so wird deutlich, dass der Gesetzgeber mit den §§ 112, 113 TKG sehr wohl die Zuordnung einzelner Kommunikationsvorgänge zur Person der Teilnehmer erlauben wollte.[110] Dem folgt die herrschende Rechtsprechung. Mit diesem Inhalt muss sich die Norm an der Verfassung messen lassen. Eine verfassungskonforme Auslegung gegen den Willen des Gesetzgebers ist nicht zulässig; sie wäre auch mit dem Gebot der Normenklarheit nicht in Einklang zu bringen.

Eine Auskunftsanforderung nach den §§ 112, 113 TKG setzt nicht voraus, dass Name oder Anschlusskennung der Zielperson angegeben wird. Es genügt bereits die Angabe der näheren Umstände eines Kommunikationsvorgangs (z.B. eines Telefonanrufs, eines Internet-Seitenabrufs), um gemäß § 113 TKG Auskunft über den „dahinter stehenden" Anschlussinhaber zu verlangen. Praxisrelevant ist die Vorschrift vor allem bei der Verfolgung von Urheberrechtsverstößen im Internet (in „Tauschbörsen") anhand der Sitzungskennung (dynamisch vergebenen IP-Adresse) des Nutzers. Durch die geplante Vorratsspeicherung von Verkehrsdaten wird § 113 TKG erheblich an Bedeutung gewinnen. Denn die Identifizierung von Internetnutzern setzt voraus, dass die Internetzugangsanbieter die Vergabe von IP-Adressen protokollieren. Zu Abrechnungszwecken ist dies nicht erforderlich, weswegen eine solche Protokollierung bislang unzulässig ist. Im Fall von T-Online haben die Gerichte dies bestätigt.[111] Mit der geplanten Vorratsspeicherung der jeweils genutzten IP-Adressen würde eine Vervielfachung der Auskunftsanforderungen nach § 113 TKG einhergehen. Das Gesetz sieht nicht einmal eine statistische Erfassung der Anzahl der Auskunftsanforderungen nach § 113 TKG vor.

2.9.5 Verhältnismäßigkeitsgebot

Das in den §§ 112, 113 TKG einzig einschränkende Tatbestandsmerkmal der Erforderlichkeit ist vor dem Hintergrund der Nutzbarkeit und Verwendungsmöglichkeiten von Bestandsdaten vollkommen unzureichend. Zum vergleichbaren Merkmal der „Sachdienlichkeit" hat das Bundesverfassungsgericht ausgeführt:

> *„Das Gewicht der Interessenbeeinträchtigung wird nicht dadurch gemindert, dass von der Beschwerdeführerin lediglich verlangt wurde, ihr Einverständnis zur Erhebung sachdienlicher Informationen zu erklären. Durch diese Einschränkung ändert sich an der weitgehenden Unmöglichkeit eines informationellen Selbstschutzes für die Beschwerdeführerin nichts. Es fehlt an einem wirksamen Kontrollmechanismus für die Überprüfung der Sachdienlichkeit einer Informationserhebung.*
> *Aufgrund der Weite des Begriffs der Sachdienlichkeit kann der Versicherungsnehmer nicht im Voraus bestimmen, welche Informationen aufgrund der Ermächtigung erhoben werden können. Das Landgericht hat ausgeführt, sachdienlich seien „alle Tatsachen, die für die Feststellung und Abwicklung der Leistungen aus dem Versicherungsvertrag rechtserheblich sein können, und sei es auch nur mittelbar als Hilfstatsachen". Damit reicht praktisch jeder Bezug zu dem behaupteten Versicherungsfall aus, um eine Auskunftserhebung zu begründen."*[112]

Zum Merkmal der „Erforderlichkeit" hat das Bundesverfassungsgericht entschieden:

---

110 Vgl. BT-Drs. 14/7008, 7 für Auskünfte über den Namen der „hinter einer" IP- oder E-Mail-Adresse stehenden Person.

111 Landgericht Darmstadt vom 25.01.2006, Az. 25 S 118/05, MMR 2006, 330, rechtskräftig nach BGH vom 28.10.2006, Az. III ZR 40/06.

112 BVerfG, 1 BvR 2027/02 vom 23.10.2006, Abs. 46 f.

„Art. 16 Abs. 1 BayDSG normiert eine allgemeine Regelung für Datenerhebungen durch staatliche Stellen. Diese Norm knüpft lediglich an die Zuständigkeit der jeweils handelnden Behörde an und begrenzt die Datenerhebung lediglich durch das Gebot der Erforderlichkeit. Aufgaben- oder bereichsspezifische Voraussetzungen der Datenerhebung fehlen. Das in Art. 16 Abs. 1 BayDSG enthaltene Gebot der Erforderlichkeit kann die behördliche Praxis nicht hinreichend anleiten oder Kontrollmaßstäbe bereitstellen, wenn es nicht auf ein näher beschriebenes Normziel ausgerichtet wird. Die Norm bietet daher keine hinreichenden Maßstäbe für die Beurteilung der Rechtmäßigkeit einer Videoüberwachung. Auch kann der Einzelne auf dieser Grundlage nicht vorhersehen, bei welcher Gelegenheit, zu welchem Zweck und auf welche Weise Informationen über ihn erhoben werden dürfen.
Art. 17 Abs. 1 BayDSG, der die Speicherung, Veränderung und Nutzung der erhobenen Daten regelt, enthält gleichfalls keine hinreichenden Vorgaben für Anlass und Grenzen der erfassten datenbezogenen Maßnahmen, um als Ermächtigungsgrundlage für den beabsichtigten Grundrechtseingriff in Betracht zu kommen. Neben dem Gebot der Erforderlichkeit wird zwar auch der Erhebungszweck als Grenze der Datenverwendung genannt. Da jedoch Art. 16 Abs. 1 BayDSG den Erhebungszweck nicht näher umschreibt, verweist Art. 17 Abs. 1 BayDSG für Daten, die nach dieser Norm erhoben wurden, gleichfalls lediglich auf die Zuständigkeitsordnung.“[113]

Nicht anders verhält es sich mit den §§ 112, 113 TKG, die vollkommen unzureichend nur an die Erforderlichkeit zur Aufgabenwahrnehmung der genannten Behörden anknüpfen, ohne bereichsspezifische Voraussetzungen der Datenabfrage zu definieren. Auch im Fachrecht finden sich solche Voraussetzungen nicht. Das Gesetz erlaubt vielmehr gegenwärtig die Identifizierung von Anrufern und Internetnutzern schon zur Verfolgung von Parksündern. Dies ist evident unverhältnismäßig.

Verhältnismäßig sind Zugriffsrechte vor dem Hintergrund der hohen Nutzbarkeit und Verwendungsmöglichkeiten von Bestandsdaten nur zur Verfolgung schwerer Straftaten. Eben dies sieht auch Artikel 1 der Richtlinie zur Vorratsdatenspeicherung vor, der auch auf vorratsgespeicherte Bestandsdaten Anwendung findet. Die Richtlinie 2006/24/EG gilt für alle darin genannten Verkehrs- und Bestandsdaten gleichermaßen. Nach der Richtlinie erfolgt die Vorratsspeicherung auch von Bestandsdaten allein für die Verfolgung „schwerer Straftaten”.

Der Begriff der „schweren Straftaten“ beschreibt, in die Terminologie des Bundesverfassungsgerichts übersetzt, Straftaten im oberen Kriminalitätsbereich.[114] Demgegenüber erlauben die §§ 112, 113 TKG den Zugriff auf Bestandsdaten bereits zur Verfolgung jeder Straftat und sogar Ordnungswidrigkeiten sowie zu vielfältigen sonst denkbaren Zwecken. Dies wird dem Verhältnismäßigkeitsgebot nicht auch nur annähernd gerecht.

2.9.6 § 113 Abs. 1 S. 2 TKG (Zugriff auf PIN und PUK)

Es wurde bereits dargelegt, dass § 113 TKG die Abfrage äußerst sensibler Zugangsdaten erlaubt, darunter Passwörter für E-Mail-Dienste. Mit einem solchen Passwort kann die gesamte elektronische Post eines E-Mail-Nutzers abgefragt werden („Webmail“). Nach § 113 Abs. 1 S. 2 TKG dürfen beispielsweise Geheimdienste ohne richterliche Genehmigung Passwörter für E-Mail-Postfächer abfragen.

Soweit der Bevollmächtigte der Bundesregierung anführt, die Bestimmung des § 113 Abs. 1 S. 2 TKG sei unproblematisch, weil die in Endgeräten gespeicherten Daten ohnehin nicht dem Fernmeldegeheimnis unterfielen, verkennt er folgendes:

113 BVerfG, 1 BvR 2368/06 vom 23.2.2007, Absatz-Nr. 54 f.

114 Vgl. S. 115 der Entwurfbegründung: „nur bei schweren Straftaten i. S. v. § 100a Abs. 1 Nr. 2, Abs. 2 StPO-E“.

Der „Zugriff auf Endgeräte" und auf „in diesen oder im Netz eingesetzte Speichereinrichtungen" ermöglicht nicht nur den Zugriff auf Daten, die nach Abschluss eines Kommunikationsvorgangs gespeichert worden sind. Er erlaubt vielmehr auch etwa die Abfrage elektronischer Anrufbeantworter und E-Mail-Postfächer. Die auf einem Anrufbeantworter oder in einem E-Mail-Postfach im Einflussbereich des Telekommunikationsanbieters gespeicherten Nachrichten, die der Rufnummerninhaber noch nicht abgerufen hat oder noch nicht abrufen konnte, unterliegen in jedem Fall dem Fernmeldegeheimnis. Der Fall liegt nicht anders als wenn die Post ein Einschreiben zur Abholung bereit hält, nachdem sie den Empfänger nicht angetroffen hat. Auch ein solches Einschreiben ist durch das Postgeheimnis geschützt.

Außerdem hat das Bundesverfassungsgericht hinsichtlich der in einem Endgerät gespeicherten Verkehrs- und Inhaltsdaten festgestellt, dass diese eine erhöhte Schutzwürdigkeit aufweisen. § 113 Abs. 1 S. 2 TKG trägt dem keine Rechnung.

2.9.7 Verfahrensrechtliche Sicherungen des Grundrechtsschutzes

Bezüglich der fehlenden Pflicht zur Benachrichtigung der von Auskünften Betroffenen ist bereits ausgeführt worden,[115] dass auch im Fachrecht keine, auch keine nachträgliche Benachrichtigung über Bestandsdatenabfragen vorgesehen ist. Es kann von den Beschwerdeführern nicht verlangt werden, ihre Beschwerde gegen Fachrecht zu richten, welches überhaupt nicht vorhanden ist. Vielmehr obliegt es dem Gesetzgeber, wenn er zu Grundrechtseingriffen ermächtigt, sicherzustellen, dass die notwendigen Vorkehrungen zum Grundrechtsschutz der Betroffenen[116] gewährleistet sind, sei es im TKG oder in einem anderen Gesetz. Verletzt der Gesetzgeber diese Obliegenheit, so ist die gesamte Eingriffsermächtigung verfassungswidrig.[117] Entgegen der Auffassung des Bevollmächtigten der Bundesregierung lässt sich nicht zwischen einem „TKG-Gesetzgeber"[118] und einem „Fachrechts-Gesetzgeber" unterscheiden, sondern es gibt einen einzigen Bundesgesetzgeber, der das Notwendige zum Grundrechtsschutz der Betroffenen sicherstellen muss.[119]

Die Einschaltung der Bundesnetzagentur im Fall des § 112 TKG gewährleistet keine wirksame Kontrolle, zumal die Ersuchen im automatisierten Verfahren vorgelegt werden (§ 112 Abs. 2 TKG) und Tausende von Auskünften am Tag erteilt werden. Auch die Kontrolle durch den Bundesdatenschutzbeauftragten kann eine richterliche Kontrolle nicht ersetzen, zumal letztere von Art. 19 Abs. 4 GG garantiert ist. Möglich ist eine richterliche Überprüfung aber nur dann, wenn die Betroffenen von der heimlichen Abfrage ihrer Bestandsdaten benachrichtigt werden.

Zu Recht weist der Bevollmächtigte der Bundesregierung darauf hin, dass im Bereich des § 113 TKG ohnehin keine Kontrolle durch Bundesnetzagentur oder Datenschutzbeauftragte erfolgt.[120] Auch das zur Auskunft verpflichtete Unternehmen kann hier keine wirksame Kontrolle gewährleisten, weil es nach der fachgerichtlichen Rechtsprechung nicht rügen darf, das Auskunftersuchen sei rechtswidrig.[121]

Die Beschwerdeschrift rügt, dass die §§ 112, 113 TKG keine Zweckbindung der beauskunfteten Daten anordnen. Dem kann nicht entgegen gehalten werden, dass bereits das Fachrecht eine entsprechende Zweckbindung vorsehe. Denn die dort vorgesehene Zweckbindung ist vielfach

115 Seite 3 oben.
116 Vgl. BVerfGE 65, 1 (45 f.).
117 Breyer, Vorratsspeicherung (2005), 106.
118 So die Stellungnahme des Bevollmächtigten der Bundesregierung, 48.
119 BVerfGE 65, 1 (59).
120 Stellungnahme des Bevollmächtigten der Bundesregierung, 102.
121 So zu § 100a StPO BGH, MMR 1999, 99 (100); vgl. auch BeckTKG-Bock, § 113, Rn. 7.

durchbrochen und schwach. Die staatliche Erhebung von Telekommunikations-Bestandsdaten stellt einen so schwerwiegenden Grundrechtseingriff dar, dass eine besondere, strikte Zweckbindung angeordnet werden muss, zumal die möglichen Erhebungszwecke nach den §§ 112, 113 TKG ohnehin schon ausufernd weit sind.

Die Beschwerdeschrift rügt, dass die §§ 112, 113 TKG die verfassungsrechtlich gebotene Anordnung der Protokollierung jeder Erhebung, Verwendung, Übermittlung und Vernichtung von Telekommunikations-Bestandsdaten vermissen lassen.[122] Dem kann nicht entgegen gehalten werden, dass dies Aufgabe des Fachrechts sei. Denn auch das Fachrecht gewährleistet die erforderliche Protokollierung nicht. Wenn der Gesetzgeber zu Grundrechtseingriffen ermächtigt, muss er gleichzeitig dafür sorgen, dass die notwendigen Vorkehrungen zum Grundrechtsschutz getroffen werden, [123] sei es im TKG oder in anderen Gesetzen.

2.9.8 Parlamentsvorbehalt

Die Beschwerdeschrift rügt hinsichtlich der Ähnlichkeitssuche die Verletzung des Parlamentsvorbehalts.[124] Insoweit gesteht der Bevollmächtigte der Bundesregierung zu, dass erst in der Rechtsverordnung nach § 112 Abs. 3 TKG zu regeln wäre, ob eine Häuserabfrage, also die Beauskunftung aller in einem Haus gemeldeten Anschlüsse, zugelassen wird.[125] Gleiches gilt für die Möglichkeit einer Straßenabfrage oder einer Ortsabfrage. Dass der Gesetzgeber selbst derart zentrale Fragen über das Ausmaß des möglichen Grundrechtseingriffs nicht geregelt hat, verdeutlicht den Verstoß gegen den Parlamentsvorbehalt.

Einer Regelung durch Parlamentsgesetz steht der Detaillierungsgrad der erforderlichen Regelung nicht entgegen. Was in eine Verordnung gefasst werden kann, kann auch in ein Gesetz geschrieben werden. Im Verlauf des Gesetzgebungsverfahrens waren bereits detaillierte Regelungen der Ähnlichkeitssuche im TKG selbst vorgesehen gewesen. Diese Regelungen sind erst im weiteren Gesetzgebungsverfahren wieder gestrichen worden.

3 Zusammenfassende Bewertung

Insgesamt hat die Stellungnahme des Bevollmächtigten der Bundesregierung einseitig nur die Effektivität staatlichen Handelns und der möglichst leichten staatlichen Überwachung der Bevölkerung im Blick.[126] Eine solche Sichtweise macht den Einzelnen zum bloßen Objekt staatlichen Handelns. Symptomatisch ist die Ansicht des Bevollmächtigten der Bundesregierung, der Staat dürfe Informationen über seine Bürger einschränkungslos überall dort – auch zwangsweise – erheben, wo er sie finden könne, selbst bei vollkommen unverdächtigen, ungefährlichen und unbeteiligten Bürgern.[127]

Die vorliegende Beschwerde stellt nicht das verfassungsmäßige Recht des Gesetzgebers in Frage, die Erhebung erforderlicher Kundendaten zuzulassen und dem Staat zur Abwendung von Gefahren für Leib und Leben sowie zur Verfolgung schwerer Straftaten Zugriff auf Telekommunikations-Bestandsdaten zu gewähren. Soweit der Bevollmächtigte der Bundesregierung – wie leider zunehmend auch der Gesetzgeber – aber darüber hinaus der Auffassung ist, der Staat müsse eine „Garantie für die öffentliche Sicherheit und Ordnung" gewährleisten[128] und es existie-

122 BVerfGE 100, 313 (395 f.).
123 BVerfGE 65, 1 (59).
124 Beschwerdeschrift, 80.
125 Stellungnahme des Bevollmächtigten der Bundesregierung, 89.
126 Etwa Stellungnahme des Bevollmächtigten der Bundesregierung, 63-66.
127 Stellungnahme des Bevollmächtigten der Bundesregierung, 65.
128 So der Titel der Habilitationsschrift des Bevollmächtigte der Bundesregierung.

re ein „Grundrecht auf Sicherheit",[129] verkennt er die Grundprinzipien des freiheitlichen Rechtsstaats. Die Gewährleistung einer „Garantie für die öffentliche Sicherheit und Ordnung" ist nicht nur faktisch unmöglich. Schon das einseitige Streben nach einer möglichst lückenlosen Gewährleistung von „Sicherheit und Ordnung" widerspricht dem Grundgesetz.[130]

Die dem Grundgesetz zugrunde liegenden historischen Erfahrungen zeigen, dass es langfristig dem Interesse unserer Gesellschaft zuwider läuft, den Staat um jeden Preis nach „Sicherheit und Ordnung" streben zu lassen. Ein freiheitlicher Rechtsstaat geht entschlossen gegen Gefahren vor, wenn dazu Veranlassung besteht. Er greift aber – anders als die §§ 95 Abs. 3-4, 111 TKG – nicht alleine deshalb in die Grundrechte seiner (unverdächtigen und ungefährlichen) Bürger ein, um deren etwaige künftige Überwachung zu erleichtern. Er handelt – und hiergegen verstoßen die §§ 112, 113 TKG – maßvoll und in Bewusstsein der Tatsache, dass die Freiheit seiner Bürger, ihre freie Entfaltung und ihre unbefangene demokratische Mitwirkung die eigentliche Grundlage unserer Gesellschaft bilden. Gerade die Achtung der Freiheit und der Würde des Menschen machen den Charakter und, auf Dauer, auch die Stärke unseres freiheitlichen Rechtsstaats aus.

Berlin, den 23.03.2007

Starostik

Rechtsanwalt

129 a.a.O.

130 BVerfG, 1 BvR 518/02 vom 04.04.2006, NJW 2006, 1939 (1945), Abs. 128: „Das Grundgesetz unterwirft auch die Verfolgung des Zieles, die nach den tatsächlichen Umständen größtmögliche Sicherheit herzustellen, rechtsstaatlichen Bindungen, zu denen insbesondere das Verbot unangemessener Eingriffe in die Grundrechte als Rechte staatlicher Eingriffsabwehr zählt."