An das

Bundesverfassungsgericht

Schloßbezirk 3

76131 Karlsruhe

Verfassungsbeschwerde

Vorratsdatenspeicherung

Entwurf vom 23.12.2006

www.vorratsdatenspeicherung.de

Inhaltsübersicht

Inhaltsverzeichnis

Verfassungsbeschwerde

1. des Herrn Dr. Patrick Breyer, ...
2. des Herrn Prof. Dr. Christoph Gusy, ...
3. des Herrn Dr. Rolf Gössner, ...
4. ...

Verfahrensbevollmächtigt: Rechtsanwalt Meinhard Starostik, Schillstr. 9, 10785 Berlin

gegen Artikel 2 des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (BGBl. 2007, ...).

Die Beschwerdeführer beantragen,

> Artikel 2 des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (BGBl. 2007, ...) für unvereinbar mit Artikel 10, Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1, Artikel 5, Artikel 12, Artikel 14 und Artikel 3 Abs. 1 des Grundgesetzes zu erklären.

Ferner beantragen die Beschwerdeführer,

> im Wege der einstweiligen Anordnung Artikel 2 des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (BGBl. 2007, ...) bis zur Entscheidung über die vorliegende Verfassungsbeschwerde außer Kraft zu setzen.

A. Tatbestand

Der Beschwerdeführer zu 1 ist Inhaber und regelmäßiger Nutzer eines Festnetztelefonanschlusses des Anbieters ..., eines Mobiltelefonanschlusses des Anbieters ..., mehrerer Emailpostfächer der Anbieter ... und eines Internetzugangs des Anbieters ... Für Telefon und Mobiltelefon hat er bisher die Löschung der Verbindungsdaten mit Rechnungsversand gewählt. Verkehrsdaten über seine Email- und Internetzugangsverbindungen sind bislang nicht gespeichert worden, weil dies zu Abrechnungszwecken nicht erforderlich ist.

Der Beschwerdeführer zu 2 ist...

B. Zulässigkeit der Verfassungsbeschwerde

I. Allgemeine Zulässigkeitsvoraussetzungen

Die Beschwerdeführer sind von den §§ 110a, 110b TKG selbst, gegenwärtig und unmittelbar betroffen:

Wer Telekommunikationsdienste für die Öffentlichkeit erbringt oder daran mitwirkt, ist nach § 110a Abs. 1-4 TKG verpflichtet, eine Reihe von Daten, die von ihm bei der Nutzung seines Dienstes erzeugt oder verarbeitet werden, sechs Monate im Inland lang zu speichern. Diese Daten beziehen sich auf die Person des Anschlussinhabers und –nutzers. Als solche sind die Beschwerdeführer von § 110a TKG selbst, gegenwärtig und unmittelbar betroffen.

Dass das Gesetz für Anbieter von Internetdiensten Übergangsfristen vorsieht, ändert nichts an der Zulässigkeit der Verfassungsbeschwerde. Von den Beschwerdeführern kann ein Abwarten der Übergangsfrist nicht verlangt werden, weil die Beschwerdefrist des § 93 Abs. 3 BVerfGG dadurch versäumt würde. Außerdem kann die Zulässigkeit einer Vorratsdatenspeicherung sinnvollerweise nur einheitlich geklärt werden, so dass es keinen Sinn macht, im Hinblick auf Internetdienste ein gesondertes Verfahren zu verlangen. Ohnehin ist es nicht unwahrscheinlich, dass die Übergangsfrist jedenfalls bis zum Tag der mündlichen Verhandlung abgelaufen sein wird. Schließlich räumt § 150 Abs. 11a TKG Anbietern im Internetbereich bereits heute das Recht zu einer Vorratsdatenspeicherung ein. Den Beschwerdeführern ist zwar nicht im Einzelnen bekannt, welche Anbieter von diesem Recht Gebrauch machen. Insoweit genügt nach der Rechtsprechung des Bundesverfassungsgerichts aber eine mögliche Grundrechtsbetroffenheit, die sich jederzeit realisieren kann und von der die Beschwerdeführer auch keine Kenntnis erlangen. Im Übrigen ist zumindest von dem Internetzugangsanbieter Deutsche Telekom AG, Geschäftsbereich T-Online bekannt, dass er IP-Adressen 80 Tage lang auf Vorrat speichert.

Gegen die unmittelbar durch Gesetz erfolgte Grundrechtsverletzung ist der Rechtsweg nicht zulässig. Die Beschwerdeführer haben auch sonst keine andere Möglichkeit, um gegen die 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. Im Übrigen stellt die Vorratsdatenspeicherung ein so grundsätzliches Problem in einer freiheitlichen Gesellschaft dar, dass nur eine Entscheidung des Bundesverfassungsgerichts Rechtsfrieden schaffen kann.

Die Beschwerdeführer zu ..., die selbst zur Datenspeicherung verpflichtet werden sollen, sind von den §§ 110a, 110b TKG ebenfalls selbst, gegenwärtig und unmittelbar betroffen. Soweit das Gesetz für Internetdienste Übergangsfristen vorsieht, ist zu beachten, dass es die Anbieter schon zuvor zu später nicht mehr korrigierbaren Dispositionen zwingt. Denn wenn ohnehin die Erneuerung eines Systems ansteht, muss ein wirtschaftlich handelnder Anbieter aus Kostengründen zukünftige gesetzliche Anforderungen berücksichtigen. Systeme, die zu einer Vorratsdatenspeicherung in der Lage sind, sind erheblich teurer als herkömmliche Systeme. Die genaue Preisdifferenz kann mangels entsprechender Angebote auf dem Markt noch nicht beziffert werden. Schon heute lässt sich aber sagen, dass Internetdienste personenbezogene Daten ihrer Nutzer traditionell nicht erfassen oder nur wenige Tage lang speichern, während künftig eine sechsmonatige Speicherung erfolgen soll. Hierzu geeignete Systeme sind erhebliche teurer. Die Beschwerdeführer können auch nicht darauf verwiesen werden, durch ein Unterlassen der rechtzeitigen Umstellung Vollzugsakte zu provozieren oder gar das Risiko eines Bußgeld- oder Strafverfahrens einzugehen. Die Speicherpflicht ist bußgeldbewehrt (§ 149 Abs. 1 Nr. 28a-28g TKG). Gemäß § 115 Abs. 2 Nr. 1 TKG kann zur Durchsetzung der Verpflichtungen zur Datenspeicherung ein Zwangsgeld bis zu € 500.000,- verhängt werden. Darüber hinaus kann gem. § 115 Abs. 3 TKG der weitere Geschäftsbetrieb teilweise oder sogar ganz untersagt werden. Diese Risiken können den Beschwerdeführern nicht zugemutet werden, um – erst und zunächst – auf der Grundlage eines solchen nachteiligen Verwaltungsaktes auf dem Verwaltungsrechtsweg die Verfassungsmäßigkeit der hier angegriffenen Normen zur Überprüfung zu stellen. Ein Abwarten bis zum Ablauf der Übergangsfrist ist für die Beschwerdeführer demnach unzumutbar.

Das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG tritt am 15.09.2007 in Kraft (Art. 15), so dass die bis zum 15.09.2008 laufende Beschwerdefrist des § 93 Abs. 3 BVerfGG gewahrt ist.

II. 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.[1] Die vorliegend angegriffenen Regelungen sind jedoch nicht zwingend europarechtlich vorgegeben (1. und 2.) und könnten, selbst wenn man dies anders beurteilte, gleichwohl zulässig im Wege der Verfassungsbeschwerde angegriffen werden (3.).

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. Bei kostenlosen Emaildiensten fallen dagegen oft keine Bestandsdaten an. § 111 TKG verbietet folglich überschießend die anonyme Bereitstellung von Emailkonten.

Ferner 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.[2] 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.[3] Gegen eine Klage wegen Vertragsverletzung durch Nichtumsetzung einer Richtlinie kann ein Mitgliedsstaat die Nichtigkeit der Richtlinie nicht einwenden.[4] 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).

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.[5] 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.

a) 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[6] und des Rates[7] 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

1 BVerfGE 102, 147, Ls. 1 und 2.
2 EuGHE 1979, 623; EuGH, C-475/01 vom 05.10.2004, Abs.-Nr. 18.
3 EuGH, C-475/01 vom 05.10.2004, Abs.-Nr. 18.
4 EuGH, C-139/03 vom 15.07.2004, Abs.-Nr. 7.
5 EuGHE 1988, 3611; EuGHE I 1992, 5437; EuGH, C-475/01 vom 05.10.2004, Abs.-Nr. 19; st. Rspr.
6 Juristische Analyse vom 22.03.2005, SEC(2005)420, http://www.statewatch.org/news/2005/apr/Commission-legal-opinion-data-retention.pdf.
7 Rechtsgutachten des Juristischen Dienstes des Rates vom 05.04.2005, http://www.statewatch.org/news/2005/apr/Council-legal-opinion-data-retention.pdf.

des EuGH zur Fluggastdatenübermittlung in die USA.[8] 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 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."[9]

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.[10]

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.[11] Die Ausführungen waren also keineswegs auf den Einzelfall beschränkt. Der Generalanwalt hat sogar ausdrücklich auf die Vorratsdatenspeicherung Bezug genommen.[12]

b) 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"[13] 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[14]. Entsprechend Art. 8 EMRK hat der Europäische Gerichtshof beispielsweise den Schutz der Privatsphäre als Gemeinschaftsgrundrecht anerkannt[15].

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[16] 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.

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

(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

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

wiederholt entschieden, dass auch Telefongespräche als „Korrespondenz“ im Sinne des Art. 8 EMRK anzusehen sind[17]. 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[18], ebenso wie die Verwendung solcher Daten und die Verweigerung ihrer Löschung[19].

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[20], weil Verbindungsdaten, „besonders die gewählten Nummern [...] integraler Bestandteil der Kommunikation“ seien[21]. Entsprechend der zu Art. 10 Abs. 1 Var. 3 GG aufgeführten Argumentation[22] ist die Vorratsspeicherung von Verkehrsdaten daher als Eingriff in Art. 8 EMRK anzusehen, selbst wenn sie von Privaten durchgeführt wird[23]. Art. 8 EMRK schützt dabei sowohl geschäftliche als auch private Kommunikation[24].

(2) Rechtfertigung von Eingriffen

(a) 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[25]. Rechtlich unverbindliche Regulierungsmechanismen wie deutsche Verwaltungsvorschriften oder eine bestimmte Praxis der zuständigen Organe genügen dagegen nicht[26]. Einen Parlamentsvorbehalt kennt das Gericht nicht.

Die Entscheidung, ob eine Einzelmaßnahme nach nationalem Recht rechtmäßig ist, überlässt der EGMR grundsätzlich den nationalen Gerichten[27], wobei deren Entscheidung nachvollziehbar sein muss[28]. 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[29]. Dem Einzelnen müsse es möglich sein, sein Verhalten den Vorschriften entsprechend einzurichten, was ein – gemessen an der Schwere des Eingriffs[30] – hinreichendes Maß an Vorhersehbarkeit voraussetze[31]. 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[32]. Bei solchen Maßnahmen muss unter anderem eine effektive, rechtsstaatliche, unabhängige und unparteiische Kontrolle über eingreifende Maßnahmen gewährleistet sein, welche grundsätzlich, zumindest

17 Frowein/Peukert-Frowein, Art. 8, Rn. 34 m.w.N.
18 Frowein/Peukert-Frowein, Art. 8, Rn. 5 m.w.N.
19 EGMR, Leander-S (1987), Publications A116, Abs. 48; EGMR, Rotaru-ROM (2000), Decisions and Reports 2000-V, Abs. 46.
20 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.
21 EGMR, Malone-GB (1984), EuGRZ 1985, 17 (23), Abs. 84.
22 Seiten 23-26.
23 So auch Allitsch, CRi 2002, 161 (166); Covington & Burling, Memorandum (I), 3; ebenso die Verfasser des RSV-Entwurfs in dessen Erwägungsgrund 9.
24 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.
25 EGMR, Huvig-F (1990), Publications A176-B, Abs. 28.
26 Vgl. EGMR, Khan-GB (2000), Decisions and Reports 2000-V, Abs. 27.
27 EGMR, Kruslin-F (1990), Publications A176-A, Abs. 29.
28 Vgl. EGMR, Craxi-IT (2003), hudoc.echr.coe.int/Hudoc1doc/HEJUD/200307/craxi%20-%2025337jv.chb1%2017072003e(sl).doc, Abs. 78 und 81.
29 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.
30 EGMR, Kruslin-F (1990), Publications A176-A, Abs. 33.
31 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.
32 EGMR, Malone-GB (1984), EuGRZ 1985, 17 (20 und 22), Abs. 67 und 81.

als nachträglicher Rechtsbehelf, durch die Justiz zu gewährleisten ist[33]. 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[34].

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[35]. 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[36].

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 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[37].

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[38]. 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[39].

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[40]. In jedem Fall muss der Staat angemessene Maßnahmen ergreifen, um zu verhindern, dass Dritte unbefugt Kenntnis von überwachten Telekommunikationsinhalten erlangen[41].

(b) 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[42]. Dabei behält sich der EGMR aber das Letztentscheidungsrecht vor, so dass er selbst ver-

33 EGMR, Klass u.a.-D (1978), EuGRZ 1979, 278 (286), Abs. 55; EGMR, Rotaru-ROM (2000), Decisions and Reports 2000-V, Abs. 59.

34 EGMR, Klass u.a.-D (1978), EuGRZ 1979, 278 (285), Abs. 50.

35 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.

36 EGMR, Kopp-CH (1998), StV 1998, 683 (684), Abs. 72.

37 EGMR, Rotaru-ROM (2000), Decisions and Reports 2000-V, Abs. 57.

38 EGMR, Kruslin-F (1990), Publications A176-A, Abs. 35; EGMR, Valenzuela Contreras-ES (1998), Decisions and Reports 1998-V, Abs. 46.

39 EGMR, Amann-CH (2000), Decisions and Reports 2000-II, Abs. 61.

40 EGMR, Malone-GB (1984), EuGRZ 1985, 17 (23), Abs. 87.

41 EGMR, Craxi-IT (2003), hudoc.echr.coe.int/Hudoc1doc/HEJUD/200307/craxi%20-%2025337jv.chb1%2017072003e(sl).doc, Abs. 74.

42 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),

tretbare nationale Entscheidungen verwerfen kann[43]. Hinsichtlich des Ausmaßes des nationalen Beurteilungsspielraums schwankt das Gericht von Entscheidung zu Entscheidung[44].

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 zu dem Gewicht des Zwecks steht[45]. Der EGMR hat dazu eindeutig erklärt, dass das Interesse des Staates gegenüber den Interessen des Einzelnen an der Achtung seiner Privatsphäre abgewogen werden müsse[46]. Eingriffe sind zwar nicht auf das unerlässliche Maß beschränkt, aber ein bloßes Nützlich- oder Wünschenswertsein genügt nicht[47]. Sind die genannten Kriterien erfüllt, dann liegt keine Verletzung von Art. 8 EMRK vor.

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[48], insbesondere, wenn nicht wegen einer bestimmten Tat oder Gefahr ermittelt wird, sondern nach möglichen Taten oder Gefahren erst gesucht werden soll[49]. Jedenfalls gelten die unten zum Grundgesetz gemachten Ausführungen analog, wonach eine generelle Verkehrsdatenspeicherung das Verhältnismäßigkeitsgebot verletzt[50]. Eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten ist daher mit Art. 8 EMRK unvereinbar[51].

bb) Das Recht auf Achtung des Eigentums (Artikel 1 ZEMRK)

Den Schutz des Eigentums gewährleistet das erste Zusatzprotokoll zur EMRK[52] (ZEMRK). Art. 1 ZEMRK bestimmt: „(1) Jede natürliche oder juristische Person hat ein Recht auf Achtung ihres Eigentums. Niemandem darf sein Eigentum entzogen werden, es sei denn, dass das öffentliche Interesse es verlangt, und nur unter den durch Gesetz und durch die allgemeinen Grundsätze des Völkerrechts vorgesehenen Bedingungen. (2) Die vorstehenden Bestimmungen beeinträchtigen jedoch in keiner Weise das Recht des Staates, diejenigen Gesetze anzuwenden, die er für die Regelung der Benutzung des Eigentums im Einklang mit dem Allgemeininteresse oder zur Sicherung der Zahlung der Steuern, sonstiger Abgaben oder von Geldstrafen für erforderlich hält."

Bei der Prüfung der Vereinbarkeit einer Maßnahme mit Art. 1 ZEMRK ist zunächst zu untersuchen, ob in Eigentum im Sinne des Artikels eingegriffen wurde. Sodann ist zu prüfen, ob ein Entzug von Eigentum (Abs. 1 S. 2), eine Regelung der Benutzung des Eigentums (Abs. 2) oder ein sonstiger Eingriff (Abs. 1 S. 1) vorliegt. Schließlich ist zu prüfen, ob der Eingriff gerechtfertigt ist.

- Schutzbereich

Die Eigentumsgarantie nach Art. 1 ZEMRK schützt – ebenso wie Art. 14 GG – nur bereits erworbenes Eigentum und nicht künftiges[53]. Das Vermögen einer Person als solches ist nicht geschützt. Der

---

hudoc.echr.coe.int/ Hudoc1doc2/HEJUD/200107/foxley%20-%2033274jv.chb3%2020062000e.doc, Abs. 43.

43 EGMR, Sunday Times-GB (1979), EuGRZ 1979, 386 (389), Abs. 59.

44 Van Dijk/van Hoof, Theory and Practise of the European Convention on Human Rights, 585 ff.

45 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.

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

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

48 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.

49 Allitsch, CRi 2002, 161 (167).

50 Seiten 28-82.

51 I.E. ebenso EP, Entschließung zur Durchführung der Datenschutzrichtlinie (I), Punkt 18.

52 Zusatzprotokoll zur Europäischen Menschenrechtskonvention zum Schutze der Menschenrechte und Grundfreiheiten vom 20.03.1952 (BGBl. II 1956, 1880), geändert durch Protokoll Nr. 11 vom 11.05.1994 (BGBl. II 1995, 578), conventions.coe.int/ Treaty/en/Treaties/Html/009.htm. Deutsche Übersetzung unter www2.amnesty.de/ internet/ai-theme.nsf/WAlleDok?OpenView&Start=1&Count=30&Expand=8.

53 EGMR, Wendenburg u.a.-D (2003), NJW 2003, 2221 (2222).

Umstand, dass eine Vorratsspeicherungspflicht die betroffenen Unternehmen wirtschaftlich belastet, begründet daher für sich genommen noch keinen Eingriff in Eigentum im Sinne des Art. 1 ZEMRK.

Nach der Rechtsprechung des EGMR ist allerdings der Kundenstamm eines Unternehmens als Eigentum im Sinne des Art. 1 ZEMRK anzusehen[54]. In dieses Eigentum greift der Staat ein, wenn eine staatliche Maßnahme zum Verlust von Kunden führt[55]. Auf diese Weise gewährleistet Art. 1 ZEMRK einen gewissen Schutz der Berufsfreiheit. Von der Rechtsprechung des EGMR nicht gedeckt ist allerdings die Aussage, geschützt sei generell das Recht am eingerichteten und ausgeübten Gewerbebetrieb[56]. Der EGMR hat in keinem Urteil darauf abgestellt, dass ein Unternehmen als solches geschütztes Eigentum darstelle.

Eine Vorratsspeicherungspflicht betrifft alle Anbieter von Telekommunikationsdiensten betreffen, so dass eine Verringerung des Kundenstamms einzelner Unternehmen nicht zu erwarten ist. Folglich lässt sich auch unter dem Gesichtspunkt einer Verminderung des Kundenstamms kein Eigentumseingriff durch eine Vorratsspeicherungspflicht annehmen.

Eine Vorratsspeicherungspflicht berührt den Schutzbereich des Art. 1 ZEMRK somit nur bezüglich des Eigentums der betroffenen Unternehmen an ihren Anlagen.

- Entzug von Eigentum

Dieses Eigentum könnte durch eine Vorratsspeicherungspflicht entzogen werden. Als Entzug von Eigentum im Sinne des Art. 1 Abs. 1 S. 2 ZEMRK sind nicht nur formelle, sondern auch „de facto"-Enteignungen anzusehen[57]. Eine solche „faktische Enteignung" liegt nach der Rechtsprechung des EGMR vor, wenn eine hoheitliche Maßnahme wegen ihrer schwerwiegenden Auswirkungen einer förmlichen Aufhebung der Eigentümerposition gleich kommt[58], insbesondere wenn die verbleibende Rechtsposition eine sinnvolle Nutzung der betroffenen vermögenswerten Gegenstände nicht mehr zulässt[59]. Ein solcher Eigentumsentzug ist in der Regel nur dann verhältnismäßig, wenn eine angemessene Entschädigung vorgesehen ist[60].

Die Anlagen und Gerätschaften der Anbieter von Telekommunikations-, Tele- und Mediendiensten stellen gegenwärtiges Eigentum dar und sind daher durch das ZEMRK geschützt. Eine Verkehrsdatenspeicherungspflicht begründet insoweit einen Eingriff in dieses Eigentum wie bisher genutzte Einrichtungen von den Nutzungsberechtigten nicht mehr genutzt werden können, weil sie eine Vorratsspeicherung von Telekommunikationsdaten nicht erlauben[61]. Dieser Eingriff ist nur unter den Voraussetzungen des Art. 1 S. 2 ZEMRK zulässig. Insbesondere müssen die Betroffenen einen angemessenen Ausgleich erhalten[62].

- Nutzungsregelung

Was das sonstige, weiterhin nutzbare Eigentum der von einer Vorratsspeicherungspflicht Betroffenen anbelangt, so kommt in Betracht, die Vorratsspeicherungspflicht als Regelung über die Benutzung des Eigentums anzusehen (Art. 1 Abs. 2 ZEMRK). Für die Annahme, dass Handlungspflichten Privater Eingriffe in Art. 1 ZEMRK darstellen können, spricht die Entscheidung der Europäischen Kommission für Menschenrechte (EKMR) für den Fall der gesetzlichen Verpflichtung Privater zur Berechnung, Einbehaltung und Abführung der Lohnsteuer[63]. Zwar lässt die EKMR die Frage eines Eigentumseingriffs offen. Sie prüft aber dann doch die Rechtfertigung der Maßnahme in der Sache, was für die Annahme spricht, dass sie einen Eigentumseingriff nicht verneint hätte, wäre es darauf angekommen.

In der Tat sind Nutzungsregelungen im Sinne des Art. 1 Abs. 2 ZEMRK grundsätzlich alle hoheitlichen Maßnahmen, die einen bestimmten Gebrauch des Eigentums gebieten oder untersagen[64]. Zwar würde die Eigentumsgarantie ausufern, wenn man jede Handlungspflicht, zu deren Erfüllung der Verpflichtete sein Eigentum einsetzen muss, als Regelung über die Benutzung des Eigentums ansähe.

54 EGMR, Wendenburg u.a.-D (2003), NJW 2003, 2221 (2222) m.w.N.
55 EGMR, Wendenburg u.a.-D (2003), NJW 2003, 2221 (2222).
56 So Frowein/Peukert-Peukert, Art. 1 ZEMRK, Rn. 6.
57 Frowein/Peukert-Peukert, Art. 1 des 1. ZP, Rn. 25; Grabenwarter, 417.
58 Frowein/Peukert-Peukert, Art. 1 des 1. ZP, Rn. 25; Grabenwarter, 417.
59 Grabenwarter, 417.
60 EGMR, James u.a.-GB (1986), Publications A98, Abs. 54; Meyer-Ladewig, Art. 1 des 1. ZP, Rn. 29 m.w.N.
61 Vgl. schon Seiten 92-93.
62 Vgl. schon Seite 93.
63 EKMR, E 7427/76, Decisions and Reports 7, 148.
64 Grabenwarter, 418; vgl. auch EKMR, E 5593/72, Collection of Decisions 45, 113: Eigentumseingriff durch eine gesetzliche Verpflichtung zur Instandhaltung von Mietshäusern.

Indes ist – anders als bei Art. 14 GG[65] – eine Abgrenzung des Anwendungsbereichs des Art. 1 ZEMRK zur Berufsfreiheit nicht erforderlich, weil letztere durch die EMRK nicht gewährleistet ist. Der Schutzbereich des Art. 1 ZEMRK kann daher weiter gezogen werden als der des Art. 14 GG. Angemessen erscheint es, mittelbare Verkürzungen von Eigentumsrechten immer dann als Eingriffe in Art. 1 Abs. 2 ZEMRK anzusehen, wenn sie die Beeinträchtigung des Eigentums typischerweise und vorhersehbar zur Folge haben oder eine besondere Beeinträchtigungsgefahr in sich bergen, die sich jederzeit verwirklichen kann[66].

Durch die Einführung einer Vorratsspeicherungspflicht zwingt der Staat die betroffenen Unternehmen, ihr Eigentum zur Speicherung und Vorhaltung von Verkehrsdaten zu nutzen. Einige Gerätschaften müssen sogar allein zu diesem Zweck eingesetzt werden und können ansonsten nicht mehr gebraucht werden. Wenn man nicht bereits einen unmittelbaren Eingriff in das Eigentum an den betroffenen Geräten annimmt, so werden die Eigentümerbefugnisse jedenfalls typischerweise und vorhersehbar verkürzt, so dass ein staatlicher Eingriff in Art. 1 ZEMRK vorliegt.

Ein solcher kann nach Art. 1 Abs. 2 ZEMRK aus Gründen des Allgemeininteresses gerechtfertigt sein, wobei den Vertragsstaaten ein weiter Beurteilungsspielraum zukommt[67]. Stets ist aber das Verhältnismäßigkeitsprinzip zu beachten[68]. In Bezug auf die Verhältnismäßigkeit einer generellen Verkehrsdatenspeicherungspflicht ist auf die obigen Ausführungen zu verweisen, wonach der Nutzen einer solchen Regelung nur gering ist[69], die finanzielle Belastung der Betroffenen dagegen erheblich ausfallen kann[70]. Wie zu Art. 12 GG im Einzelnen dargelegt[71], ist die Verhältnismäßigkeit einer Verkehrsdatenspeicherungspflicht daher auch unter dem Aspekt des Art. 1 ZEMRK zu verneinen, weil die zur Durchführung der Verkehrsdatenspeicherung Verpflichteten einen erheblichen Teil der anfallenden Kosten aus eigenen Mitteln tragen müssen. Entgegen dem ursprünglichen Entwurf sieht die Richtlinie keine Pflicht zur Entschädigung vor.

cc) 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[72]. In technischer Hinsicht geschützt sind alle Kommunikationsformen[73], 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[74].

Wie bei Art. 5 GG[75] 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 Telekommunikations-Verkehrsdaten der Fall[76]. Eine Behinderung der Kommunikation erfolgt insoweit einerseits durch den Abschreckungseffekt, der mit einer generellen Vorratsspeicherung von Verkehrsdaten verbunden ist, andererseits aber auch durch die Kostensteigerungen, die mit einer nutzerfinanzierten Vorratsspeicherung einher gehen[77]. Die Einführung einer Vorratsspeicherung von Telekommunikationsdaten stellt damit einen Eingriff in Art. 10 EMRK dar.

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[78], insbesondere das Verhältnismäßig-

65 Seiten 92-93.
66 Vgl. Seite 24.
67 EGMR, Tre Traktörer Aktiebolag-S (1989), Publications A159, Abs. 62.
68 EGMR, Tre Traktörer Aktiebolag-S (1989), Publications A159, Abs. 59; Frowein/Peukert-Peukert, Art. 1 ZEMRK, Rn. 62.
69 Seite 34 ff.
70 Seiten 89-90.
71 Seiten 90-91.
72 Frowein/Peukert-Frowein, Art. 10, Rn. 5; Kugelmann, EuGRZ 2003, 16 (20) m.w.N.
73 Frowein/Peukert-Frowein, Art. 10, Rn. 5; Kugelmann, EuGRZ 2003, 16 (19).
74 Vgl. Frowein/Peukert-Frowein, Art. 10, Rn. 15 ff.
75 Seiten 93-98.
76 Seiten 96-97.
77 Seiten 96-97.
78 Seiten 12-14.

keitsprinzip. Wie zu Art. 5 GG gezeigt[79], 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 Telekommunikations-Verkehrsdaten 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[80]. Entsprechend den Ausführungen zu den Grundrechten des Grundgesetzes[81] 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.

c) 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.

d) 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.[82] 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 der Telekommunikation aller Europäer in einer demokratischen Gesellschaft nicht erforderlich und verhältnismäßig ist, ist evident.

2. Fehlende Umsetzungspflicht nach Völkerrecht

Zum 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[83], seien sie inexistent oder nicht. Die mit der Umsetzung befassten Staatsorgane sind aus verfassungsrechtlichen Gründen gehindert, diese Rechtsakte in Deutschland anzuwenden[84], 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.[85]

Dass die Richtlinie 2006/24/EG formell wie materiell gegen das primäre Gemeinschaftsrecht und damit gegen den EG-Vertrag verstößt, ist bereits dargelegt worden.[86] Unabhängig davon, wie das

79 Seite 98.
80 Zur Diskussion Kugelmann, EuGRZ 2003, 16 (20) m.w.N.
81 Seiten 94-95.
82 EuGH, Urteil vom 30.05.2006, Az. C-317/04 und C-318/04.
83 BVerfGE 89, 155 (188).
84 BVerfGE 89, 155 (188).
85 BVerfGE 89, 155 (188).
86 Seite 10 ff.

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.

3. Zulässigkeit trotz Umsetzungspflicht

Selbst wenn man auch nach Völkerrecht eine Umsetzungspflicht annähme, gebietet 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 drohende Zwangsprotokollierung ihrer Telekommunikation 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.

C. Begründetheit der Verfassungsbeschwerde

1. Das Fernmeldegeheimnis und das Recht auf informationelle Selbstbestimmung (Artikel 10 Abs. 1 Var. 3 GG und Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 GG)

Gerügt wird eine Verletzung des Fernmeldegeheimnisses und des Rechts auf informationelle Selbstbestimmung.

a) Schutzbereich

Das Fernmeldegeheimnis gewährleistet den an einem räumlich distanzierten Kommunikationsvorgang Beteiligten die Vertraulichkeit von Inhalt und näheren Umständen eines Telekommunikationsvorgangs[87]. Dem Bundesverfassungsgericht zufolge schützt Art. 10 Abs. 1 Var. 3 GG vor jeder staatlichen „Einschaltung", die nicht im Einverständnis mit beiden Kommunikationspartnern erfolgt[88]. Geschützt ist etwa die Information, ob und wann zwischen welchen Personen und Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat oder versucht worden ist[89]. Der Begriff „Fernmeldegeheimnis" erfasst nicht nur althergebrachte Formen des Fernmeldeverkehrs wie die Sprachtelefonie, sondern beispielsweise auch die Kommunikation per E-Mail[90]. Das Gleiche gilt für die Kommunikation etwa per SMS-Nachricht oder per IRC-Chat.

Verkehrsdaten über die Nutzung von Festnetztelefon, Mobiltelefon, Email, Internet und Internettelefonie fallen danach in den Schutzbereich des Fernmeldegeheimnisses, weil sich mit ihrer Hilfe die näheren Umstände von Telekommunikationsvorgängen aufklären lassen: Wer hat wann und von wo aus mit wem kommuniziert?

(1) Massenkommunikation

Selbst wenn man das Fernmeldegeheimnis nur für Individualkommunikation für einschlägig hielte, schützt es in jedem Fall die Information, wer wann unter welcher Nummer (Internet-Protocol-Adresse) das Internet genutzt hat. Denn eine Internet-Zugangsverbindung ist Voraussetzung jeder Individualkommunikation per Internet, sei es per Email oder per Internettelefonie. Richtigerweise unterfällt die Internetnutzung dem Fernmeldegeheimnis aber nicht nur, soweit Dienste der Individualkommunikation genutzt werden, sondern auch bei der Nutzung als Medium der Massenkommunikation, etwa beim Surfen im Internet.

Technische Voraussetzung jeder Internetnutzung ist die Zuweisung einer IP-Adresse. Diese Adresse identifiziert den Nutzer im Internet, gerade auch gegenüber den genutzten Diensten. Anhand dieser IP-Adresse zeichnen Internetdienste verbreitet auf, was der Nutzer genau tut. Ist also – wie von § 110a TKG angeordnet – bekannt, wer wann unter welcher IP-Adresse das Internet genutzt hat, kann sich auch nachvollziehen lassen, mit wem diese Person per Internet kommuniziert und was sie sonst im Internet getan hat.

Während der Schutz des Fernmeldegeheimnisses nach allgemeiner Meinung im Ausgangspunkt nur solche Informationen umfassen soll, die an einen bestimmten Adressatenkreis gerichtet sind[91], besteht Uneinigkeit bezüglich der Behandlung von Massenkommunikation, die mittels Fernmeldetechnik abgewickelt wird[92]. Massenkommunikation wird dabei als öffentlich zugängliche Kommunikation definiert[93]. Insbesondere im Hinblick auf den Abruf öffentlicher Internetseiten („Surfen") ist die Frage relevant.

87 BVerfGE 100, 313 (358); BVerfGE 85, 386 (396); BVerfGE 67, 157 (172).

88 BVerfGE 85, 386 (399).

89 BVerfG seit E 67, 157 (172).

90 Schaar, Sicherheit und Freiheitsrechte (I), 21; Deckers, Geheime Aufklärung (I).

91 Vgl. nur Dreier-Hermes, Art. 10, Rn. 34; J/P6-Jarass, Art. 10, Rn. 7; AK-GG-Bizer, Art. 10, Rn. 64.

92 J/P6-Jarass, Art. 10, Rn. 7: Art. 10 soll in Fällen gelten, in denen die „technische Adressierung" einer Kommunikation nicht ermittelt werden kann, nicht dagegen für öffentliche Inhalte des Internet; Dreier-Hermes, Art. 10, Rn. 36: Es komme entscheidend auf den formalen Anknüpfungspunkt der fernmeldetechnischen Übermittlungsart an; ders., Art. 10, Rn. 35: Es genüge die Möglichkeit, dass auf einem fernmeldetechnischen Übermittlungsweg individuelle Kommunikationsvorgänge stattfinden könnten; ebenso P/S, Rn. 773; Sachs-Krüger, Art. 10, Rn. 14: „Art. 10 scheidet von vornherein aus, wenn der Inhalt einer Nachricht schon von der Art der Übermittlung her für die Öffentlichkeit bestimmt ist."; AK-GG-Bizer, Art. 10, Rn. 64 lässt die Möglichkeit einer individuellen Nutzung von Telekommunikationstechnik genügen; vMKS-Gusy, Art. 10, Rn. 42 f. ist wohl gegen jede Einbeziehung von Massenkommunikation.

93 vMKS-Gusy, Art. 10, Rn. 42.

Die Befürworter einer weiten Auslegung des Art. 10 Abs. 1 Var. 3 GG berufen sich teilweise darauf, dass sich aus der Tatsache, dass ein Internetangebot genutzt wurde, immer auch auf den zugrunde liegenden Telekommunikationsvorgang schließen lässt[94]. Dies allein kann den Ausschlag aber nicht geben, weil Art. 10 Abs. 1 Var. 3 GG nur vor der besonderen Übermittlungsgefahr räumlich distanzierter Kommunikation schützt. So ist beispielsweise die Beschlagnahme von Gesprächsnotizen, die Rückschlüsse auf erfolgte Ferngespräche erlauben, nicht deswegen unzulässig, weil sich die §§ 94 ff. StPO nicht ausdrücklich auf Telekommunikationsvorgänge beziehen (vgl. § 88 Abs. 3 S. 3 TKG)[95]. Bei der Beschlagnahme von Unterlagen eines Kommunizierenden über seine Kommunikation mit anderen handelt es sich nämlich nicht um ein telekommunikationsspezifisches Risiko. Auf die Möglichkeit des Rückschlusses auf einen Telekommunikationsvorgang kann es daher nicht ankommen.

Vertreter der engen Auffassung machen geltend, ein Vertraulichkeitsschutz sei nicht sinnvoll, wenn die Kommunikation von vornherein auf Öffentlichkeit angelegt sei[96]. Dieses Argument kann allerdings nur insoweit Gültigkeit beanspruchen, wie allein der Kommunikationsinhalt von einem Eingriff betroffen ist. An einer Geheimhaltung der personenbezogenen Kommunikationsumstände besteht auch bei öffentlich zugänglichen Informationen ein legitimes Interesse. Bei dem Abruf öffentlicher Therapieinformationen durch eine drogenabhängige Person etwa liegt dies auf der Hand. Aber auch hinsichtlich des Inhalts ist nicht einzusehen, warum man dem Staat nicht zumuten können soll, sich öffentlich zugängliche Informationen wie jeder andere auch selbst zu beschaffen, anstatt sie auf dem Übermittlungsweg abzufangen.

Hinzu kommt, dass eine Trennung von Individual- und Massenkommunikation in den Telekommunikationsnetzen oft nicht möglich ist. Telekommunikationsnetze stellen nämlich technisch gesehen stets punktuelle („point-to-point“) Verbindungen her, meist zwischen genau zwei Telekommunikationsanschlüssen. Bei solchen Punkt-zu-Punkt-Verbindungen ist der technische Adressatenkreis (Telefonnummer, IP-Adresse, E-Mail-Adresse) stets im Voraus bestimmt, so dass es sich hierbei um kein taugliches Abgrenzungskriterium handelt.

Eine Trennung von Individual- und Massenkommunikation ließe sich daher allenfalls durch Kenntnisnahme des Kommunikationsinhalts vornehmen. Bereits dies aber würde dem Schutzzweck des Art. 10 Abs. 1 Var. 3 GG zuwider laufen, da hiermit auch die Kenntnisnahme von – unbestritten geschützter – Individualkommunikation verbunden wäre[97]. Mit dem Argument, lediglich Massenkommunikation zu suchen, könnte der Staat in jeden Kommunikationsvorgang eingreifen, ohne jeglichen Einschränkungen aus Art. 10 Abs. 1 Var. 3 GG – auch verfahrensrechtlicher Art – zu unterliegen.

Hinzu kommt, dass selbst die Kenntnisnahme des Kommunikationsinhalts oftmals keine Abgrenzung von Individual- und Massenkommunikation erlaubt. So kann eine E-Mail individuelle Kommunikation enthalten, aber auch Massenkommunikation, etwa bei so genannten „Newsletters“, die per E-Mail an jeden verschickt werden, der sich für diesen Dienst anmeldet. Derartige Massenkommunikationen können mit personalisierten Elementen verbunden sein, so dass sich aus dem Inhalt einer Nachricht selbst oftmals nicht ersehen lässt, ob der Adressatenkreis bestimmt oder unbestimmt ist. Auch einer übermittelten World Wide Web-Seite sieht man nicht an, ob sie öffentlich zugänglich ist oder nicht: Für manche WWW-Angebote können sich nur bestimmte Personen anmelden (z.B. Mitglieder eines Clubs), und manches Angebot ist deswegen nicht öffentlich, weil der Standort (URL) nur bestimmten Personen mitgeteilt wurde. Aus Kommunikationsinhalt und -umständen geht der Adressatenkreis regelmäßig nicht hervor. Auch dies spricht dafür, öffentlich zugängliche Informationen, die mittels Telekommunikation übertragen werden, in den Schutz des Art. 10 Abs. 1 Var. 3 GG einzubeziehen.

Der Wortlaut des Art. 10 Abs. 1 Var. 3 GG enthält keine Einschränkung in Bezug auf Massenkommunikation, die unter Verwendung von Fernmeldetechnik abgewickelt wird. „Fernmeldegeheimnis“ ist eher technisch formuliert und grenzt die Art der „Fernmeldung“ nicht ein. Als „Meldung“ lässt sich sowohl Individual- als auch Massenkommunikation beschreiben. Historisch wurde die Telegraphen- und Telefontechnik zwar unbestritten nur zur Individualkommunikation eingesetzt. Dies bedeutet aber nicht, dass der Verfassungsgeber die Geltung des Fernmeldegeheimnisses auf Individualkommunikation beschränken wollte.

Teleologisch ist bedeutsam, dass das Fernmeldegeheimnis gerade deswegen in Art. 10 Abs. 1 Var. 3 GG ausdrücklich geschützt ist, weil Eingriffe durch die räumliche Distanz und die Einschaltung des Nachrichtenmittlers besonders leicht zu bewerkstelligen sind. Im Bereich des Internet ist der Bürger

94 Schaar, Datenschutz im Internet, Rn. 141.

95 Schaar, Datenschutz im Internet, Rn. 804; Schenke, AöR 125 (2000), 1 (2 f.); a.A. Graf, Jürgen (Generalbundesanwalt), zitiert bei Neumann, Andreas: Internet Service Provider im Spannungsfeld zwischen Strafverfolgung und Datenschutz, Bericht von der Veranstaltung in Bonn am 26./27.02.2002, www.artikel5.de/artikel/ecoveranstaltung2002. html.

96 vMKS-Gusy, Art. 10, Rn. 42.

97 Germann, 118; allgemein zu diesem Aspekt Gusy, JuS 1986, 89 (90); Dreier-Hermes, Art. 10, Rn. 16 und 35.

aber überall gleichermaßen gefährdet, ob er E-Mails liest oder öffentliche Internetseiten. In beiden Fällen ist er dem geheimen und verhältnismäßig einfachen Zugriff des Staates ausgeliefert.

Mithin erscheint es erforderlich, auch die Inanspruchnahme von Massenmedien mittels Telekommunikation in den Schutz von Art. 10 Abs. 1 Var. 3 GG einzubeziehen. Dabei ist wohlgemerkt der Inhalt öffentlich zugänglicher Informationen als solcher nicht von Art. 10 Abs. 1 Var. 3 GG geschützt, sondern nur die Übermittlung dieses Inhalts an eine ihn abrufende Person sowie die näheren Umstände dieses Abruf- und Übermittlungsvorgangs. Der Staat greift also nur dann nicht in Art. 10 Abs. 1 Var. 3 GG ein, wenn er auf öffentlich zugängliche Informationen wie jeder andere zugreift, etwa mittels eines eigenen Internet-Anschlusses.

Diesen Gedanken verfolgen auch Krüger und Pagenkopf, wenn sie ausführen, der Schutzbereich des Art. 10 Abs. 1 Var. 3 GG sei nicht betroffen, wenn der Staat wie jeder andere auf Informationen zugreifen könne[98]. Der Schutzbereich des Fernmeldegeheimnisses sei nur dann eröffnet, wenn der Wille der Teilnehmer darauf gerichtet sei, einen übertragungssicheren Weg zu nutzen[99]. Auf der Basis dieser richtigen Prämisse gelangen Krüger und Pagenkopf allerdings zu dem unzutreffenden Ergebnis, dass die Kommunikation über das Internet (etwa per E-Mail) nicht von Art. 10 Abs. 1 Var. 3 GG geschützt sei[100]. Dieser Irrtum beruht auf der irrigen Annahme der Autoren, dass die Kommunikation via Internet im Grunde einer öffentlichen Kommunikation mit allgemeiner Teilnahmemöglichkeit entspreche und dass prinzipiell jedermann die Kommunikation einsehen und manipulieren könne[101].

Tatsächlich erfolgt die Nutzung des Internet zwar in der Tat zumeist ohne Verschlüsselung und Authentifizierung der übertragenen Informationen. Dies eröffnet aber nicht jedermann, sondern nur den Kommunikationsmittlern Möglichkeiten der Kenntnisnahme und Manipulation. Dass der Schutzbereich des Art. 10 Abs. 1 Var. 3 GG auch unter diesen Umständen einschlägig ist, zeigt schon die traditionelle Sprachtelefonie, die mit Hilfe eines zwischengeschalteten Lautsprechers ohne Weiteres abhörbar war, und zwar nicht nur für die eingesetzten Telefondienstunternehmen. Im Unterschied hierzu ist die Kenntnisnahme von über das Internet abgewickelten Kommunikationsvorgängen erheblich schwieriger. Im Übrigen können auch verschlossene Briefe durch Einsatz von Wasserdampf zur Kenntnis genommen werden, ohne dass sie deswegen vom Schutzbereich des Briefgeheimnisses ausgenommen wären.

Dass über das Internet abgewickelte Kommunikation unbefugt zur Kenntnis genommen werden kann, führt daher nicht zu einer Einschränkung des Schutzbereichs des Art. 10 Abs. 1 Var. 3 GG. Umgekehrt begründet dieser Umstand eher eine besondere Schutzbedürftigkeit der Internetkommunikation. Der Schutzbereich des Fernmeldegeheimnisses ist bereits dann eröffnet, wenn der Wille der Teilnehmer darauf gerichtet ist, ein regelmäßig übertragungssicheres Medium in Anspruch zu nehmen. Dies ist bei dem Internet der Fall.

(2) Bestandsdaten

Vom Schutzbereich des Fernmeldegeheimnisses erfasst sind auch Angaben über das Telekommunikationsunternehmen, das ein Kunde in Anspruch nimmt, sowie Angaben über die Ausgestaltung des Vertragsverhältnisses (sogenannte Bestandsdaten, z.B. zugewiesene Rufnummer, Anschrift und Geburtsdatum des Kunden). Nur, wenn auch Angaben über das Vertragsverhältnis mit Telekommunikationsunternehmen vor staatlichen Zugriffen geschützt sind, ist eine vertrauliche Inanspruchnahme der Telekommunikation frei von staatlicher Kenntnisnahme gewährleistet. Zur weiteren Begründung wird auf die Ausführungen bei Breyer, RDV 2003, 218 (218 f.) verwiesen, wobei die zentralen Argumente die folgenden sind:

- Bestandsdaten beschreiben die einzelnen Kommunikationsvorgänge näher (z.B. nach dem eingesetzten Unternehmen und den an der Kommunikation Beteiligten) und ermöglichen den staatlichen Zugriff auf Inhalts- und Verkehrsdaten (z.B. durch Überwachungsanordnungen oder durch den unmittelbaren Zugriff auf Mailboxen mittels Zugangscodes).
- Schutzzweck des Fernmeldegeheimnisses ist es, die an der Telekommunikation Beteiligten so zu stellen, wie sie bei unmittelbarer Kommunikation miteinander stünden. Im Fall unmittelbarer Kommunikation aber würden keine Bestandsdaten anfallen und gespeichert werden.

98 Sachs³-Krüger/Pagenkopf, Art. 10, Rn. 14a.
99 Sachs³-Krüger/Pagenkopf, Art. 10, Rn. 14a.
100 Sachs³-Krüger/Pagenkopf, Art. 10, Rn. 14a.
101 Sachs³-Krüger/Pagenkopf, Art. 10, Rn. 14a.

Die relevanten Ausführungen bei Breyer, RDV 2003, 218 (218 f.) lauten im Einzelnen wie folgt:

Verfassungsrechtliche Einordnung

Bestandsdaten sind personenbezogene Daten, die als solche jedenfalls durch das Recht auf informationelle Selbstbestimmung geschützt sind. Dies entspricht dem Schutzzweck dieses Rechts, Grundrechtsträger vor der Gefahr zu schützen, dass der Staat über sie unbegrenzt Kenntnisse sammelt und infolgedessen nachteilige Maßnahmen ihnen gegenüber ergreifen kann. Nicht nur die staatliche Kenntnis von Kommunikationsinhalten oder Verbindungsdaten begründet diese Gefahr. Auch die Kenntnis der Tatsache, dass ein Bürger überhaupt ein vertragliches Verhältnis mit einem bestimmten Diensteanbieter begründet hat und wie dieses ausgestaltet ist, kann zu unerwünschten Kommunikationsanpassungen seitens des Einzelnen führen. Wer beispielsweise an der Teilnahme an einem Internet-Chat für Muslime in Deutschland interessiert ist, wird es in Erinnerung an Maßnahmen der „Anti-Terror-Rasterfahndung“ mit anschließender Befragung der „Ausgefilterten“ möglicherweise vorziehen, auf die Ausübung seiner Grundrechte (hier unter anderem der Religionsfreiheit) zu verzichten. Dasselbe kann etwa für die Anmeldung zur Teilnahme an einem Meinungsforum gelten, in dem Protestaktivitäten gegen die Atomkraft diskutiert werden (Meinungsfreiheit, Versammlungsfreiheit). Auch die Mitgliedschaft in sonstigen geschlossenen Netzen, bereitgestellt etwa von einer Aids-Selbsthilfegruppe, kann Rückschlüsse auf bestimmte Problemlagen erlauben. Dasselbe gilt bereits für Standard-Telekommunikationsdienste. Wer beispielsweise einen Internetzugang zum Pauschaltarif nutzt, wird von den Behörden als intensiver Internetnutzer angesehen werden. Wer bei der deutschen Telefongesellschaft „Alo Vatan“ angemeldet ist, wird im Zweifel einen Bezug zu der Türkei aufweisen. Wer einen bestimmten Optionstarif im Mobilfunknetz nutzt, bei dem man fünf Festnetzanschlüsse vom Handy aus besonders preisgünstig erreichen kann (wird etwa von der Firma Eplus angeboten), gibt schon mit diesen Bestandsdaten preis, mit wem er oft telefoniert. Die genannten Beispiele zeigen, dass Bestandsdaten nicht nur besonders sensibel sein können, sondern auch weit gehende Rückschlüsse auf Inhalt und Umstände einzelner Kommunikationsvorgänge erlauben können.

Fraglich ist, ob Telekommunikations-Bestandsdaten auch durch das Fernmeldegeheimnis (Art. 10 GG) geschützt sind. Einer Einbeziehung von Bestandsdaten in den Schutzbereich des Art. 10 GG steht der Wortlaut „Fernmeldegeheimnis“ zunächst nicht entgegen. Er erlaubt die Auslegung, dass das „Geheimnis“ auch das Vertragsverhältnis umfassen soll, welches den einzelnen Fernmeldevorgängen zugrunde liegt.

Für eine Einbeziehung von Bestandsdaten in den Schutzbereich des Art. 10 GG spricht, dass die Information, welcher Anbieter für die Telekommunikation genutzt wird und wie das Vertragsverhältnis zu diesem Anbieter ausgestaltet ist, die im Rahmen dieses Vertragsverhältnisses abgewickelten Kommunikationsvorgänge inhaltlich näher beschreibt und damit einen näheren Umstand der einzelnen Kommunikationsvorgänge darstellt. Dass das Fernmeldegeheimnis für die näheren Umstände einzelner Kommunikationsvorgänge gilt, ist anerkannt. Bestandsdaten unterscheiden sich von Verbindungsdaten nur dadurch, dass sie die Umstände von Kommunikationsvorgängen stets in gleicher Weise wiedergeben, während sich Verbindungsdaten typischerweise von Verbindung zu Verbindung ändern. Dass darin kein relevanter Unterschied liegt, zeigt aber das Beispiel der Internetnutzung. Während manche Internet-Access-Provider dem Nutzer eine IP-Adresse fest zuweisen (dann Bestandsdatum), teilen andere Dienste dem Nutzer für jede Verbindung eine andere IP-Adresse zu (dann Verbindungsdatum). Solche Zufälligkeiten können für die Bestimmung des Schutzbereichs des Fernmeldegeheimnisses richtigerweise keine Rolle spielen.

Darüber hinaus lässt sich aus der Information, dass eine Person Kunde eines Kommunikationsmittlers ist, regelmäßig schließen, dass der jeweilige Dienst auch in Anspruch genommen wird. Bereits die Tatsache, dass sich jemand des Mediums der Telekommunikation bedient, fällt als „Ob“ der Telekommunikation nach der Definition des Bundesverfassungsgerichts in den

102 OVG Münster, MMR 2002, 563 (564).

103 DSB-Konferenz vom 14./15.03.2000, www.bfd.bund.de/information/info5/anl/an06.html.

104 Vgl. ULD-SH, Sichere Informationsgesellschaft, www.datenschutzzentrum.de/material/themen/cybercri/cyberkon.htm, Punkt 7c.

105 Dafür, soweit Bestandsdaten eine staatliche Überwachung ermöglichen AK-GG-Bizer, Art. 10 Rn. 71; dagegen OVG Münster, MMR 2002, 563 (564); Schaar, Sicherheit und Freiheitsrechte, www.peter-schaar.de/schutzkonzepte.pdf, 21; Kooperationskreis „IuK-Datenschutz“, in: Garstka, Jahresbericht 1998, www.datenschutz-berlin.de/jahresbe/98/teil5.htm, unter 5.3 sowie die h.M.

106 A.A. ohne Begründung Wuermeling/Felixberger, CR 97, 230 (234).

Schutzbereich des Art. 10 GG, wenn das Gericht feststellt, zu den Kommunikationsumständen gehöre „insbesondere, ob, wann und wie oft zwischen welchen Personen oder Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat“. Diese Definition ist bereits ihrem Wortlaut nach nicht auf einzelne Telekommunikationsvorgänge beschränkt.

Hinzu kommt, dass die Kenntnis von Bestandsdaten oftmals Vorbedingung für den staatlichen Zugriff auf einzelne Kommunikationsvorgänge ist. Anbieter von Telekommunikationsdiensten müssen beispielsweise immer auf Bestandsdaten zurück greifen, um dem Staat Auskunft darüber erteilen zu können, welche Personen an einem Kommunikationsvorgang beteiligt waren. In den Aufzeichnungen der Anbieter über einzelne Kommunikationsvorgänge ist nämlich regelmäßig nur ein technisches Merkmal zur Identifizierung der Kunden gespeichert (beispielsweise deren Rufnummer), nicht aber auch deren Name und Anschrift. Auch dieser Zusammenhang spricht dafür, Bestandsdaten in den Schutz des Fernmeldegeheimnisses einzubeziehen.

Schließlich ist der Schutzzweck des Fernmeldegeheimnisses zu beachten, nämlich die an der Telekommunikation Beteiligten so zu stellen, wie sie bei unmittelbarer Kommunikation miteinander stünden. Im Falle der unmittelbaren Kommunikation gäbe es keine Vertragsverhältnisse zu einem Kommunikationsmittler, in deren Rahmen personenbezogene Daten über die an der Kommunikation Beteiligten gespeichert würden. Insoweit realisiert sich das spezifische Risiko für die Vertraulichkeit der Telekommunikation, das mit der Inanspruchnahme von Telekommunikationsdiensten verbunden ist, in der Speicherung von Bestandsdaten bei Kommunikationsmittlern. Bestandsdaten über das Vertragsverhältnis mit Kommunikationsmittlern sind daher nicht nur durch das Recht auf informationelle Selbstbestimmung sondern auch durch das Fernmeldegeheimnis geschützt.

(3) Recht auf informationelle Selbstbestimmung

Das Bundesverfassungsgericht leitet aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG das Grundrecht auf informationelle Selbstbestimmung ab. Es gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte erhoben, gespeichert, verwendet oder weiter gegeben werden[109]. Unerheblich ist, ob dies gerade im Weg automatisierter Datenverarbeitung erfolgt[110]. Ein persönlicher Lebenssachverhalt liegt bereits dann vor, wenn die Verknüpfung des Lebenssachverhalts mit der zugehörigen Person möglich ist[111], wenn also nicht ausgeschlossen werden kann, dass ein Personenbezug zu einem späteren Zeitpunkt einmal hergestellt werden wird[112]. Bei der Frage, ob eine Person bestimmbar ist, sind alle Mittel zu berücksichtigen, die vernünftigerweise von der speichernden Stelle oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen[113].

Sämtliche nach § 110a Abs. 1-4 TKG zu speichernde Daten sind personenbezogen. Soweit also das Gericht das Fernmeldegeheimnis nicht für einschlägig erachten sollte, ist der Schutzbereich des Rechts auf informationelle Selbstbestimmung betroffen.

b) Eingriffstatbestand

Jede staatliche Erhebung, Speicherung, Verarbeitung, Verwendung und Weitergabe von personenbezogenen Informationen stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung[114] und, soweit das Fernmeldegeheimnis einschlägig ist, in Art. 10 Abs. 1 Var. 3 GG[115] dar. Entsprechend diesen Kriterien stellt die staatliche Kenntnisnahme von Telekommunikationsdaten ebenso einen Eingriff in Art. 10 Abs. 1 Var. 3 GG dar wie eine Rechtsnorm, die den Staat zu einer solchen Kenntnisnahme ermächtigt.

107 BVerfGE 100, 313 (358).
108 BVerfGE 85, 386 (396); BVerfGE 100, 313 (363); Gusy, JuS 86, 89 (90 f.); vgl. auch Dreier-Hermes, Art. 10 Rn. 47.
109 St. Rspr. seit BVerfGE 65, 1 (42 f.); in neuerer Zeit etwa BVerfGE 103, 21 (32 f.).
110 BVerfGE 78, 77 (84).
111 BVerfGE 65, 1 (42 und 49); BVerfGE 67, 100 (143); BVerfGE 77, 1 (46); BVerfGE 103, 21 (33); zu Art. 10: BVerfGE 100, 313 (366).
112 Germann, 472.
113 Vgl. Erwägungsgrund 26 der Richtlinie 95/46/EG; a.A. Gola/Schomerus, BDSG, § 3, Rn. 9 zum BDSG: Maßgeblich seien nur die Mittel, die der speichernden Stelle zu Verfügung stehen; ebenso Schaffland/Wiltfang, BDSG, § 3, Rn. 17; Bergmann/Möhrle/Herb, Datenschutzrecht, § 3, Rn. 16.
114 BVerfGE 65, 1 (43) und BVerfGE 103, 21 (33): „Erhebung, Speicherung, Verwendung und Weitergabe“.
115 BVerfGE 85, 386 (398) und BVerfGE 100, 313 (366) für „jede Kenntnisnahme, Aufzeichnung und Verwertung“.

aa) Vorratsspeicherungspflicht als Eingriff

Mit den §§ 110a, 110b TKG greift der Gesetzgeber in Art. 10 Abs. 1 Var. 3 GG ein, weil er Telekommunikationsunternehmen die Pflicht auferlegt, personenbezogene Kommunikationsdaten auf Vorrat zu erheben, zu speichern und für den Abruf durch staatliche Behörden verfügbar zu halten.

Für den Fall einer Auskunftsanordnung nach § 12 FAG (jetzt § 100g StPO) hat das Bundesverfassungsgericht entschieden, dass bereits die gerichtliche Anordnung gegenüber einem Kommunikationsmittler, Telekommunikationsdaten an staatliche Stellen zu übermitteln, einen Eingriff in den Schutzbereich des Fernmeldegeheimnisses darstelle[116]. Bereits die gerichtliche Anordnung ermögliche nämlich die spätere Kenntnisnahme der Telekommunikationsdaten durch staatliche Stellen[117]. Auch eine generelle Vorratsspeicherungspflicht ermöglicht eine spätere staatliche Kenntnisnahme der Daten. Im Unterschied zur gerichtlichen Anordnung steht im Fall einer Vorratsspeicherung allerdings noch nicht fest, dass eine staatliche Kenntnisnahme erfolgen wird. Das Kommunikationsunternehmen wird zunächst nur zur Vorhaltung der Daten verpflichtet.

Nach dem modernen Eingriffsbegriff schützen die speziellen Grundrechte auch vor mittelbaren Eingriffen durch staatliche Maßnahmen, welche die Beeinträchtigung eines grundrechtlich geschützten Verhaltens typischerweise und vorhersehbar zur Folge haben oder die eine besondere Beeinträchtigungsgefahr in sich bergen, die sich jederzeit verwirklichen kann[118]. Auf dieser Linie liegt das Bundesverfassungsgericht, wenn es bereits die einer Kenntnisnahme von Telekommunikation „vorangehenden Arbeitsschritte“ als Eingriff ansieht, soweit es sich nicht um eine rein sachbedingte Speicherung handelt: „Für die Kenntnisnahme von erfassten Fernmeldevorgängen durch Mitarbeiter des Bundesnachrichtendienstes steht folglich die Eingriffsqualität außer Frage. Aber auch die vorangehenden Arbeitsschritte müssen in ihrem durch den Überwachungs- und Verwendungszweck bestimmten Zusammenhang betrachtet werden. Eingriff ist daher schon die Erfassung selbst, insofern sie die Kommunikation für den Bundesnachrichtendienst verfügbar macht und die Basis des nachfolgenden Abgleichs mit den Suchbegriffen bildet. An einem Eingriff fehlt es nur, soweit Fernmeldevorgänge zwischen deutschen Anschlüssen ungezielt und allein technikbedingt zunächst miterfasst, aber unmittelbar nach der Signalaufbereitung technisch wieder spurenlos ausgesondert werden.“[119]

Die Beurteilung einer Vorratsspeicherung von Telekommunikationsdaten kann nicht anders ausfallen[120], denn auch die Speicherung von Telekommunikations-Verkehrsdaten macht diese für eine spätere staatliche Kenntnisnahme verfügbar und birgt damit die latente Gefahr späterer, weiterer Eingriffe. Deswegen stellt eine Vorratsspeicherung auch nicht nur eine „allein technikbedingt[e]“ Miterfassung dar, die keine Spuren hinterlässt und damit jede staatliche Kenntnisnahme ausschließt. Hiervon kann allenfalls die Rede sein, soweit bestimmte auf einen Kommunikationsvorgang bezogene Daten für die Dauer des Vorgangs technikbedingt gespeichert sein müssen. Eine Verpflichtung zur Vorratsspeicherung von Verkehrsdaten über diese Dauer hinaus begründet dagegen die besondere Gefahr, dass der Staat die gespeicherten Daten aufgrund von staatlichen Zugriffsbefugnissen wie den §§ 100g, 100h StPO anfordert. Beeinträchtigungen der von Art. 10 Abs. 1 Var. 3 GG geschützten Vertraulichkeit der Telekommunikation vor dem Staat sind daher die typische und vorhersehbare Folge einer generellen Verkehrsdatenspeicherungspflicht. Damit stellt bereits die Anordnung einer generellen Vorratsspeicherung von Telekommunikations-Verkehrsdaten durch den Normgeber einen staatlichen Eingriff in Art. 10 Abs. 1 Var. 3 GG dar.

Dass sich der Staat zur Speicherung privater Unternehmen bedient, kann keinen Unterschied machen, wenn er sich gleichzeitig den Zugriff auf die gespeicherten Daten eröffnet[121]. Andernfalls könnte der Staat seine Grundrechtsbindung durch ein bloßes „Outsourcing“ umgehen. Die Inanspruchnahme Privater erhöht das Gewicht des Eingriffs sogar noch, weil sich der Kreis von – weitgehend ohne Schuld – beeinträchtigten Personen durch den zusätzlichen Eingriff in Art. 12 GG noch vergrößert. Zudem ist das Risiko, dass gespeicherte Daten missbraucht werden, bei einer Verkehrsdatenspeicherung durch eine Vielzahl von Privatunternehmen erheblich höher einzuschätzen als bei einer staatlichen Speicherung, so dass die Privilegierung einer privaten Vorratsspeicherung auch sachlich nicht gerechtfertigt wäre.

Bereits entschieden hat das Bundesverfassungsgericht, dass die Übermittlung von Telekommunikation an staatliche Stellen durch einen privaten Kommunikationsmittler, der die Telekommunikation auf

116 BVerfGE 107, 299 (313 f.).
117 BVerfGE 107, 299 (314).
118 Windthorst, § 8, Rn. 50 und 52 m.w.N.
119 BVerfGE 100, 313 (366).
120 Ebenso für eine Pflicht zur generellen Speicherung von Telekommunikations-Bestandsdaten unter dem Aspekt des Grundrechts auf informationelle Selbstbestimmung BVerwGE 119, 123 (126).
121 Vgl. Bizer, Forschungsfreiheit, 159 für das „Auf-Abruf-Bereithalten“ von Daten.

gerichtliche Anordnung gemäß § 100a StPO hin aufzeichnet und den staatlichen Stellen verfügbar macht, einen Eingriff in das Fernmeldegeheimnis der an dem Kommunikationsvorgang Beteiligten darstellt[122]. Die Tatsache, dass sich der Staat dabei eines Privaten bediene, sei unerheblich, da der Eingriff hoheitlich angeordnet werde und dem Privaten kein Handlungsspielraum zur Verfügung stehe[123]. Ebenso verhält es sich bei einer Vorratsspeicherungspflicht.

Auch die Bundesregierung sieht das Fernmeldegeheimnis für eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten als einschlägig an[124]. Dass auch der Gesetzgeber von einem Eingriff insoweit ausgehen würde, zeigt sich daran, dass er in § 16b WpHG Art. 10 GG zitiert hat. § 16b WpHG sieht vor, dass unter bestimmten Umständen angeordnet werden kann, dass ein Unternehmen bereits gespeicherte Telekommunikations-Verbindungsdaten aufzubewahren hat. Ob die Behörde die aufbewahrten Verbindungsdaten später tatsächlich anfordert und zur Kenntnis nimmt, steht in diesem Zeitpunkt noch nicht fest. Wie das Zitat des Art. 10 GG zeigt, sieht der Gesetzgeber bereits in dieser vorsorglichen Aufbewahrung von Verkehrsdaten zu staatlichen Zwecken einen Eingriff in die Rechte der an dem Kommunikationsvorgang Beteiligten aus Art. 10 Abs. 1 Var. 3 GG.

Unerheblich für die Einordnung als Eingriff ist auch, ob die betroffenen Unternehmen Verkehrsdaten allein zu staatlichen Zwecken speichern müssen oder ob ihnen zugleich die Nutzung der gespeicherten Daten zu eigenen Zwecken erlaubt ist, etwa zu Abrechnungs- oder Marketingzwecken. In jedem Fall begründet das Bestehen staatlicher Zugriffsrechte die latente Gefahr staatlicher Eingriffe. An dieser Gefahr ändern zusätzliche Nutzungsrechte nichts.

Zu einer abweichenden Beurteilung einer Vorratsspeicherungspflicht gibt auch die Ansicht des Bundesverfassungsgerichts keinen Anlass, dass die so genannte Zielwahlsuche nur einen Eingriff in die Grundrechte derjenigen Personen darstelle, deren Anschlussnummern schließlich an den Staat übermittelt werden[125]. Eine Zielwahlsuche nach § 100g Abs. 2 StPO kann angeordnet werden, wenn ermittelt werden soll, von welchen Anschlüssen aus in einem bestimmten Zeitraum Verbindungen zu einem bestimmten, der Eingriffsbehörde bekannten, anderen Telefonanschluss hergestellt worden sind. Im Fall eines Mordes kann beispielsweise von Interesse sein, welche Personen das Opfer in der letzten Zeit vor seinem Tod angerufen haben. Da Verbindungsdaten bei den Telefongesellschaften geordnet nach der Rufnummer des Anrufers gespeichert werden, ist zur Durchführung einer Suche nach bestimmten Zielrufnummern die Durchsuchung des gesamten Datenbestands der Telefongesellschaft erforderlich. Die letztendlich erteilte Auskunft enthält dann nur die Rufnummern, von denen aus der vorgegebene Anschluss angerufen wurde. Aus ihr lässt sich aber auch entnehmen, dass die Nummer von anderen Telefonanschlüssen aus nicht angerufen wurde. Das Bundesverfassungsgericht sieht einen Grundrechtseingriff in diesem Fall gleichwohl nur bezüglich derjenigen Personen, deren Anschlussnummern schließlich an die Behörden übermittelt werden. Hinsichtlich der übrigen Personen erfolge der Zugriff lediglich maschinell und bleibe anonym, spurenlos und ohne Erkenntnisinteresse für die Strafverfolgungsbehörden, so dass es insoweit an einem Eingriff fehle[126]. Auf den Fall der Vorratsspeicherung übertragen könnte diese Ansicht bedeuten, dass ein Eingriff nur in Bezug auf diejenigen Personen vorläge, deren Daten schließlich an die Behörden übermittelt würden.

Subsumiert man den Vorgang der Zielwahlsuche jedoch unter die anerkannte Definition, der zufolge jede dem Staat zuzurechnende Verarbeitung von Daten, die durch das Fernmeldegeheimnis geschützt sind, einen Eingriff in Art. 10 Abs. 1 Var. 3 GG darstellt[127], so ergibt sich klar, dass ein Eingriff auch in das Fernmeldegeheimnis der unmittelbar nicht von der Auskunft betroffenen Personen vorliegt[128]. Auch ihre Daten werden im Rahmen der Zielwahlsuche nämlich verarbeitet. In einer früheren Entscheidung stellte das Bundesverfassungsgericht ausdrücklich fest, dass die „Prüfung, ob die mittels der Fernmeldeüberwachung erlangten personenbezogenen Daten für die Zwecke, die diese Maßnahmen legitimieren, erforderlich sind, [...] Eingriffsqualität [hat], weil es sich um einen Selektionsakt handelt“[129]. Dass die Verarbeitung im Rahmen der Zielwahlsuche dem Staat zuzurechnen ist, ergibt sich daraus, dass die staatliche Kenntnisnahme der Zweck der Zielwahlsuche ist. Die Eingriffsqualität kann auch nicht davon abhängen, an welchen der übermittelten Daten die Behörde im Zeitpunkt der Übermittlung gerade interessiert sein mag. Woran die Behörde interessiert ist, lässt sich nicht feststellen und kann sich jederzeit ändern. Weiterhin ist auch die Information, wer nicht mit dem Zielanschluss

122 BVerfGE 107, 299 (313 f.).
123 BVerfGE 107, 299 (313 f.).
124 BT-Drs. 14/9801, 14 (15).
125 BVerfGE 107, 299 (328).
126 BVerfGE 107, 299 (313 f.).
127 Seite 23.
128 So offenbar auch BVerwGE 119, 123 (126) für Bestandsdaten und das Recht auf informationelle Selbstbestimmung.
129 BVerfGE 100, 313 (367).

telefoniert hat, nicht unbedingt ohne Erkenntnisinteresse für die Strafverfolgungsbehörden. Denkbar ist beispielsweise der Fall, dass ein Beschuldigter angibt, zum Tatzeitpunkt in einer Kneipe mit einem Freund telefoniert zu haben. Stellt sich durch eine Zielwahlsuche heraus, dass in der fraglichen Zeit zu dem Telefonanschluss des Freundes keine Verbindungen hergestellt wurden, dann ist diese Negativauskunft für die Strafverfolgungsbehörde durchaus von Interesse und wirkt für den Betroffenen auch belastend. Solange einer Behörde das Ergebnis der Zielwahlsuche bekannt ist, kann auch keine Rede davon sein, dass die Daten der nicht unmittelbar Betroffenen „spurlos" ausgesondert würden; der Auskunft lässt sich im Umkehrschluss schließlich jederzeit entnehmen, von welchen Anschlüssen aus keine Verbindungen hergestellt wurden. Auch die Information, dass keine Anrufe erfolgt sind, kann jederzeit in den Mittelpunkt des staatlichen Ermittlungsinteresses geraten. Die Zielwahlsuche stellt somit einen Eingriff in die Grundrechte sämtlicher Anschlussinhaber dar. Der gegenteiligen Ansicht des Bundesverfassungsgerichts kann nicht gefolgt werden, so dass es auf die Bedeutung dieser Ansicht für eine Vorratsspeicherungspflicht nicht ankommt.

bb) Berechtigung Privater zur Vorratsdatenspeicherung als Eingriff

Der Gesetzgeber greift in Art. 10 Abs. 1 Var. 3 GG bereits dadurch ein, wenn er Internet-Telekommunikationsunternehmen bis Herbst 2009 fakultativ das Recht einräumt, Verkehrsdaten länger als für ihre Zwecke erforderlich speichern zu dürfen, und den staatlichen Behörden gleichzeitig den Zugriff auf diese Daten ermöglicht.

Dass eine Speicherung freiwillig erfolgt, ist im Hinblick auf die oben dargestellte Eingriffsdefinition irrelevant, denn auch eine freiwillige Datenspeicherung birgt die latente Gefahr staatlicher Kenntnisnahme, wenn der Staat entsprechende Zugriffsrechte vorsieht. Nur ein Einverständnis der betroffenen Grundrechtsträger würde der Annahme eines staatlichen Eingriffes entgegen stehen, nicht aber das Einverständnis des speichernden Unternehmens. Für das Vorliegen eines Eingriffs in Art. 10 Abs. 1 Var. 3 GG kommt es somit nicht darauf an, ob Kommunikationsmittler zur Datenspeicherung verpflichtet oder nur berechtigt werden.

§ 110a Abs. 1-4 TKG i.V.m. § 150 Abs. 11a TKG ermächtigt Anbieter von Internet-Telefondiensten, von Diensten der elektronischen Post und von Internetzugangsdiensten zur Speicherung von Verbindungsdaten für bis zu sieben Monate lang (vgl. § 110b Abs. 2 TKG). Auf diese Daten können die gesetzlich ermächtigten Behörden zu staatlichen Zwecken zugreifen (etwa nach § 100g StPO), so dass § 110a TKG einen staatlichen Grundrechtseingriff darstellt, wenn er die Speicherung von Verkehrsdaten über die sachlich gebotene Dauer hinaus erlaubt.

Für die Berechnung des Nutzungsentgelts ist eine Speicherung von Verkehrsdaten nur bei kostenpflichtigen Diensten und auch dann nur für kurze Zeit erforderlich. Nach Beendigung eines Nutzungsvorgangs kann unter Einsatz der heute verwendeten Computertechnik das angefallene Entgelt sofort ermittelt und sämtliche Verkehrsdaten sodann gelöscht werden. Dementsprechend sieht § 96 Abs. 2 S. 2 TKG vor, dass nicht benötigte Daten „unverzüglich", also ohne schuldhaftes Zögern, zu löschen sind.

Eine Speicherung von Verkehrsdaten über den Zeitpunkt der Berechnung des Entgelts hinaus könnte zunächst damit gerechtfertigt werden, dass es Telekommunikationsunternehmen möglich sein müsse, diejenigen Benutzer zu identifizieren, die ihre Leistungen in der Absicht in Anspruch nehmen, ihnen das geschuldete Entgelt vorzuenthalten. Es ist allerdings kein Grund ersichtlich, weshalb gerade Telekommunikationsunternehmen Selbsthilferechte eingeräumt werden sollten. Telekommunikationsunternehmen können im Falle des Verdachts einer Straftat (hier § 265a StGB) wie jedes andere Opfer einer Straftat Strafanzeige erstatten und die Ermittlungen den zuständigen Behörden überlassen. Liegen tatsächliche Anhaltspunkte für Leistungserschleichung durch bestimmte Nutzer vor, so kann die Speicherung derer Daten im Einzelfall als erforderlich angesehen werden (vgl. §§ 6 Abs. 8 TDDSG, 19 Abs. 9 MDStV). Eine generelle Speicherung von Verkehrsdaten zur Aufdeckung von Leistungserschleichungen ist jedoch nicht gerechtfertigt.

Teilweise wird unter den Tatbestand der Leistungserschleichung auch illegales Nutzerverhalten subsumiert, das sich nicht gegen den genutzten Dienst, sondern gegen Dritte richtet, etwa die Begehung von Betrug gegenüber einem anderen Internetnutzer unter Inanspruchnahme der Leistungen eines Internet-Providers. Zur Begründung wird darauf verwiesen, dass die meisten Dienste in ihren AGB die Inanspruchnahme des Dienstes zu illegalen Zwecken untersagten[130]. Die Inanspruchnahme eines Dienstes zu illegalen Zwecken führt aber auch aufgrund solcher AGB nicht dazu, dass der Nutzungsvorgang selbst illegal wird, solange das Entgelt dafür entrichtet wird. Wenn es schon in Fällen von Leistungserschleichungen keinen Grund gibt, Telekommunikationsunternehmen Selbsthilferechte

130 LINX, Traceability (I), Punkt 11.2.

einzuräumen, so gilt dies erst recht, wenn die Unternehmen von illegalem Verhalten nicht selbst betroffen sind. Telekommunikationsunternehmen müssen sich also auch hier darauf verweisen lassen, sich wie jeder Andere an die zuständigen Behörden zu wenden. Dies gilt auch für das Argument, Verkehrsdaten müssten aufbewahrt werden, um gestohlene Mobiltelefone mit Hilfe ihrer IMEI-Codes identifizieren zu können[131].

Fraglich ist, ob die Möglichkeit einer Verfolgung vorsätzlicher Angriffe auf die Einrichtungen eines Anbieters, z.B. durch „Hacking", eine generelle Speicherung der Verkehrsdaten aller Kunden rechtfertigt. Zwar müssen dem Anbieter angemessene Maßnahmen zur Gewährleistung des ordnungsgemäßen Betriebs seiner Anlagen zugestanden werden. Insoweit kommen aber zuallererst technische Abwehrmaßnahmen in Betracht. Nur diese sind in der Lage, eine bestimmte Angriffsart dauerhaft und auch gegenüber anderen Nutzern zu unterbinden. Die Identifizierung eines einzelnen Störers wird dagegen regelmäßig nicht erforderlich sein. Jedenfalls genügt es hierzu, im Fall eines Angriffs eine Aufzeichnung von Verkehrsdaten vorzunehmen. Eine generelle Aufzeichnung und Aufbewahrung von Verkehrsdaten ist nicht erforderlich.

Soweit kein vorsätzliches Handeln einzelner Personen im Spiel ist, etwa bei technischen Problemen, kann ebenfalls nicht davon ausgegangen werden, dass zur Gewährleistung der Netzsicherheit, also zur Bereitstellung des Angebots frei von technischen Störungen, die Nutzung personenbezogener Daten erforderlich ist. Insoweit kann allenfalls eine Speicherung technischer Daten in anonymisierter Form gerechtfertigt sein[132]. Das Gleiche gilt für ähnliche Zwecke wie die Beobachtung der Netzauslastung[133], die Erstellung von Fehlerstatistiken, die Überprüfung der Zuverlässigkeit des Dienstes, die Überprüfung der Funktionstüchtigkeit einzelner technischer Elemente eines Dienstes, die Erstellung von Statistiken über die Entwicklung der Leistungsfähigkeit des Dienstes und die Vorhersage von Auslastungsgraden. Es gibt zumutbare technische Mittel zur unwiederbringlichen Anonymisierung von Datenbeständen, deren Einsatz gleichwohl die Nutzbarkeit der Daten zu den genannten Zwecken gewährleistet[134]. Es ist unbefriedigend, dass solche Verfahren nicht in gängige Softwarepakete zur Verwaltung von Verkehrsdaten integriert sind. Ebenso wie die Regierungen eine Erleichterung der Telekommunikationsüberwachung durch die technische Gestaltung von Produkten auf Herstellerebene forcieren[135], müsste auch auf die standardmäßige Berücksichtigung datenschutzfreundlicher Techniken hingewirkt werden.

Eine Speicherung von Verkehrsdaten über den Zeitpunkt der Berechnung des Entgelts hinaus kann somit nur „zu Beweiszwecken für die Richtigkeit der berechneten Entgelte" erforderlich sein. Fraglich ist, ob § 110a TKG die Aufbewahrung von Verkehrsdaten auf das zu Beweiszwecken erforderliche Maß beschränkt. Zunächst ist zu berücksichtigen, dass es im Vergleich zu den insgesamt anfallenden Entgelten nur in wenigen Fällen zu Entgeltstreitigkeiten kommt[136]. Zudem ist die Aufstellung eines Einzelverbindungsnachweises erst seit Einführung der Digitaltechnik Anfang der 90er Jahre möglich. Vor dieser Zeit konnte man Entgeltstreitigkeiten also offenbar auch ohne Einzelverbindungsnachweis hinreichend klären.

Nach gegenwärtiger Rechtslage trifft den Telekommunikationsanbieter keine Beweislast für die Richtigkeit seiner Abrechnung, soweit er Verkehrsdaten gelöscht hat, weil er zur Löschung verpflichtet war (§ 16 Abs. 2 S. 1 TKV)[137]. Mithin kann für die Bemessung der Aufbewahrungsfrist nur das Interesse der Telekommunikationsnutzer maßgeblich sein. Dieses Interesse rechtfertigt es grundsätzlich nicht, Verkehrsdaten allein deswegen zu speichern, weil sie den Nutzungsvorgang im Falle eines Rechtsstreits über angefallene Nutzungsentgelte plausibel machen können[138]. Mit diesem Argument ließe sich sogar eine Inhaltsspeicherung rechtfertigen, weil auch Telekommunikationsinhalte Indizien für die Berechtigung einer Entgeltforderung darstellen können. Für einen Nachweis der Richtigkeit

131 Dazu BfD, 18. Tätigkeitsbericht, BT-Drs. 14/5555, 90.

132 LINX, User Privacy (I), Punkt 7.2.4.

133 LINX, User Privacy (I), Punkt 7.2.5.

134 Nähere Beschreibung bei LINX, User Privacy (I), Punkt 7.4.

135 DG Research, Economic risks arising from the potential vulnerability of electronic commercial media to interception; Weichert, Bekämpfung von Internet-Kriminalität (I).

136 OVG Bremen, NJW 1995, 1769 (1773): „Es ist mit dem verfassungsrechtlichen Maßstab des Übermaßverbotes unvereinbar, Datenspeicherungen in großem Umfang vorzunehmen, nur um Beweiserleichterungen in den am Gesamtvolumen der Entgeltfälle gemessen wenigen Entgeltstreitigkeiten zu erreichen, wenn es technische Möglichkeiten gibt, die den berechtigten Beweisinteressen der Telekom und den berechtigten Verbraucherschutzinteressen ihrer Kunden in angemessener Weise genügen, dabei aber in geringerer Weise in die grundrechtsgeschützte Sphäre des Fernmeldegeheimnisses eingreifen."

137 Vgl. auch Bizer, Telekommunikation und Innere Sicherheit 2000, 505: „Zwar handelt es sich [bei der Sechsmonatsfrist] nur um eine 'kann'-Regelung, jedoch ist unter den TK-Dienstanbietern entgegen § 16 TKV die Meinung verbreitet, eine frühzeitige Löschung führe zu Beweisnachteilen, wenn Kunden die Höhe eines Entgeltes bestreiten."

138 LINX, User Privacy (I), Punkt 7.3.

einer Entgeltforderung wird vielmehr oft die Angabe von Uhrzeit und Dauer eines Gesprächs sowie weniger Ziffern der Anschlussnummer genügen[139].

In Anlehnung an Fristen, die im Geschäftsverkehr beispielsweise zur Prüfung von Kontoauszügen der Banken üblich sind, erscheint grundsätzlich eine vierwöchige Aufbewahrung der für die Berechnung der Entgeltforderung maßgeblichen Daten ausreichend, um den Kunden nach Übersendung einer Rechnung hinreichende Zeit zur Erhebung von Einwendungen zu geben. Wird die Rechnung innerhalb dieses Zeitraums vorbehaltlos beglichen, ist eine Aufbewahrung von Verkehrsdaten nicht mehr erforderlich[140].

Eine Aufbewahrung von Verkehrsdaten ist auch dann nicht erforderlich, wenn der Kunde im Voraus auf Einwendungen gegen Rechnungsforderungen verzichtet. Diesen Gedanken setzt § 97 Abs. 4 TKG nicht um. Verzichtet der Kunde im Voraus auf Einwendungen gegen Rechnungsforderungen, dann ist die Aufbewahrung seiner Verbindungsdaten auch bis zum Versand einer Rechnung nicht erforderlich. Es genügt vielmehr, das angefallene Entgelt sofort nach Beendigung eines Nutzungsvorgangs zu ermitteln und die Verbindungsdaten sodann zu löschen.

§ 110a TKG ist somit auch im Hinblick auf Anbieter von Internet-Telefondiensten, von Diensten der elektronischen Post und von Internetzugangsdiensten als Eingriff in Art. 10 Abs. 1 Var. 3 GG anzusehen, weil er Telekommunikationsunternehmen das Recht einräumt, Verkehrsdaten länger als für ihre Zwecke erforderlich speichern zu dürfen, und den staatlichen Behörden damit auch den Zugriff auf diese Daten ermöglicht.

c) Verfassungsmäßige Rechtfertigung

Aus dem Rechtsstaatsprinzip folgt das Gebot der Verhältnismäßigkeit[141]. Eine Beschränkung von Grundrechten ist danach nur insoweit zulässig, wie sie zur Erreichung des angestrebten Zweckes geeignet und erforderlich ist und der mit ihr verbundene Eingriff seiner Intensität nach nicht außer Verhältnis zur Bedeutung der Sache und den von den Betroffenen hinzunehmenden Einbußen steht[142].

Der Verhältnismäßigkeitsgrundsatz verlangt insbesondere, dass der Verlust an grundrechtlich geschützter Freiheit nicht in einem unangemessenen Verhältnis zu den Gemeinwohlzwecken stehen darf, denen die Grundrechtsbeschränkung dient[143]. Bei einer Gesamtabwägung zwischen der Schwere des Eingriffs und dem Gewicht der ihn rechtfertigenden Gründe muss die Grenze des Zumutbaren noch gewahrt sein[144]. Der Gesetzgeber muss zwischen den Allgemein- und Individualinteressen einen angemessenen Ausgleich herbeiführen[145]. Dabei sind der Grundsatz der grundrechtsfreundlichen Auslegung und die grundsätzliche Freiheitsvermutung zu beachten[146]. Jede Grundrechtsbeschränkung muss durch überwiegende Allgemeininteressen gerechtfertigt sein[147], so dass nicht jedes staatliche Interesse zur Rechtfertigung einer Grundrechtsbeschränkung genügt[148].

Fraglich ist, ob die Abwägung abstrakt anhand des Gewichts der betroffenen Rechtsgüter erfolgen kann. Gegen eine solche Abwägungsmethode sprechen die Schwierigkeiten bei der Bestimmung des Gewichts von Rechtsgütern im Vergleich zueinander. So hat das Bundesverfassungsgericht einerseits festgestellt, dass das Grundgesetz dem Fernmeldegeheimnis hohen Rang zuweise, weil es die freie Entfaltung der Persönlichkeit durch einen privaten, vor den Augen der Öffentlichkeit verborgenen Austausch von Nachrichten, Gedanken und Meinungen (Informationen) gewährleiste und damit die Würde des denkenden und freiheitlich handelnden Menschen wahre[149]. Andererseits hat das Gericht wiederholt[150] die unabweisbaren Bedürfnisse einer wirksamen Strafverfolgung und Verbrechensbekämpfung sowie das öffentliche Interesse an einer möglichst vollständigen Wahrheitsermittlung im Strafprozess betont, die wirksame Aufklärung gerade schwerer Straftaten als einen wesentlichen Auf-

139 LINX, User Privacy (I), Punkt 7.3 für Internet-Access-Provider.
140 Vgl. DSB-Konferenz, Vorratsspeicherung (I).
141 BVerfGE 43, 127 (133); BVerfGE 61, 126 (134); BVerfGE 80, 109 (120).
142 BVerfGE 65, 1 (54).
143 BVerfGE 100, 313 (375 f.).
144 St. Rspr. des BVerfG seit E 4, 7 (15 f.); in neuerer Zeit BVerfGE 78, 77 (85 und 87).
145 BVerfGE 100, 313 (375 f.).
146 BVerfGE 6, 55 (72); BVerfGE 32, 54 (72); BVerfGE 55, 159 (165); BVerfGE 103, 142 (153): „Derjenigen Auslegung einer Grundrechtsnorm ist der Vorrang zu geben, die ihre Wirksamkeit am stärksten entfaltet."
147 St. Rspr. seit BVerfGE 65, 1 (44, 46); in neuerer Zeit etwa BVerfGE 100, 313 (375 f.); BVerfGE 109, 279 (376).
148 EGMR, Klass u.a.-D (1978), EuGRZ 1979, 278 (285), Abs. 49; SächsVerfGH, JZ 1996, 957 (965); IWGDPT, Terrorismus (I); L/D3-Bäumler, J 680: vermutete Nützlichkeit ist ungenügend; Lisken, ZRP 1990, 15 (16): „Es genügt nicht, dass die vom Gesetzgeber auszuwählenden Methoden im Sinne größtmöglicher Verwaltungseffektivität ‚erforderlich' erscheinen."; Minderheitenvotum in BVerfGE 30, 1 (46): „Die ‚Staatsraison' ist kein unbedingt vorrangiger Wert.".
149 BVerfGE 67, 157 (171).
150 Etwa BVerfGE 44, 353 (374) m.w.N.; BVerfGE 46, 214 (222); BVerfGE 77, 65 (76); BVerfGE 80, 367 (375); BVerfGE 103, 21 (33).

trag eines rechtsstaatlichen Gemeinwesens bezeichnet und die Notwendigkeit der Aufrechterhaltung einer funktionstüchtigen Rechtspflege, ohne die der Gerechtigkeit nicht zum Durchbruch verholfen werden könne, hervorgehoben[151]. In einer Entscheidung des Gerichts heißt es dazu: „Die Sicherheit des Staates als verfaßter Friedens- und Ordnungsmacht und die von ihm zu gewährende Sicherheit seiner Bevölkerung sind Verfassungswerte, die mit anderen im gleichen Rang stehen und unverzichtbar sind, weil die Institution Staat von ihnen die eigentliche und letzte Rechtfertigung herleitet.“[152] Gegenüber diesen Interessen der Allgemeinheit komme dem Persönlichkeitsrecht allerdings keine geringere Bedeutung zu[153]. Vielmehr betont das Bundesverfassungsgericht, dass die Überwachung des Fernmeldeverkehrs nicht nur zu Verhaltensanpassungen bei einer Vielzahl einzelner Grundrechtsträger führen könne, sondern auch die freie Kommunikation der Gesellschaft insgesamt gefährde[154]. Eine freie Kommunikation sei „elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens“[155]. Im Ergebnis zeigen diese Ausführungen, dass sich eine Abwägung nicht schon abstrakt auf Rechtsgüterebene vornehmen lässt. Nutzen und Schaden einer Regelung müssen vielmehr im Einzelnen festgestellt und abgewogen werden.

Die aufgezeigten Umschreibungen des Gebots der Verhältnismäßigkeit im engeren Sinne machen deutlich, dass bei der Abwägung der gesamte Verlust an grundrechtlich geschützter Freiheit zu berücksichtigen ist („Gesamtabwägung“). Greift eine Maßnahme also in mehrere Grundrechte ein, so müssen sich die damit verfolgten Gemeinwohlzwecke an dem gesamten Gewicht des Eingriffs messen lassen. Es kann nicht richtig sein, die Verhältnismäßigkeit nur für jedes Grundrecht gesondert zu prüfen und dadurch die verfolgten Gemeinwohlzwecke mehrfach in die Waagschale zu werfen. Daraus folgt, dass sich die Unverhältnismäßigkeit einer Regelung auch erst aus der Summe ihrer nachteiligen Wirkungen auf verschiedene Grundrechte ergeben kann.

(a) Gewichtung der geförderten Interessen

Auf Seiten der Gemeinwohlinteressen ist für die Abwägung das Gewicht der Ziele und Belange maßgeblich, denen die Grundrechtsbeschränkung dient. Bei deren Gewichtung kommt es unter anderem darauf an, wie groß die Gefahren sind, denen mit Hilfe der Eingriffe begegnet werden soll, und wie wahrscheinlich deren Eintritt ist[156]. Die Gewährleistung der physischen Integrität von Personen rechtfertigt weiter gehende Freiheitseingriffe als die Verfolgung nur sozialer oder ökonomischer Ziele[157]. Wenn der Allgemeinheit eine Gefahr droht, sind weitergehende Eingriffe zulässig, als wenn es nur um die Rechtsgüter Einzelner geht[158]. Neben dem Gewicht der Belange, denen eine Grundrechtsbeschränkung dient, kann auch das Maß an Eignung der Grundrechtsbeschränkung zur Förderung dieser Belange für die Frage ihrer Angemessenheit nicht ohne Bedeutung sein. Mit dem Schutzzweck der Grundrechte ließe es sich nämlich nicht vereinbaren, wenn eine kaum effektive, aber mit schwerwiegenden Grundrechtsbeschränkungen verbundene Norm alleine deshalb als verhältnismäßig anzusehen wäre, weil sie in seltenen Fällen dem Schutz höchster Gemeinschaftsgüter dienen kann.

(b) Gewichtung der beeinträchtigten Interessen

Das Gewicht eines Eingriffs bemisst sich der Rechtsprechung des Bundesverfassungsgerichts zufolge danach, unter welchen Voraussetzungen Eingriffe zulässig sind, welche und wie viele Grundrechtsträger von ihnen betroffen sind und wie intensiv die Grundrechtsträger beeinträchtigt werden[159]. Zu berücksichtigen ist auch, ob und in welcher Zahl Personen mitbetroffen werden, die für den Eingriff keinen Anlass gegeben haben[160]. Die Eingriffsintensität hängt bei Informationseingriffen unter anderem von Art, Umfang und denkbaren Verwendungen der erhobenen Daten sowie von der Gefahr ihres Missbrauchs ab[161]. Bei der Feststellung der Möglichkeiten zur Verwendung erlangter Daten ist zu berücksichtigen, ob die Betroffenen anonym bleiben und welche Nachteile ihnen aufgrund der Maßnahmen drohen oder von ihnen nicht ohne Grund befürchtet werden[162]. Bei der Gewichtung möglicher Nachteile ist die Nutzbarkeit und Verwendungsmöglichkeit der Daten maßgeblich, und zwar unter

151 Nachweise bei BVerfGE 34, 238 (248 f.).
152 BVerfGE 49, 24 (56 f.).
153 BVerfGE 85, 367 (375); BVerfGE 106, 28 (49).
154 BVerfGE 100, 313 (381).
155 BVerfGE 65, 1 (43).
156 BVerfGE 100, 313 (376).
157 Callies, ZRP 2002, 1 (7).
158 Ossenbühl, Tatsachenfeststellungen und Prognoseentscheidungen, 509.
159 BVerfGE 109, 279 (353).
160 BVerfGE 109, 279 (353).
161 BVerfGE 65, 1 (46).
162 BVerfGE 100, 313 (376).

besonderer Berücksichtigung der Möglichkeit, dass die Daten mit anderen Daten kombiniert und dadurch weitergehende Kenntnisse gewonnen werden können[163].

Für die Beurteilung der Verhältnismäßigkeit sind primär die rechtlich zulässigen Verwendungsmöglichkeiten maßgeblich. Einzubeziehen sind aber auch die sonstigen, tatsächlich und technisch vorhandenen Verwendungsmöglichkeiten. Dies ist einerseits vor dem Hintergrund erforderlich, dass sich die rechtlichen Grenzen des staatlichen Zugriffs vergleichsweise leicht erweitern lassen, nachdem die grundsätzliche Zugriffsmöglichkeit erst einmal eingeführt und die erforderliche Überwachungsstruktur aufgebaut worden ist[164]. Die unzählige Male vorgenommene Ausweitung des Straftatenkatalogs in § 100a StPO zeigt, wie wahrscheinlich eine solche Entwicklung auch in anderen Bereichen ist. Zum anderen ist auch an die Gefahr eines illegalen Missbrauchs zu denken, gerade dort, wo dieser nur schwer zu bemerken ist. Zwar ist, was den Staat selbst angeht, die bloß abstrakte Möglichkeit eines Missbrauches, das heißt unbegründete Befürchtungen dahin gehend, nicht zu berücksichtigen, weil grundsätzlich davon auszugehen ist, dass eine Norm „in einer freiheitlich-rechtsstaatlichen Demokratie korrekt und fair angewendet wird“[165]. Eine reale Missbrauchsgefahr ist im Rahmen der Abwägung demgegenüber durchaus zu berücksichtigen[166]. Die Grundrechte schützen den Einzelnen nämlich auch „vor fehlerhafter, mißbräuchlicher oder exzessiver Verwertung von Kommunikationsdaten durch [...] staatliche Stellen“[167]. Die „in der Gesprächsbeobachtung liegende Gefahr einer Grundrechtsverletzung der [...] Gesprächsteilnehmer wie auch die Gefahr der Sammlung, Verwertung und Weitergabe der Informationen zu anderen Zwecken“ als den gesetzlich vorgesehenen darf daher nicht aus den Augen verloren werden[168]. Wenn das Fernmeldegeheimnis das unbefangene Gebrauchmachen von Grundrechten in einer Demokratie schützen soll, dann darf außerdem nicht unberücksichtigt bleiben, dass sich der einzelne Bürger bei seinen Entscheidungen weniger durch die Feinheiten der Gesetzesformulierung beeindrucken lassen wird als vielmehr durch seine Eindrücke, Emotionen und Befürchtungen. Dementsprechend kommt es im Rahmen der Abwägung auch nicht nur darauf an, welche Nachteile den Grundrechtsträgern konkret aufgrund der Überwachungsmaßnahmen drohen. Ebenso zu berücksichtigen sind entferntere Risiken, deren Eintritt von den Bürgern nicht ohne Grund befürchtet wird[169]. Das Gewicht drohender oder befürchteter Nachteile in der Abwägung hängt dabei unter anderem von der Wahrscheinlichkeit des Eintritts eines Schadens und von dessen potenziellem Ausmaß ab.

Auf die Frage, inwieweit von einer gesetzlichen Eingriffsermächtigung tatsächlich Gebrauch gemacht wird, kann es bei der Beurteilung der Eingriffsintensität richtigerweise nicht ankommen[170], weil eine Vollzugspraxis jederzeit geändert werden kann[171] und weil der Gesetzgeber verpflichtet ist, die wesentlichen Eingriffsgrenzen selbst zu regeln. Eine Verwaltungspraxis ist für die Betroffenen regelmäßig nicht vorhersehbar und daher bei der Verhältnismäßigkeitsprüfung ohne Bedeutung[172]. Zwar entspricht es der Eigenart von Rechtsnormen, dass diese bis zu einem gewissen Grad allgemein gehalten sind. Nichtsdestotrotz muss der Gesetzgeber eine Norm jedenfalls dann eingrenzen, wenn sie ansonsten in abstrakt umschreibbaren Fallgruppen zu Eingriffen ermächtigen würde, in denen der Verhältnismäßigkeitsgrundsatz durchweg verletzt würde[173]. Dem Bundesverfassungsgericht ist daher entgegenzutreten, wenn es bei der Bestimmung des Gewichts eines Eingriffs damit argumentiert, dass dieser „sowohl rechtlich als auch tatsächlich begrenzt“[174] sei.

Daneben ist zu beachten, dass rechtliche oder tatsächliche Begrenzungen gesetzlicher Eingriffsermächtigungen die Eignung der Maßnahme für den angestrebten Zweck beeinträchtigen können, etwa wenn eine Überwachungsmaßnahme nur einen Teil aller Kommunikationsvorgänge erfasst. Gerade wo vorhersehbar ist, welche Kommunikationsvorgänge nicht erfasst werden, bieten sich Schlupflöcher, die

163 BVerfGE 65, 1 (45).

164 Vgl. Dembart, Lee: The End User Privacy undone, International Herald Tribune, 10.06.2002, coranet.radicalparty.org/-pressreview/print_250.php?func=detail&par=2477 über die Vorratsspeicherung von Verkehrsdaten, die ursprünglich als Maßnahme gegen den Terrorismus dargestellt wurde: „As surely as night follows day, law enforcement will use that database to investigate things other than terrorism.“ Vgl. auch Kaleck, Wolfgang u.a.: Stellungnahme von Bürgerrechtsorganisationen zur Anhörung des Innenausschusses des Deutschen Bundestages am 30.11.2001 zum Entwurf eines Gesetzes zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz), www.cilip.de/terror/atg-stell-281101.pdf, 5; Ruhmann/Schulzki-Haddouti, Abhör-Dschungel (I).

165 BVerfGE 30, 1 (27).

166 BVerfGE 65, 1 (45 f.).

167 BVerfGE 85, 386 (397).

168 BVerfGE 85, 386 (400).

169 BVerfGE 100, 313 (376).

170 MVVerfG, LKV 2000, 149 (154); AK-GG-Bizer, Art. 10, Rn. 86; a.A. wohl BVerfGE 100, 313 (376 ff.).

171 Vgl. BVerfGE 100, 313 (380).

172 EGMR, Khan-GB (2000), Decisions and Reports 2000-V, Abs. 27.

173 Vgl. BVerfGE 100, 313 (384 f.).

174 BVerfGE 100, 313 (376).

insbesondere von denjenigen genutzt werden, die ein Maximum an krimineller Energie aufwenden und denen die Regelung daher zuvörderst gilt[175]. Eine solchermaßen reduzierte Eignung geht zu Lasten der Verhältnismäßigkeit einer Maßnahme und kann schwerer wiegen als der Nutzen einer Begrenzung. Insgesamt sind Begrenzungen daher differenziert zu beurteilen.

(c) Unsicherheitssituationen

Die Prüfung der Verhältnismäßigkeit der Vorratsdatenspeicherung wird durch Unsicherheiten tatsächlicher Art erschwert. Wenn entweder schon die gegenwärtige Sachlage unbekannt ist oder aber sich zukünftige Entwicklungen nicht sicher abschätzen lassen, ist die Anwendung des Verhältnismäßigkeitsprinzips nicht ohne weiteres möglich. Bei der Überprüfung der Verfassungsmäßigkeit von Gesetzen gebietet es das Demokratieprinzip (Art. 20 Abs. 1 GG), dass der demokratisch gewählte und verantwortliche Gesetzgeber das letzte Wort haben muss und nicht das Bundesverfassungsgericht. Dem Gesetzgeber kommt in Unsicherheitssituationen also ein Einschätzungsspielraum zu[176]. Innerhalb gewisser Grenzen obliegt ihm die Entscheidung, in welchem Umfang er Anstrengungen zur Aufklärung der maßgeblichen Tatsachen unternimmt und, soweit er von einer Aufklärung absieht oder eine Klärung nicht möglich ist, von welchen Tatsachen und zukünftigen Entwicklungen er für seine Entscheidung ausgeht.

Der Einschätzungsspielraum des Gesetzgebers bezieht sich wohlgemerkt nur auf Tatsachen und nicht auf Rechtsfragen[177]; die letztverbindliche Auslegung und Anwendung des Rechts obliegt nach der Kompetenzordnung des Grundgesetzes den Gerichten und nicht dem Gesetzgeber. Daraus folgt, dass der Gesetzgeber das Vorliegen rechtlicher Merkmale, etwa der Eignung einer Norm, nicht einfach annehmen darf. Sein Einschätzungsspielraum ist erst dann einschlägig, wenn er konkrete Annahmen über Tatsachen macht. Erst diese Tatsachen können dann den Rechtsbegriff ausfüllen, also beispielsweise die Eignung der Norm begründen.

Wie weit der Einschätzungsspielraum des Gesetzgebers reicht, hängt einerseits von den verfügbaren Möglichkeiten der Bildung eines sicheren Urteils ab[178]. Diese sind reduziert, wenn ein Sachgebiet raschen Veränderungen unterliegt oder der Regelungsgegenstand komplex und schwer überschaubar ist[179]. Daneben sind für die Bemessung des Einschätzungsspielraums auch das Gewicht der auf dem Spiel stehenden Rechtsgüter[180] und, bei Grundrechtseingriffen, die Eingriffsintensität maßgeblich[181]. Während zumutbare, schon vor Normerlass bestehende Aufklärungsmöglichkeiten sowie hohe aufgrund einer Norm drohende Belastungen den Handlungsspielraum des Gesetzgebers reduzieren, eröffnen ihm wahrscheinliche Gefahren für wichtige Rechtsgüter einen erweiterten Handlungsspielraum. Äußere oder vom Gesetzgeber zu vertretende Umstände wie Zeitnot oder unzureichende Beratung begründen keine Einschätzungsspielräume des Gesetzgebers[182].

Mit dem variablen Einschätzungsspielraum des Gesetzgebers korrespondiert ein variabler Maßstab bei der verfassungsrechtlichen Prüfung. Teilweise hat es das Bundesverfassungsgericht genügen lassen, wenn die Einschätzung des Gesetzgebers nicht evident unzutreffend war[183], etwa wo es um den Grundlagenvertrag mit der DDR[184] oder um das Weinwirtschaftsgesetz[185] ging. Bei Eingriffen niedriger Intensität ist der Gesetzgeber auch nicht zu tatsächlichen Feststellungen verpflichtet[186]. In Fällen von größerem Gewicht hat das Bundesverfassungsgericht verlangt, dass die Einschätzung des Gesetzgebers vertretbar sein müsse[187]. Insoweit sei erforderlich, dass der Gesetzgeber durch Ausschöpfung der ihm zugänglichen Erkenntnisquellen[188] die maßgeblichen gegenwärtigen und vergangenen Tatsachen möglichst vollständig ermittele[189], um eine möglichst zuverlässige Einschätzung treffen zu können[190]. Auf welche Weise der Gesetzgeber die maßgeblichen Tatsachen feststellt, ist grundsätzlich ihm

175 Germann, 325.
176 St. Rspr. des BVerfG seit E 50, 290 (332 f.); in neuerer Zeit etwa BVerfGE 90, 145 (173); ebenso für den Verordnungsgeber BVerfGE 53, 135 (145) und BVerfG, NJW 2002, 1638 (1639).
177 Baumeister, Das Rechtswidrigwerden von Normen, 235 ff.
178 BVerfGE 50, 290 (332 f.); BVerfGE 57, 139 (159); BVerfGE 62, 1 (50); BVerfGE 106, 62 (152).
179 BVerfGE 50, 290 (333); BVerfGE 106, 62 (152).
180 BVerfGE 50, 290 (333); BVerfGE 106, 62 (152).
181 BVerfGE 90, 145 (173).
182 BVerfGE 106, 62 (152).
183 BVerfGE 36, 1 (17); BVerfGE 40, 196 (223).
184 BVerfGE 36, 1 (17 f.).
185 BVerfGE 37, 1 (20 f.).
186 BVerfGE 88, 203 (310).
187 BVerfGE 25, 1 (12 f. und 17); BVerfGE 39, 210 (225 f.).
188 BVerfGE 50, 290 (333 f.).
189 BVerfGE 106, 62 (151).
190 BVerfGE 50, 290 (334).

überlassen[191]. Von dem Vertretbarkeitsmaßstab ist das Bundesverfassungsgericht etwa im Volkszählungsurteil ausgegangen[192]. Wo es um zentrale Rechtsgüter wie die Gesundheit oder Freiheit einer Person ging, hat das Gericht schließlich eine eigene und intensive inhaltliche Kontrolle vorgenommen[193]. Dieser Maßstab wurde auch bei Gesetzen angewandt, welche die freie Berufswahl einschränkten[194].

Zu beachten ist, dass die unterschiedliche Kontrollintensität auf den beiden letztgenannten Stufen nur quantitativer Art ist[195], weswegen die Bedeutung der Unterscheidung zwischen diesen beiden Stufen nicht überbewertet werden darf. Der Prüfungsmaßstab unterscheidet sich lediglich in den unterschiedlichen Anforderungen, die an die Eindeutigkeit des Prüfungsergebnisses gestellt werden[196]. Auch die Dogmatik zu Art. 3 Abs. 1 GG unterscheidet nur zwischen einer Willkürprüfung einerseits und einer Verhältnismäßigkeitsprüfung andererseits, was dafür spricht, dies im Bereich anderer Grundrechte ebenso zu handhaben.

In dem aufgezeigten Rahmen ist der Gesetzgeber zur Feststellung aller gegenwärtigen und vergangenen Tatsachen verpflichtet, von denen die Verfassungsmäßigkeit eines Gesetzes abhängt[197]. Diese Pflicht des Gesetzgebers ist aus dem Rechtsstaatsprinzip herzuleiten[198], aus dem sich auch weitere Eingriffsgrenzen ergeben: Schon das allgemeine Verwaltungsrecht folgert aus dem Rechtsstaatsprinzip, dass Eingriffe der Verwaltung vor der vollständigen Ermittlung des Sachverhalts nur ausnahmsweise gerechtfertigt sind[199]. Auch auf dem Gebiet des Polizeirechts entnimmt man dem Rechtsstaatsprinzip, dass in Fällen von Gefahrenverdacht grundsätzlich nur vorläufige Eingriffe zulässig sind, die keinen irreparablen Schaden anrichten und die allein der Gefahrenerforschung dienen dürfen[200]. Diese Grundgedanken müssen auch für Maßnahmen des Gesetzgebers gelten, für den das Rechtsstaatsprinzip ebenso verbindlich ist[201]. In Unsicherheitssituationen sind irreparable Grundrechtseingriffe durch den Gesetzgeber daher grundsätzlich erst dann zulässig, wenn der Gesetzgeber die ihm zugänglichen Erkenntnisquellen ausgeschöpft und die maßgeblichen gegenwärtigen und vergangenen Tatsachen möglichst vollständig ermittelt hat[202]. Insofern tritt von Verfassungs wegen eine „Beweislastumkehr“ ein, der zufolge der Gesetzgeber die Verfassungsmäßigkeit einer geplanten Norm nachweisen muss, bevor er sie erlassen darf[203]. Nur unter außergewöhnlichen Umständen können Sofortmaßnahmen ohne die an sich erforderliche Aufklärung des Sachverhalts zulässig sein, nämlich wenn die Maßnahme zum Schutz wichtiger Rechtsgüter vor dringenden und hinreichend wahrscheinlichen Gefahren, hinter welche die beeinträchtigten Rechtspositionen zurücktreten müssen, erforderlich ist.

Ein Hauptanwendungsfall eines gesetzgeberischen Einschätzungsspielraums stellt die Eignung einer Norm zur Erreichung ihres Zwecks beziehungsweise das Maß an Eignung der Norm dar. Ist die Effektivität einer Regelung im Zeitpunkt ihres Erlasses noch nicht absehbar, dann ist dem Normgeber grundsätzlich die experimentelle Einführung der Regelung gestattet, wenn dies zur Gewinnung gesicherter Erkenntnisse über ihre Effektivität erforderlich ist[204]. Allerdings muss die begründete Erwartung der Effektivität der Regelung bestehen[205]. Auch ist das allgemeine Verhältnismäßigkeitsprinzip zu beachten, das der experimentellen Einführung einer Norm entgegen stehen kann. Überdies bleibt es

191 BVerfGE 106, 62 (151).
192 BVerfGE 65, 1 (55 f.).
193 BVerfGE 7, 377 (415); BVerfGE 45, 187 (238).
194 Etwa BVerfGE 7, 377.
195 Chryssogonos, Verfassungsgerichtsbarkeit und Gesetzgebung, 187.
196 Chryssogonos, Verfassungsgerichtsbarkeit und Gesetzgebung, 187.
197 BVerfGE 106, 62 (150).
198 Zur Ableitung von Verhaltenspflichten des Gesetzgebers aus dem Rechtsstaatsprinzip Köck, VerwArch 93 (2002), 1 (15 und 18) m.w.N.
199 Stelkens/Bonk/Sachs-Stelkens/Stelkens, § 35, Rn. 175.
200 L/D3-Denninger, E 38; Schenke, Polizei- und Ordnungsrecht, Rn. 86 f.
201 Vgl. auch Ossenbühl, Tatsachenfeststellungen und Prognoseentscheidungen, 486: Bei zweifelhafter tatsächlicher Basis müsse der Gesetzgeber von Eingriffen absehen, „in dubio pro libertate“; ders., 487: Verfassungsrechtlich sei „eine verlässliche empirischen Basis“ für einen Eingriff erforderlich, weil die Dispositionsfreiheit des Gesetzgebers lediglich im Bereich der Wertung, nicht aber im Bereich der Tatsachenfeststellung liege.
202 Vgl. schon Seite 31.
203 Lisken, ZRP 1990, 15 (16): Vorfeldbefugnisse müssten „unabweisbar, also nachweislich, für den Grundrechtsschutz notwendig“ sein; Bürgerrechtsorganisationen: Die falsche Antwort auf den 11. September: Der Überwachungsstaat, Presseerklärung vom 24.10.2001, www.cilip.de/terror/pe241001.htm; Kaleck, Wolfgang u.a.: Stellungnahme von Bürgerrechtsorganisationen zur Anhörung des Innenausschusses des Deutschen Bundestages am 30.11.2001 zum Entwurf eines Gesetzes zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz), www.cilip.de/terror/-atg-stell-281101.pdf, 6; Ossenbühl, Tatsachenfeststellungen und Prognoseentscheidungen, 486.
204 SächsVerfGH, DuD 1996, 429 (435) für die Erhebung personenbezogener Daten zur Gefahrenabwehr unter verdeckter Anwendung technischer Mittel.
205 SächsVerfGH, DuD 1996, 429 (435) für die Erhebung personenbezogener Daten zur Gefahrenabwehr unter verdeckter Anwendung technischer Mittel.

dabei, dass die bereits vor Einführung der Norm zugänglichen Erkenntnisquellen vorab ausgeschöpft werden müssen, um die Eignung der Norm möglichst zuverlässig prognostizieren zu können.

Allgemein gilt für Prognosen über zukünftige Tatsachen folgendes: Die oben genannten Grundsätze bezüglich der Feststellung gegenwärtiger und vergangener Tatsachen gelten uneingeschränkt auch für die Feststellung derjenigen gegenwärtigen und vergangenen Tatsachen, die einer Prognose über zukünftige Tatsachen zugrunde liegen[206]. Hinsichtlich des angewandten Prognoseverfahrens hat das Bundesverfassungsgericht entschieden, dass es sich um ein angemessenes Verfahren handeln muss, dass das gewählte Verfahren konsequent verfolgt werden muss, dass in die Prognose keine sachfremden Erwägungen einfließen dürfen und dass das Prognoseergebnis ein vertretbares Resultat des Prozesses darstellen muss[207]. Was die Richtigkeit des Prognoseergebnisses anbelangt, so liegt es in der Natur der Sache, dass sich selbst die beste Prognose im zeitlichen Verlauf als falsch erweisen kann. Dieses Risiko kann einem Handeln des Gesetzgebers nicht von vornherein entgegen stehen, weil ein Nichthandeln des Gesetzgebers noch größere Risiken bergen kann. Soweit also das Prognoseergebnis nicht bereits durch gesicherte empirische Daten oder verlässliche Erfahrungssätze vorgeben ist[208], greift in Bezug auf das Prognoseergebnis wieder der oben aufgezeigte, variable Einschätzungsspielraum des Gesetzgebers ein[209].

(d) Angemessenheit einer generellen Vorratsspeicherung von Telekommunikations-Verkehrsdaten

Im Rahmen der Prüfung der Angemessenheit einer generellen Vorratsspeicherung von Telekommunikations-Verkehrsdaten kommt es auf eine Reihe von Tatsachen an, bezüglich derer erhebliche tatsächliche Unsicherheiten bestehen, etwa im Hinblick auf die Auswirkungen einer solchen Regelung. Aus diesem Grund fragt sich, welcher Einschätzungsspielraum dem Gesetzgeber insoweit zusteht.

Es ist zunächst nicht ersichtlich, dass der maßgebliche Sachverhalt raschen Veränderungen unterliegen könnte oder besonders komplex oder schwer überschaubar wäre. Eine Aufklärung der maßgeblichen Tatsachen ist bereits vor Einführung einer Vorratsspeicherung in vielerlei Hinsicht möglich und zumutbar, vor allem was das Maß an Eignung einer Vorratsspeicherung anbelangt. Eine Vorratsspeicherung von Verkehrsdaten würde im Wesentlichen nur eine quantitative Ausweitung der bestehenden Zugriffsbefugnisse auf Telekommunikations-Verkehrsdaten bewirken (z.B. § 100g StPO), weil eine größere Menge an Verkehrsdaten als bisher gespeichert würde. Dies macht es möglich, auch ohne die experimentelle Einführung einer Vorratsspeicherung deren mögliche Wirksamkeit zu überprüfen, indem man die zuständigen Behörden festhalten lässt, in wie vielen und in welchen Fällen ein Auskunftsersuchen daran scheitert, dass die gewünschten Daten nicht oder nicht mehr verfügbar sind. Anhand dieser Statistik ließe sich überprüfen, in wie vielen Fällen eine Vorratsspeicherung Abhilfe hätte schaffen können[210]. Die Aussagekraft der Statistik wäre weiter zu verbessern, indem auch der Anlass des Auskunftsersuchens registriert wird. Damit ließe sich überprüfen, ob es in einer erheblichen Anzahl von Fällen schwerer Kriminalität an Verkehrsdaten fehlt.

Auch mit Blick auf die Frage, inwieweit eine Vorratsspeicherung tatsächlich zur Abwehr von Gefahren oder zu strafgerichtlichen Verurteilungen führen könnte, ließen sich bereits durch die Evaluierung der bestehenden Befugnisse wichtige Anhaltspunkte gewinnen. Da die Einführung einer Vorratsspeicherung im Wesentlichen eine quantitative Ausweitung dieser Befugnisse zur Folge hätte, kann man davon ausgehen, dass der Anteil erfolgreicher Auskunftsersuchen im Falle einer generellen Vorratsspeicherung jedenfalls nicht niedriger liegen würde als bisher.

Die Evaluierung der bisher bestehenden Befugnisse für den Zugriff auf Telekommunikations-Verkehrsdaten müsste dazu freilich in Angriff genommen werden, was bisher – wie bei fast allen informationell eingreifenden Ermittlungsmaßnahmen – versäumt worden ist[211]. Während bereits im Bereich der Telekommunikationsüberwachung nach § 100a StPO vielfach beklagt wird, dass empirische kriminalistische Daten weitgehend unbekannt sind[212], existieren im Bereich des isolierten Zugriffs auf Verkehrsdaten bisher augenscheinlich keinerlei Statistiken[213].

206 BVerfGE 106, 62 (150 f.).
207 BVerfGE 106, 62 (152 f.).
208 BVerfGE 106, 62 (151).
209 BVerfGE 106, 62 (152).
210 Entsprechende Untersuchungen fordert auch ISPA, Internet Service Providers' Association (UK): Memorandum by the Internet Services Providers' Association (ISPA), 19 November 2001, www.parliament.the-stationery-office.co.uk/pa/-cm200102/cmselect/cmhaff/351/351ap10.htm.
211 Weichert, Bekämpfung von Internet-Kriminalität (I), Punkt 7.
212 Welp, TKÜV, 3 (7).
213 Fox, DuD 2002, 194 (194).

Von der nationalen Ebene abgesehen existieren auf internationaler Ebene geradezu ideale Bedingungen für eine Evaluierung dadurch, dass einige EU-Staaten eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten bereits eingeführt haben und andere dies in Kürze zu tun beabsichtigen[214]. Dies macht es möglich, sowohl im zeitlichen Vergleich innerhalb dieser Staaten wie auch im Vergleich mit Staaten ohne Vorratsspeicherung zu überprüfen, inwieweit die Vorratsspeicherung den Gefahrenabwehr- und Strafverfolgungsbehörden tatsächlich hilft, in wie vielen und welchen Fällen die Vorratsspeicherung für die Gefahrenabwehr oder Strafverfolgung letztlich wesentlich war, ob es den Strafverfolgungsorganen gelungen ist, in die Reihe der Hintermänner organisierter Kriminalität einzudringen, und ob die Einführung der Vorratsspeicherung insgesamt eine spürbare Senkung des Kriminalitätsniveaus herbei geführt hat. Im Bereich der Netzkriminalität im engeren Sinne ließe sich als Indikator etwa die Aufklärungsquote in Bezug auf diese Delikte heranziehen. Diese Quote wird in den meisten Staaten ohnehin ermittelt und müsste einige Zeit nach der Einführung einer Vorratsspeicherung von Telekommunikations-Verkehrsdaten merklich ansteigen, wenn dieser Mechanismus tatsächlich effektiv sein sollte. In die Evaluierung ließen sich auch die negativen Effekte einer generellen Vorratsspeicherung von Telekommunikations-Verkehrsdaten einbeziehen, soweit sie offen zutage treten, etwa Standortverlagerungen von Firmen oder Preiserhöhungen.

Eine Vorratsspeicherung von Telekommunikationsdaten stellt einen empfindlichen Eingriff in die Privatsphäre der Betroffenen dar, weil die Kenntnis von Verkehrsdaten große Verknüpfungs- und Verwendungsmöglichkeiten eröffnet und dementsprechend einschneidende Folgen für die Betroffenen haben kann. Eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten würde dazu führen, dass es unbeobachtete Telekommunikation grundsätzlich nicht mehr gäbe. Sie rückt damit in die Nähe einer Antastung des Wesensgehaltes des Fernmeldegeheimnisses nach Art. 10 Abs. 1 Var. 3 GG und ist äußerst belastungsintensiv. Anders als im Bereich der Außenpolitik oder der Wirtschaftslenkung kann man daher nicht von einem Eingriff eher geringer Intensität ausgehen, der die Beschränkung auf eine Willkürprüfung erlauben würde.

Mit dem Volkszählungsurteil des Bundesverfassungsgerichts wird man vielmehr zumindest eine vertretbare Entscheidung des Gesetzgebers verlangen müssen, zumal das Volkszählungsgesetz 1983 nur eine inhaltlich begrenzte, einmalige und offene Datenerhebung zu primär statistischen Zwecken und damit eine erheblich weniger eingreifende Maßnahme vorsah. Die Anwendung des Vertretbarkeitsmaßstabs macht eine eigene inhaltliche Prüfung der Verhältnismäßigkeit im engeren Sinne erforderlich, anhand deren Ergebnis dann zu entscheiden ist, ob der Gesetzgeber vertretbar die Verhältnismäßigkeit einer generellen Vorratsspeicherung von Telekommunikations-Verkehrsdaten annehmen darf.

(aa) Durch Telekommunikation gefährdete Gemeinschaftsgüter, ihr Gewicht und die Wahrscheinlichkeit ihrer Beeinträchtigung

(i) Einschlägige Gemeinschaftsgüter

Im Rahmen der Abwägung ist auf Seiten der Gemeinwohlinteressen zunächst fraglich, welche Rechtsgüter die einschlägigen Regelungsvorschläge hinsichtlich der Einführung einer Vorratsspeicherung schützen sollen. Eine Kommunikationsdatenspeicherung wird vor allem zur Effektivierung der Strafverfolgung angestrebt. Bei der Bemessung des Gewichts der Gewährleistung einer effektiven Strafverfolgung ist die Rechtsprechung des Bundesverfassungsgerichts zu beachten, der zufolge die Gewährleistung einer effektiven Strafverfolgung eine wesentliche Staatsaufgabe sein soll[215]. Im Rahmen der Verhältnismäßigkeitsprüfung sieht das Gericht in der effektiven Strafverfolgung – teilweise spricht es auch von der „Rechtspflege“ – ein eigenständiges Verfassungsgut, das aus dem Rechtsstaatsprinzip herzuleiten sei und zu dessen Gewährleistung der Gesetzgeber verpflichtet sei[216]. Den Inhalt dieses Verfassungsgutes sieht das Gericht abstrakt in der „Durchsetzung von Gerechtigkeit“, der Gewährleistung einer „wirksamen Strafverfolgung“, einer „umfassenden Wahrheitsermittlung im Strafverfahren“, der „Aufklärung schwerer Straftaten“ und der „umfassenden Aufklärung der materiellen Wahrheit“[217], ohne dass es darauf ankomme, ob der konkrete Eingriff dem Schutz von Rechtsgütern dienen könne[218].

Diese Ansicht ist abzulehnen. Strafverfolgung ist kein Selbstzweck[219] und eine „geordnete Strafrechtspflege“ als solche ist daher auch kein Verfassungswert[220]. Andernfalls könnte der Staat, der die

214 Übersicht bei MDG, EU-Questionnaire (I).
215 Seite 28.
216 Etwa BVerfGE 77, 65 (76).
217 Etwa BVerfGE 77, 65 (76).
218 BVerfGE 107, 299 (324): „eigenständige verfassungsrechtliche Bedeutung“.
219 BVerfGE 39, 1 (46); BGHSt 24, 40 (42): kein Schuldausgleich um seiner selbst willen.

Definitionsmacht über das Strafrecht hat, alle Grundrechte im Staatsinteresse relativieren[221]. Der Gedanke einer „Durchsetzung von Gerechtigkeit“ im Strafverfahren zielt bei genauer Betrachtung auf nichts anderes als Vergeltung. Strafe als bloße Vergeltung für in der Vergangenheit begangenes Unrecht kann aber keine Eingriffe in Grundrechte legitimieren[222], jedenfalls keine Eingriffe in die Grundrechte Unbeteiligter, wie sie mit den meisten strafrechtlichen Ermittlungsverfahren verbunden sind.

Auch aus dogmatischer Sicht ist ein Verfassungsgut „Strafrechtspflege“ abzulehnen. In der Abwägung mit Grundrechten und anderen Verfassungsgütern lässt sich das Gewicht eines derart abstrakten Verfassungsgutes nicht bestimmen. Daran ändert es nichts, wenn das Bundesverfassungsgericht allgemein feststellt, dass bei der Strafverfolgung höhere Eingriffsschwellen hingenommen werden müssen als bei der präventiven Gefahrenabwehr[223], dass Strafverfolgungsinteressen also von geringerem Gewicht sind als der unmittelbare Rechtsgüterschutz.

Eingriffe können auch nicht allein mit dem Argument der Sicherung der Gleichmäßigkeit der Strafverfolgung legitimiert werden, also durch den bloßen Verweis darauf, dass Straftäter gegenwärtig in vielen Kriminalitätsbereichen nicht systematisch aufgespürt, sondern nur in vergleichsweise wenigen und vorwiegend leichten Fällen durch Zufall entdeckt werden können. Wenn die staatlichen Mittel zur Sicherung einer gleichmäßigen Strafverfolgung nicht ausreichen, dann spricht dies allein gegen die Verhältnismäßigkeit der jeweiligen Strafnorm selbst und wirft die Frage auf, ob das Strafrecht insoweit ein probates Mittel zur Erreichung des gesetzgeberischen Ziels ist. Zur Rechtfertigung weiter gehender Eingriffsbefugnisse können Vollzugsdefizite nicht heran gezogen werden, weil die Strafverfolgung kein Selbstzweck ist.

Fraglich ist, ob erweiterte Ermittlungsbefugnisse mit dem Verweis auf die Interessen des in einem Strafverfahren Beschuldigten gerechtfertigt werden können. Das Bundesverfassungsgericht argumentiert insoweit, dass Ermittlungsbefugnisse auch der Entlastung unschuldiger Beschuldigter dienen könnten, die ansonsten zu Unrecht einem Ermittlungsverfahren ausgesetzt oder gar verurteilt werden könnten. Ohne hinreichende Kenntnisse bestünde die Gefahr, dass Gerichte ihre Entscheidungen auf mangelhafter Tatsachengrundlage träfen[224].

Bei dieser Argumentation wird indes unbesehen davon ausgegangen, dass erweiterte Ermittlungsbefugnisse mehr Unschuldige ent- als belasten. Hiervon kann aber jedenfalls auf dem Gebiet des staatlichen Zugriffs auf Kommunikationsdaten keine Rede sein. Kommunikationsdaten dienen im Wesentlichen dazu, Ermittlungsansätze oder Indizien zu bilden[225]. Sie sind demgegenüber nicht hinreichend aussagekräftig, um eine Person unmittelbar zu be- oder entlasten, weil sie sich nur auf einen Telekommunikationsanschluss beziehen und nicht erkennen lassen, wer diesen Anschluss bedient hat[226]. Aus diesem Grund stellen Kommunikationsdaten nicht nur als Ermittlungsansätze ein unsicheres Mittel dar. Sie bergen auch die besondere Gefahr in sich, dass unschuldige Personen einem falschen Verdacht ausgesetzt werden[227]. Dies hat sich in den USA gezeigt, wo die Industrie gerichtlich gegen vermeintliche Nutzer illegaler Tauschbörsen für urheberrechtlich geschützte Inhalte vorgegangen ist. In mehreren Fällen sind dort im Laufe des Verfahrens Zweifel aufgetreten, ob die Beklagten zu den von den Rechteverwertern angegebenen Zeitpunkten ihren Computer überhaupt benutzt haben[228].

Eine erhöhte Gefahr falscher Verdächtigungen entsteht, wenn die Sicherheitsbehörden durch Abarbeiten einer lange Liste von „Verdächtigen“ nach dem Eliminierungsprinzip vorgehen, wie es Auskünfte über Telekommunikationsdaten oft erforderlich machen (etwa bei einer Auskunft über alle Personen, die innerhalb eines bestimmten Zeitraums einen bestimmten Telefonanschluss angerufen haben, oder über alle Personen, die sich zu einer bestimmten Zeit im Bereich einer bestimmten Mobilfunkzelle aufgehalten haben). Es spricht daher viel dafür, dass der staatliche Zugriff auf Kommunikationsdaten mehr Unschuldige be- als entlastet. Daneben ist zu beachten, dass Maßstab einer gerichtlichen Verurteilung die richterliche Überzeugung ist. Im Zweifel ist von einer Verurteilung abzusehen

220 L/D2-Lisken/Denninger, D 25.

221 L/D2-Lisken/Denninger, D 25, Fn. 81.

222 Vgl. schon Platon, in deutscher Übersetzung bei Niggli, Kriminologische Überlegungen zur Strafzumessung (I), 3: „Niemand bestraft einen Rechtsbrecher aufgrund abstrakter Überlegungen oder einfach deshalb, weil der Täter das Recht gebrochen hat, es sei denn einer nehme unbedacht Rache wie ein wildes Tier. Jener der mit Vernunft straft, rächt sich nicht für das geschehene Unrecht, denn er kann es nicht ungeschehen machen. Vielmehr schaut er in die Zukunft und versucht, den Täter und andere mit der Strafe davon abzuhalten, das Recht wieder zu brechen.“

223 BVerfGE 100, 313 (394 ff.); ebenso Schenke, AöR 125 (2000), 1 (29); dagegen AK-GG-Bizer, Art. 10, Rn. 95.

224 BVerfGE 77, 65 (76).

225 Clayton, Richard: The Limits of Traceability, 28.08.2001, www.cl.cam.ac.uk/~rnc1/The_Limits_of_Traceability.html.

226 Clayton, Richard: The Limits of Traceability, 28.08.2001, www.cl.cam.ac.uk/~rnc1/The_Limits_of_Traceability.html.

227 Clayton, Richard: The Limits of Traceability, 28.08.2001, www.cl.cam.ac.uk/~rnc1/The_Limits_of_Traceability.html.

228 Krempl, Stefan: Schwere Bedenken gegen Ausschnüffelung der Nutzer bei Copyright-Verstößen, Heise-Verlag, Meldung vom 12.12.2003, www.heise.de/newsticker/data/jk-12.12.03-005/.

(Art. 6 Abs. 2 EMRK). Aus diesem Grund ist die Gefahr, dass Gerichte aufgrund mangelhafter Tatsachengrundlage verurteilen, klar begrenzt. Schließlich ist darauf hinzuweisen, dass der Staat entsprechend dem Verhältnismäßigkeitsprinzip erheblich weiter gehende Eingriffe vorsehen darf, wenn er die Verwendung der Kenntnisse effektiv auf die mögliche Entlastung von Beschuldigten beschränkt. Die Erforderlichkeit einer Maßnahme zur Entlastung von Beschuldigten zwingt daher keineswegs dazu, die Maßnahme auch zur Belastung von Personen vorzusehen. In letztgenannten Fall gebietet es das Verhältnismäßigkeitsprinzip vielmehr, die Eingriffsschwelle erheblich höher anzusiedeln. Festzuhalten bleibt damit, dass sich ein erweiterter staatlicher Zugriff auf Telekommunikationsdaten nicht mit dem Verweis auf eine mögliche Entlastung Unschuldiger begründen lässt.

Durch die genannten Argumente lassen sich Eingriffe zum Zwecke der Strafverfolgung mithin nicht rechtfertigen. Das Strafrecht ist vielmehr nur als Mittel des Rechtsgüterschutzes legitim[229], als Instrument zur Verhütung des Eintritts konkreter Schäden. Die Gewährleistung einer geordneten Strafrechtspflege als solche ist demgegenüber nicht als Gemeinschaftsgut im Rahmen der Verhältnismäßigkeitsprüfung anzusehen und bleibt daher im Folgenden außer Betracht.

(ii) Einschlägige Gemeinschaftsgüter im Bereich der Netzkriminalität

Fraglich ist, welche konkreten Rechtsgüter mit Hilfe einer generellen Vorratsspeicherung von Telekommunikationsdaten geschützt werden können, welches Gewicht diese Rechtsgüter aufweisen und in welchem Maße sie bedroht sind.

Besonders nützlich ist eine generelle Vorratsspeicherung von Telekommunikationsdaten im Bereich von Straftaten, die unter Verwendung von Telekommunikationsnetzen begangen werden, weil sich oftmals nur anhand von Kommunikationsdaten ermitteln lässt, wer an dem entsprechenden Telekommunikationsvorgang beteiligt war. Zum Ersten ist das Feld der Netzkriminalität im engeren Sinne zu betrachten. Computer und Telekommunikationsnetze bilden heute eine wichtige Stütze unserer Volkswirtschaften[230]. Insofern ist es wichtig, die Verfügbarkeit der Systeme und Netze zu gewährleisten und die gespeicherten und übertragenen Daten vor unberechtigtem Zugang und Manipulationen zu schützen[231]. Das unberechtigte Auslesen, Schreiben, Verändern oder Löschen von automatisch verarbeiteten Daten ist in weiten Bereichen ohne Telekommunikationsnetze undenkbar. Dies gilt beispielsweise für die rasche Verbreitung von Computerviren per E-Mail oder für die Sabotage von Internetangeboten durch „DDoS-Attacks“. Es liegt daher auf der Hand, dass viele Fälle von Hacking die Benutzung der Telekommunikationsnetze voraussetzen. Insoweit kann man von Telekommunikationsnetzen als „gefährlichen Werkzeugen“ sprechen.

Denkbar ist, dass von Telekommunikationsnetzen ein eigenständiges Gefahrenpotenzial ausgehen könnte. Für diese Annahme könnte sprechen, dass es in der Vergangenheit vorgekommen ist, dass sich ansonsten unbescholtene Jugendliche („Script-Kiddies“) „zum Spaß“ öffentlich zugänglicher Software bedient haben, um bekannte kommerzielle Internetangebote „lahm zu legen“. Erst das Internet hat es möglich gemacht, Schäden diesen Ausmaßes derart leicht und grenzüberschreitend zu verursachen. Andererseits waren Jugendliche schon immer anfällig für die Begehung milieutypischer Straftaten, die der Profilierung in ihrem Umfeld dienen.

Allgemein ist denkbar, dass sich die Netzkriminalität im engeren Sinne im Wesentlichen durch eine Verlagerung von Kriminalität aus anderen Feldern erklären lässt. Für diese These spricht, dass der Siegeszug der Informationsgesellschaft nicht zu einem höheren Gesamtkriminalitätsniveau geführt hat, wie die Entwicklung der polizeilichen Kriminalitätsstatistik über die letzten Jahre hinweg zeigt. Aus der Tatsache, dass Telekommunikationsnetze zur Begehung von Straftaten eingesetzt werden, lässt sich mithin nicht eindeutig schließen, ob und inwieweit das Kriminalitätsniveau ohne Telekommunikationsnetze niedriger wäre. Vielmehr spricht die allgemeine Erkenntnis, dass Kriminalität ein normales gesellschaftliches Phänomen darstellt, für die Annahme, dass mit der zunehmenden Verlagerung des sozialen Lebens in den Bereich der Telekommunikationsnetze die Kriminalität in diesem Bereich in gleichem Maße zunimmt.

Hinzu kommt das vergleichsweise geringe Gewicht der durch Netzkriminalität im engeren Sinne bedrohten Rechtsgüter. In ihren praktischen Auswirkungen führt diese Art von Kriminalität vor allem zu Vermögensschäden, sei es durch die Störung von Computersystemen, sei es durch die Weitergabe von Geschäftsgeheimnissen. Die Wahrscheinlichkeit, dass Leib und Leben von Menschen gefährdet wer-

229 BVerfGE 38, 312 (321); BVerfGE 39, 1 (46); BVerfGE 88, 203 (257 f.); vgl. auch BVerfGE 45, 187 (228): „der Mensch muss immer Zweck an sich selbst bleiben“; a.A. BVerfGE 107, 299 (324): „Das Interesse an der Aufklärung und Verfolgung von Straftaten hat neben dem Interesse an der Verhinderung weiterer Straftaten eine eigenständige verfassungsrechtliche Bedeutung.“

230 Kommission, Sichere Informationsgesellschaft (I), 7.

231 Kommission, Sichere Informationsgesellschaft (I), 7.

den könnten, wird zwar allenthalben heraufbeschworen. Die „lebenswichtigen Infrastrukturen“ wie Stromnetze, deren Störung zu solchen Gefahren führen könnte, sind aber in aller Regel nicht an das Internet angeschlossen und für telekommunikative Angriffe daher nicht zugänglich. Dass solche Infrastrukturen mit Hilfe von Telekommunikationsnetzen angegriffen werden könnten oder gar ein organisierter Angriff auf einen Staat unter Einsatz von Telekommunikationsnetzen („Information Warfare“, „Cyberwar“, „Infowar“) stattfinden könnte, muss man daher auf absehbare Zeit in den Bereich der Science-Fiction verweisen[232]. Ein Anschluss national wichtiger Systeme an öffentlich zugängliche Telekommunikationsnetze ist nicht erforderlich und wäre auch äußerst leichtsinnig. Hier ist zuallererst an technische Maßnahmen zur Abwendung von Schäden zu denken. Eine US-amerikanische Umfrage hat keinerlei terroristisch motivierte Netzkriminalität feststellen können[233].

Mithin beschränken sich die Auswirkungen von Netzkriminalität im engeren Sinne fast durchweg auf Vermögensschäden. Dies macht es möglich, derart entstandene Schäden gegen die finanziellen Kosten abzuwägen, die der Gesellschaft durch eine generelle Vorratsspeicherung von Telekommunikationsdaten entstehen würden. Zu diesen Kosten zählen etwa die Aufwendungen der Telekommunikationsunternehmen bei der Mitwirkung an der staatlichen Telekommunikationsüberwachung. Diese Kosten werden von den Unternehmen über ihre Preise auf die Nutzer abgewälzt. Eine umfassende Abwägung der Kosten wäre angesichts der Belastung durch eingreifende Maßnahmen angebracht, findet bisher aber nicht statt.

Zweitens ist der Bereich der Netzkriminalität im weiteren Sinne zu betrachten. Einen Teil der Netzkriminalität im weiteren Sinne stellen Inhaltsdelikte dar, also das rechtswidrige Übermitteln von Inhalten über Telekommunikationsnetze. Zu nennen ist etwa der illegale Austausch von urheberrechtlich geschütztem Material, von Kinderpornografie oder von rassistischer Propaganda. Die neuen Netze ermöglichen solche Delikte nicht erst; sie können ihre Begehung aber erleichtern. Dies gilt wohlgemerkt nur bei abstrakter Betrachtung. In einzelnen Fällen mögen auch Inhaltsdelikte erst wegen den Möglichkeiten der Telekommunikationsnetze begangen werden. Diese Frage ist bisher allerdings noch nicht untersucht worden.

Eine Gefährdung von Leib, Leben oder Freiheit erscheint auch im Bereich der Netzkriminalität im weiteren Sinne in aller Regel ausgeschlossen. Gerade im Bereich des illegalen Austauschs von Inhalten liegt es zwar auf der Hand, dass es das Internet so leicht wie nie zuvor macht, an illegale Inhalte zu gelangen. Dies bedeutet allerdings noch nicht, dass die leichtere Erreichbarkeit auch zu mehr Anhängern von Kinderpornografie, Rassismus usw. geführt hat. Diesen Schluss zu ziehen, wäre ohne eine eingehende Untersuchung verfehlt. Das Internet beruht gerade auf dem Konzept eines freien Informationsaustausches und auf der Idee des mündigen Bürgers. Benutzer des Internet stoßen nicht unfreiwillig auf illegales Material, sondern sie müssen aktiv nach solchen Inhalten suchen, um mit ihnen konfrontiert zu werden.

Selbst wenn sie das tun, ist noch nicht gesagt, dass der Konsum solcher Materialien schädliche Auswirkungen hat. Gerade bei Jugendlichen ist es natürlich, dass sie die Grenzen des sozial Erlaubten ausloten, um ganz regelmäßig schließlich doch wieder in die Mitte der Gesellschaft zurückzukehren. In anderen Fällen legen die Umstände zwar nahe, dass bestimmte Inhalte mitursächlich für Straftaten waren, etwa im Falle des Schulmassakers von Erfurt. Inwieweit eine Ursächlichkeit tatsächlich gegeben ist, ist allerdings ungeklärt. In dem zuletzt genannten Fall ging es übrigens um eine Beeinflussung des Täters durch bestimmte Videofilme, Bücher, CDs und Computerspiele, so dass eine Verbindung zu Telekommunikationsnetzen nicht bestand.

Welche Auswirkungen eine Prohibition von Inhalten und deren Aufhebung haben kann, verdeutlicht folgendes Beispiel[234]: In Dänemark gab es bis 1967 steigende Zahlen für die Herstellung und den Absatz verbotener pornographischer Literatur. Schon zwei Jahre nach der Aufhebung diesbezüglicher Verbotsbestimmungen gingen diese Zahlen rapide zurück. Es liegt nahe, dass dies auf einen Sättigungsprozess durch Befriedigung der diesbezüglichen Neugierde der Bevölkerung zurückzuführen ist. Dementsprechend lässt sich auch in anderen Bereichen nicht von vornherein behaupten, dass die Zugänglichkeit illegaler Inhalte über das Internet sozial schädlich sei, zumal der Konsum solcher Inhalte nicht in jedem Fall und allenfalls mittelbar Gefahren für konkrete Rechtsgüter mit sich bringt.

Auch im Bereich von Verstößen gegen das Urheberrecht ist nicht geklärt, ob die immer weitere Stärkung der IP-Rechte dem Zweck des Rechtsinstituts des geistigen Eigentums entspricht. Ein Copy-

232 Olaf Lindner (Direktor Security Services bei Symatec), zitiert bei Schürmann, Hans: Angriff aus dem Web abgewehrt, Handelsblatt vom 10.02.2003, S. 19; BMI/BMJ, Sicherheitsbericht 2001, 205: „Konkrete Hinweise hinsichtlich [...] eines ‚Information Warfare‘ existieren [...] derzeit nicht.“

233 Symantec, Symantec Internet Security Threat Report (I), 5.

234 Eisenberg, Kriminologie, § 23, Rn. 50.

rightschutz aus rein wirtschaftlichen Gründen steht nämlich tendenziell im Widerspruch zum ursprünglichen Sinn des Urheberschutzes, den Fortschritt auf diesem Gebiet zu fördern, indem ein Anreiz für Erfindungen und Weiterentwicklungen geschaffen wird[235]. Heutzutage dient der Schutz geistigen Eigentums nur selten dem kleinen Tüftler, sondern zumeist den Interessen weltweit tätiger Unternehmen. Deren Interessen scheinen dem Allgemeinwohl nicht selten zu widersprechen. Besonders deutlich zeigt sich dies an der Diskussion über Patente an Aids-Medikamenten: Die Inhaber dieser Patente verlangen ein Vielfaches der Produktionskosten für die lebensrettenden Stoffe und nehmen so den Tod unzähliger Aidskranker vor allem in Entwicklungsländern in Kauf.

Zwar hat der ursprüngliche Gedanke des Schutzes geistigen Eigentums, dass sich die Entwicklung von Innovationen nur bei einem angemessenem Schutz der Rechte an dem Produkt lohnt, auch weiterhin seine Berechtigung. Angesichts der langen Schutzfristen stellt sich aber die Frage, ob dies den Fortschritt nicht eher behindert als fördert. Beispielsweise ist fraglich, ob das gegenwärtige Recht einen ausreichenden Anreiz für den Softwaremonopolisten Microsoft bietet, seine profitablen Produkte zu verbessern. Zweifel hieran wecken die zahlreichen Qualitätsmängel (etwa „Abstürze“ und Sicherheitsmängel) der Produkte dieses Unternehmens. Teilweise wird sogar vertreten, Copyrightverstöße könnte die Verbreitung eines Produkts fördern und dessen Marktmacht unter Umständen noch stärken. Jedenfalls sind Einschränkungen der freien Internetnutzung insoweit kontraproduktiv, wie sie das Vertrauen der Bürger in dieses Medium schwächen und daher auch den Absatz von Produkten in diesem Bereich erschweren. Außerdem können sie zu einem Ausweichen auf kostenfrei verfügbare „Open Source“-Software führen, was nicht im Sinne der Anbieter kommerzieller Produkte liegen kann. In anderen Fällen würde die Unterbindung illegaler Kopien dazu führen, dass auf die Benutzung der Software gänzlich verzichtet würde. Nur in einem geringen Teil der Fälle würde anstelle der Anfertigung illegaler Kopien die Originalsoftware gekauft, was die astronomischen Schadensschätzungen der Industrie nicht berücksichtigen.

Weiterhin sind „Raubkopien“ auch außerhalb der Telekommunikationsnetze verbreitet, gerade durch die Technologie der CD-Brenner. Man denke nur an den Tausch von Software oder Musik-CDs auf dem Schulhof. Auch kommt in Betracht, dass Straftäter ohne die Möglichkeiten der Telekommunikationsnetze teilweise andere Straftaten im Bereich traditioneller Kriminalität begehen könnten. Wenn das Motiv eines potenziellen Täters beispielsweise darin besteht, unbedingt an ein teures Computerspiel zu bekommen, könnte er statt einer „Raubkopie“ aus dem Internet auch einen Diebstahl in Betracht ziehen. Er könnte auch jemanden betrügen, um an Geld zu kommen, mit dem er das Spiel erwerben könnte.

Somit ist auch im Bereich des geistigen Eigentums das letzte Wort in Bezug auf den tatsächlich durch „Raubkopien“ entstehenden Schaden noch nicht gesprochen. Zudem ist in der Abwägung wiederum zu berücksichtigen, dass auch hier nur Vermögensschäden entstehen können, was es fraglich erscheinen lässt, ob derart weit reichende Überwachungsmaßnahmen, wie sie die Industrie zu ihrem Vorteil fordert, gerechtfertigt sind.

Überhaupt ist es im Bereich der Netzkriminalität im weiteren Sinne fragwürdig, ob die Telekommunikationsnetze zu einem insgesamt höheren Kriminalitätsniveau führen. In diesem Feld, in dem Telekommunikationsnetze lediglich als Medium für zwischenmenschliche Kommunikation eingesetzt werden, besteht ein besonders hohes Maß an Substituierbarkeit. Dies legt die Annahme nahe, dass die Telekommunikation in diesem Bereich größtenteils die unmittelbare Kommunikation in der „Offline-Welt“ nachvollzieht und im Wesentlichen nur eine Verlagerung von ehemaligem „Offline-Verhalten“ in die Telekommunikationsnetze stattfindet. Die neuen Medien scheinen in diesem Bereich also den Platz traditioneller Kommunikationsmittel einzunehmen, ohne – der Kriminalitätsstatistik nach zu urteilen – eine spürbare Kriminalitätssteigerung nach sich zu ziehen. Eine erhöhte Gefahr durch Telekommunikationsnetze kann daher auf der Basis bisheriger Erkenntnisse nicht angenommen werden.

(iii) Ausmaß der Gefährdung durch Netzkriminalität

Bisher liegen keine zuverlässigen Statistiken über das Ausmaß an Netzkriminalität oder die dadurch verursachten oder verursachbaren Schäden vor[236]. Erst recht sind keine Erkenntnisse über die insgesamt durch Telekommunikation verursachten Schäden vorhanden. Wenn überhaupt, dann wurde meist das zahlenmäßige Ausmaß von Computerkriminalität untersucht. Aber auch auf diesem Gebiet fehlt es

235 Tallo, Bericht zum Entwurf des Cybercrime-Abkommens (I), Unterpunkt F.36.

236 BMI/BMJ, Sicherheitsbericht 2001, 201; Holznagel, Bernd: Stellungnahme für die öffentliche Anhörung „Von der Industrie- zur Wissensgesellschaft: Wirtschaft, Arbeitswelt und Recht, Privatisierung und Patentierung von Wissen“, 08.10.2001, www.bundestag.de/gremien/welt/weltto/weltto126_stell004.pdf, 22.

weitgehend an verlässlichen Statistiken[237]. Jenseits statistischer Angaben ist immerhin anerkannt, dass sich die Nutzer der neuen Medien in den allermeisten Fällen legal verhalten und dass der Missbrauch der Datennetze im Vergleich zu ihrer legaler Nutzung einen verschwindend geringen Anteil bildet[238].

Für den Bereich der Netzkriminalität im engeren Sinne lässt sich diese Annahme durch die deutsche polizeiliche Kriminalitätsstatistik bestätigen. Allerdings ist vorweg darauf hinzuweisen, dass die Aussagekraft der Kriminalitätsstatistik nicht überschätzt werden darf. Dies gilt insbesondere im Hinblick auf die erhebliche Anzahl von Straftaten, die den Strafverfolgungsorganen nicht bekannt werden (Dunkelfeld). Das Ausmaß des Dunkelfeldes schwankt sowohl im zeitlichen Vergleich wie auch im Vergleich der einzelnen Deliktsgruppen zueinander in kaum vorhersehbarer Weise. Tatsächlich gibt es so viele Ursachen für Veränderungen der erfassten Fallzahlen, dass Schlüsse auf die Entwicklung des tatsächlichen Kriminalitätsniveaus verfehlt wären[239].

Lässt man diese Bedenken außer Acht, weil die polizeiliche Kriminalitätsstatistik einen der wenigen tatsächlichen Anhaltspunkte zur Einschätzung des Ausmaßes an Netzkriminalität im engeren Sinne darstellt, dann ergibt sich folgendes Bild: Auf je 1000 Einwohner kam 2001 ein Fall von Computerkriminalität im engeren Sinne[240], wobei mehr als die Hälfte der Fälle auf Betrug mittels rechtswidrig erlangter Karten für Geld- oder Kassenautomaten entfiel. Nach Abzug dieser Delikte, bei denen von vornherein kein Zusammenhang mit Telekommunikationsnetzen bestehen kann, verbleiben höchstens 30.000 Fälle von Netzkriminalität im engeren Sinne im Jahre 2001. In dieser Größenordnung liegen ansonsten bereits einzelne Deliktsgruppen wie „Diebstähle aus Neubauten“ oder der Handel mit Cannabis. Zum Vergleich: Es gab 100-mal mehr Diebstähle, 20-mal mehr Sachbeschädigungen und fünfmal mehr Beleidigungen als alle potenziellen Fälle von Netzkriminalität zusammen genommen. Gemessen an der Gesamtzahl der erfassten Delikte handelt es sich um 0,5% der Delikte. Das Kriminalitätsfeld der Netzkriminalität im engeren Sinne ist der polizeilichen Kriminalitätsstatistik zufolge also eher zu vernachlässigen. Gegen ein großes Ausmaß von Netzkriminalität im engeren Sinne im Vergleich zu dem allgemeinen Kriminalitätsniveau sprechen auch Zahlen aus Großbritannien, denen zufolge der Zugriff auf Kommunikationsdaten regelmäßig im Zusammenhang mit Ermittlungen wegen allgemeiner Kriminalität erfolgt, dagegen nur in einem Bruchteil der Fälle im Zusammenhang mit Computerkriminalität[241].

Es ist plausibel, im Bereich der Netzkriminalität von steigenden Fallzahlen auszugehen[242], weil die Nutzung der Telekommunikationsnetze allgemein zunimmt. Die durchschnittliche jährliche Steigerungsrate der Computerkriminalität in den letzten Jahren (1997-2001: 21%)[243] liegt allerdings weit[244] unter der durchschnittlichen jährlichen Wachstumsrate der Anzahl von Internetnutzern in Deutschland (1997-2002: 49%)[245]. Für die statistisch ausgewiesenen Fallzahlen im Bereich der Netzkriminalität ist zudem in großem Maße der Umfang polizeilicher Aufklärungsaktivitäten maßgebend[246], weswegen tatsächlich eine erheblich geringere Steigerungsrate des Ausmaßes an Netzkriminalität vorliegen kann als sie sich aus der Kriminalitätsstatistik ergibt.

Fest steht, dass die polizeiliche Kriminalitätsstatistik nur einen Teil aller Fälle von Computerkriminalität widerspiegelt und die tatsächlichen Zahlen erheblich höher sind[247]. Auf dem Gebiet der Netz-

237 BMI/BMJ, Sicherheitsbericht 2001, 201; Kommission, Sichere Informationsgesellschaft (I), 13: „Mangels aussagekräftiger Statistiken ist es erforderlich, stichhaltige Belege für das Ausmaß der Computerkriminalität zusammenzutragen.“

238 Holznagel, Bernd: Stellungnahme für die öffentliche Anhörung „Von der Industrie- zur Wissensgesellschaft: Wirtschaft, Arbeitswelt und Recht, Privatisierung und Patentierung von Wissen“, 08.10.2001, www.bundestag.de/gremien/welt/-weltto/weltto126_stell004.pdf, 22; Norbert Geis (MdB) u.a., BT-Drs. 14/4173, 1; ULD-SH, Sichere Informationsgesellschaft (I), Punkt 6.

239 BMI/BMJ, Sicherheitsbericht 2001, 1; str., vgl. Kury, Kriminalistik 2001, 74 (77) m.w.N.

240 BMI/BMJ, Sicherheitsbericht 2001, 201; Holznagel, Bernd: Stellungnahme für die öffentliche Anhörung „Von der Industrie- zur Wissensgesellschaft: Wirtschaft, Arbeitswelt und Recht, Privatisierung und Patentierung von Wissen“, 08.10.2001, www.bundestag.de/gremien/welt/weltto/weltto126_stell004.pdf, 20.

241 NCIS Submission (I), Punkt 6.1.1.

242 BMI/BMJ, Sicherheitsbericht 2001, 197; Holznagel, Bernd: Stellungnahme für die öffentliche Anhörung „Von der Industrie- zur Wissensgesellschaft: Wirtschaft, Arbeitswelt und Recht, Privatisierung und Patentierung von Wissen“, 08.10.2001, www.bundestag.de/gremien/welt/weltto/weltto126_stell004.pdf, 21 f.

243 Nach BMI, PKS 2001 (I) und ohne Abzug von Betrug mit Zahlungskarten.

244 Holznagel, Bernd: Stellungnahme für die öffentliche Anhörung „Von der Industrie- zur Wissensgesellschaft: Wirtschaft, Arbeitswelt und Recht, Privatisierung und Patentierung von Wissen“, 08.10.2001, www.bundestag.de/gremien/welt/-weltto/weltto126_stell004.pdf, 22: „deutlich“.

245 Heise Verlag: 44 Prozent der Deutschen gehen ins Netz, Meldung vom 05.09.2002, www.heise.de/newsticker/data/anw-05.09.02-005/.

246 BMI/BMJ, Sicherheitsbericht 2001, 197.

247 Sieber, COMCRIME-Studie (I), 22 f.; Kommission, Sichere Informationsgesellschaft (I), 13; Holznagel, Bernd: Stellungnahme für die öffentliche Anhörung „Von der Industrie- zur Wissensgesellschaft: Wirtschaft, Arbeitswelt und Recht, Privatisierung und Patentierung von Wissen“, 08.10.2001, www.bundestag.de/gremien/welt/weltto/-

kriminalität ist dies beispielsweise darin begründet, dass viele Straftaten nicht bemerkt werden (z.B. Hacking) oder von betroffenen Unternehmen nicht gemeldet werden, um kein schlechtes Bild in der Öffentlichkeit abzugeben[248].

Fraglich ist aber, ob das Dunkelfeld auf dem Gebiet der Netzkriminalität im Vergleich zu anderen Deliktsgruppen besonders hoch ist[249]. Nur in diesem Fall würde es sich um eine besorgniserregende Besonderheit auf diesem Gebiet handeln. Grundsätzlich existiert die Dunkelfeldproblematik bei allen Delikten. Ob ein besonders hohes Dunkelfeld auf dem Gebiet der Netzkriminalität existiert, ist soweit ersichtlich noch nicht empirisch untersucht worden[250]. Eine Umfrage unter 3.623 Unternehmen weltweit – darunter 1.476 europäischen Unternehmen – ergab, dass über die Hälfte der Unternehmen jeden Fall von Wirtschaftskriminalität anzeigen[251]. Ein weiteres Drittel der Unternehmen reagiert ab einer bestimmten Erheblichkeitsschwelle mit einer Anzeige[252], so dass insgesamt nahezu 90% der befragten Unternehmen gravierende Fälle von Wirtschaftskriminalität – darunter auch Netzkriminalität – anzeigen. Einer Meinungsumfrage unter US-amerikanischen Unternehmen und Organisationen zufolge haben immerhin 34% der Befragten auf Fälle von Computerkriminalität meistens mit einer Strafanzeige reagiert[253], was eine Dunkelziffer von 66% der Gesamtkriminalität bedeuten würde.

In anderen Kriminalitätsbereichen wird die Dunkelziffer weit höher geschätzt[254]. Beispielsweise ist anzunehmen, dass nur ein kleiner Bruchteil aller Beleidigungen angezeigt wird, weil in der Gesellschaft andere Regelungsmechanismen für diese Fälle existieren. Auch in vielen Fällen von versuchtem Betrug wird oft von einer Anzeige abgesehen werden, weil die betroffene Person die versuchte Täuschung bemerkt und daher keinen Schaden erleidet. Bei vollendetem Betrug werden sich viele Opfer schämen, dass sie auf den Täter hereingefallen sind. Dabei kann es sich auch um Anlagebetrug in Millionenhöhe von prominenten Mitgliedern der Gesellschaft handeln, so dass sich das Dunkelfeld nicht auf Bagatellfälle beschränkt. Auch bei Delikten, bei denen in der Bevölkerung kein Unrechtsbewusstsein existiert und die dementsprechend weit verbreitet sind, geht man von einem großen Dunkelfeld aus[255]. Diese beispielhaft aufgezählten Bereiche außerhalb der Netzkriminalität sprechen gegen die Annahme, dass gerade im Bereich der Netzkriminalität ein außergewöhnlich hohes Dunkelfeld bestehen könnte.

Für ein besonders großes Dunkelfeld spricht auch nicht, dass Computerviren äußerst verbreitet sind und dennoch kaum einmal Anzeigen diesbezüglich erstattet werden[256]. Die insoweit einschlägigen Straftatbestände setzen sämtlich Vorsatz voraus, wohingegen sich Computerviren ganz regelmäßig unbemerkt verbreiten. Zwar wird der Programmierer eines Computervirus regelmäßig vorsätzlich handeln. Dieses Delikt würde aber nur als ein Fall in die Kriminalitätsstatistik eingehen und fiele daher kaum ins Gewicht. Computerviren stammen außerdem vergleichsweise selten aus Deutschland, so dass Ermittlungen deutscher Behörden regelmäßig keinen Erfolg versprechen.

Für ein erhöhtes Dunkelfeld könnte sprechen, dass ein Teil der Netzkriminalität in den Bereich der Wirtschaftskriminalität fällt und die Kriminologie der Wirtschaftskriminalität insgesamt ein vergleichsweise großes Dunkelfeld zuschreibt[257]. Bei Straftaten, die persönliche oder staatliche Schutzgüter erheblich verletzen, schätzt die Wissenschaft das Dunkelfeld allerdings als vergleichsweise klein ein[258], weil – selbst innerhalb geschlossener Zirkel – Schäden für Leib, Leben oder Freiheit einer Person oder Vermögensschäden Dritter der Außenwelt kaum verborgen bleiben werden. Ein hohes Dun-

---

weltto126_stell004.pdf, 21; für Internetkriminalität auch BMI/BMJ, Sicherheitsbericht 2001, 197 und 198; French Delegation of Police Cooperation Working Party, Enfopol 38 (I), 10.

248 Kommission, Sichere Informationsgesellschaft (I), 13; Weichert, Bekämpfung von Internet-Kriminalität (I), Punkt 2; Sieber, COMCRIME-Studie (I), 22 f.; French Delegation of Police Cooperation Working Party, Enfopol 38 (I), 10; BSI, zitiert bei Lücke, Hayo: Studie: 60 Prozent der Firmen Opfer von Computer-Sabotage, Meldung des Internet-Portals teltarif.de vom 06.03.2003, www.teltarif.de/arch/2003/kw10/s10049.html.

249 In diese Richtung für Internetkriminalität BMI/BMJ, Sicherheitsbericht 2001, 197, wonach „von einem extrem großen Dunkelfeld ausgegangen werden" müsse.

250 Etwa BMI/BMJ, Sicherheitsbericht 2001, 198 für Internetkriminalität: „Bei Kriminalität im Internet kann von einem großen Dunkelfeld ausgegangen werden; entsprechende Dunkelfeldforschungen existieren bisher jedoch nicht. Insofern ist eine aussagekräftige Beschreibung des Phänomens anhand statistischer Zahlenwerte kaum möglich."

251 PricewaterhouseCoopers, Wirtschaftskriminalität 2003 (I), 11.

252 PricewaterhouseCoopers, Wirtschaftskriminalität 2003 (I), 11.

253 CSI/FBI, 2002 Survey (I), 20.

254 Zahlen bei Eisenberg, Kriminologie, § 44, Rn. 16 ff.: Das Dunkelfeld bei einfachen Diebstahlsdelikten betrage einer deutschen Untersuchung zufolge 89%, einer amerikanischen Studie zufolge 75% bei Gewaltkriminalität, einer britischen Studie zufolge 80% insgesamt, 83% bei Körperverletzung, 92% bei Sachbeschädigung; vgl. auch Kury, Kriminalistik 2001, 74 (78).

255 Kury, Kriminalistik 2001, 74 (78).

256 In diese Richtung aber BMI/BMJ, Sicherheitsbericht 2001, 201.

257 Kury, Kriminalistik 2001, 74 (78); BMI/BMJ, Sicherheitsbericht 2001, 160.

258 Kury, Kriminalistik 2001, 74 (78).

kelfeld auf dem Gebiet der Netzkriminalität kann man damit allenfalls dort sehen, wo ausschließlich das Vermögen oder Geschäftsgeheimnisse des Opfers von Netzkriminalität beschädigt wurden. Dabei handelt es sich nicht um höchstwertige Rechtsgüter, was im Rahmen der Abwägung von Bedeutung ist.

Es erscheint auch wahrscheinlich, dass Firmen ihre Geheimhaltungsinteressen zurückstellen, wenn es um wirklich hohe Summen geht oder wenn sie sich einer dauerhaften Gefahr ausgesetzt sehen. Für diese Annahme spricht, dass schwere Delikte generell eher angezeigt werden als leichte[259] und dass der Hauptgrund für das Absehen von einer Strafanzeige darin liegt, dass die betroffenen Personen den entstandenen Schaden als zu gering einschätzen als dass eine Anzeige lohnen würde[260]. Außerdem muss man anerkennen, dass geschädigte Firmen, die aus Gründen ihres guten Rufes von einer Anzeige absehen, insoweit regelmäßig rational und wohlbegründet handeln. Ein Ermittlungs- und Strafverfahren, von dem die Öffentlichkeit erfahren würde, könnte sie in der Tat mehr schädigen als ihnen die präventiven Wirkungen eines Strafverfahrens selbst im besten Fall nutzen könnten. Sind staatliche Ermittlungsverfahren in bestimmten Fällen aber nicht sinnvoll, dann kann ein insoweit bestehendes Dunkelfeld auch nicht angeführt werden, um weiter gehende staatliche Eingriffe im Ermittlungsverfahren zu legitimieren.

Dass die Anzahl von Fällen, in denen Straftaten durch das Opfer nicht erkannt werden, im Bereich der Netzkriminalität besonders hoch sein soll, ist nicht ersichtlich. Das Bundesamt für Sicherheit in der Informationstechnik schätzt, dass nur zehn Prozent aller Angriffe auf Unternehmen von diesen nicht erkannt werden[261]. Der Hauptgrund für das Dunkelfeld auf dem Gebiet der Netzkriminalität wird vielmehr in der mangelnden Anzeigebereitschaft liegen.

Zusammenfassend lässt sich sagen, dass ohne spezifische empirische Nachweise nicht davon ausgegangen werden kann, dass das Dunkelfeld im Bereich der Netzkriminalität größer ist als im Bereich anderer Kriminalität.

In Bezug auf die Höhe der Vermögensschäden durch Netzkriminalität liegen keine aussagekräftigen Daten vor[262]. Das Bundesamt für Sicherheit in der Informationstechnik gibt als jährlichen Gesamtschaden durch Computerkriminalität in Deutschland „einen hohen dreistelligen Millionenbetrag“ an[263]. Auf welche Quellen sich diese Schätzung stützt und inwieweit die angegebenen Schäden unter Verwendung von Telekommunikationsnetzen verursacht wurden, bleibt offen. Eine im Jahr 2003 durchgeführte Unternehmensbefragung ergab, dass 6% der beklagten Schäden durch Wirtschaftskriminalität auf Computerkriminalität zurückgeführt wurden[264]. Demgegenüber machte etwa Industriespionage 30% der angegebenen Schäden aus[265].

Absolute Zahlen benennt eine in den USA jährlich stattfindende, nicht repräsentative Umfrage über Computerkriminalität und -sicherheit[266]. Lässt man diejenigen der untersuchten Deliktsgruppen außer Acht, bei deren Begehung Telekommunikationsnetze von vornherein nicht (z.B. Laptopdiebstahl) oder kaum (z.B. Missbrauch von Internetzugängen durch Mitarbeiter) als Tatwerkzeug in Betracht kommen, dann wurden von den befragten Organisationen Schäden in Höhe von 389 Millionen US-$ im Jahre 2001 beklagt. Die Angabe von 389 Millionen US-$ kann einerseits zu niedrig sein, weil nur vergleichsweise wenige Organisationen befragt wurden. Sie kann aber auch zu hoch sein, weil sie lediglich auf freien Schätzungen der Organisationen beruht. Jedenfalls müsste jede Bezifferung in Relation zu anderen Zahlen gesetzt werden, etwa zu den gesamten Ausgaben oder Umsätzen der befragten Organisationen in dem betreffenden Jahr. So ist bekannt, dass der Kreditkartengesellschaft Mastercard 1999 durch Kreditkartenmissbrauch ein Verlust in Höhe von ca. 700 Millionen US-$ weltweit entstanden ist, dass dieser Schaden aber nur 0,1% der Kreditkartenumsätze ausmachte[267]. Im Jahr 2001 entstand übrigens allein in Deutschland und allein durch Diebstahl ein Schaden in Höhe von 2,2 Milliarden Euro[268].

259 Eisenberg, Kriminologie, § 44, Rn. 16.

260 Kury, Kriminalistik 2001, 74 (80).

261 BSI, zitiert bei Lücke, Hayo: Studie: 60 Prozent der Firmen Opfer von Computer-Sabotage, Meldung des Internet-Portals teltarif.de vom 06.03.2003, www.teltarif.de/arch/2003/kw10/s10049.html.

262 Holznagel, Bernd: Stellungnahme für die öffentliche Anhörung „Von der Industrie- zur Wissensgesellschaft: Wirtschaft, Arbeitswelt und Recht, Privatisierung und Patentierung von Wissen“, 08.10.2001, www.bundestag.de/gremien/welt/-weltto/weltto126_stell004.pdf, 22.

263 BSI, zitiert bei Lücke, Hayo: Studie: 60 Prozent der Firmen Opfer von Computer-Sabotage, Meldung des Internet-Portals teltarif.de vom 06.03.2003, www.teltarif.de/arch/2003/kw10/s10049.html.

264 PricewaterhouseCoopers, Wirtschaftskriminalität 2003 (I), 12.

265 PricewaterhouseCoopers, Wirtschaftskriminalität 2003 (I), 12.

266 CSI/FBI, 2002 Survey (I).

267 Kubica, Die Kriminalpolizei 9/2001.

268 BMI, PKS 2001 (I), 11.

Auch aus weiteren Gründen ist bei der Übertragung von Zahlen aus dem Gebiet der Computerkriminalität auf den Bereich der Netzkriminalität Vorsicht angebracht. Zwar wurde das Internet von 74% der befragten Firmen als häufiger Angriffspunkt genannt, interne Computer dagegen nur von 33%[269]. Dies bedeutet aber nicht, dass die zahlenmäßig selteneren Fälle internen Missbrauchs nicht für den Großteil der Schäden verantwortlich sein könnten. Zu vermuten ist, dass ein großer Teil der schadensträchtigen Computerkriminalität von Mitarbeitern oder ehemaligen Mitarbeitern eines Unternehmens begangen wird und dass der Zugriff mittels Telekommunikationsnetzen insoweit keine Rolle spielt, weil Mitarbeiter direkten Zugriff auf die Computeranlagen ihres Unternehmens haben und durch deren Nutzung vermeiden können, dass aufgrund der Zwischenschaltung von Telekommunikationsnetzen Datenspuren entstehen, die sie verraten könnten. Einer deutschen Untersuchung zufolge gehen zwei Drittel der Fälle von Computerkriminalität im engeren Sinne von Mitarbeitern oder ehemaligen Mitarbeitern des angegriffenen Unternehmens aus[270]. Eine US-amerikanische Umfrage kommt zu dem Ergebnis, dass mehr als 50% aller Fälle von Netzkriminalität auf internen Missbrauch zurückzuführen seien; außerdem seien die aufgetretenen Schäden in diesem Bereich besonders hoch[271]. Die oben zitierte, jährliche Umfrage unter US-amerikanischen Unternehmen und Organisationen ergab, dass sich 76% der befragten Unternehmen und Organisationen von ihren eigenen Mitarbeitern angegriffen fühlten[272] und dass immerhin 44% aller Schäden mit Telekommunikationsnetzrelevanz auf unbefugte Informationsabrufe zurückzuführen seien. Gerade unbefugte Informationsabrufe dürften besonders oft und besonders erfolgreich von den Mitarbeitern des betroffenen Unternehmens vorgenommen werden, weil diese entsprechendes Insiderwissen besitzen.

Die Höhe der Vermögensschäden, die gerade durch den Missbrauch von Telekommunikationsnetzen entstehen, darf daher nicht überschätzt werden, gerade im Verhältnis zu dem Aufwand, der mit der Einführung einer Vorratsspeicherung von Kommunikationsdaten verbunden wäre. Allgemein ist zu beobachten, dass sich die politische Diskussion auf Felder wie Wirtschaftskriminalität, Rauschgiftkriminalität, organisierte Kriminalität und jetzt auch Netzkriminalität konzentriert, obwohl diese Kriminalitätsfelder nur einen Bruchteil der Gesamtkriminalität ausmachen[273] und die Bürger im Vergleich zur Massenkriminalität nicht merklich beeinträchtigen.

(iv) Einschlägige Gemeinschaftsgüter im Bereich sonstiger Kriminalität

Weiterhin ist zu untersuchen, ob von den Telekommunikationsnetzen Gefahren ausgehen, wenn sie nicht unmittelbar als Werkzeug zur Begehung von Straftaten eingesetzt werden. In Betracht kommt zunächst die Nutzung durch Straftäter im Zusammenhang mit der Begehung traditioneller Straftaten, etwa als Hilfsmittel bei der Vorbereitung oder Begehung einer Straftat oder bei der Flucht, dem Absatz der Beute usw. Das klassische Beispiel in diesem Bereich ist das Mobiltelefon, dass sich bei Kriminellen offenbar größter Beliebtheit erfreut, weil es eine ständige Kommunikation mit Komplizen ermöglicht. Durch allgemeine Kriminalität können potenziell Rechtsgüter jeder Art gefährdet werden. Fraglich ist allerdings, ob es für die Begehung einer Straftat wirklich eine Rolle spielt, ob Telekommunikationsmöglichkeiten zur Verfügung stehen. Auch in diesem Bereich ist es problematisch, von der Nutzung des Mediums durch Straftäter darauf zu schließen, dass ohne die Telekommunikationsnetze weniger Straftaten begangen würden.

Der Zugriff auf Kommunikationsdaten ist schließlich nicht nur dann von Bedeutung, wenn Telekommunikationsnetze im Zusammenhang mit einer Straftat genutzt wurden. Es geht vielmehr oft um das Überführen oder Auffinden Beschuldigter anhand von deren allgemeiner Telekommunikationsnutzung, die sich von der jedes anderen Bürgers nicht unterscheidet. In dieser Fallkonstellation, die sogar die Mehrzahl der Zugriffe auf Telekommunikationsdaten ausmachen könnte, lässt sich nicht sagen, dass von der Telekommunikationsnutzung Gefahren ausgehen. Zwar mag von der Person, gegen die ermittelt wird, eine Gefahr ausgehen, zu deren Beseitigung das Auffinden und Überführen der Person erforderlich sein mag. Diese Gefahr würde aber auch dann bestehen, wenn der Beschuldigte auf die Telekommunikationsnutzung verzichten würde, so dass den Telekommunikationsnetzen in diesen – zahlenmäßig bedeutenden – Fällen kein eigenständiges Gefährdungspotenzial zugeschrieben werden kann. Nichtsdestotrotz ist der Zugriff auf Telekommunikationsdaten in diesem Bereich geeignet, Rechtsgüter aller Art vor strafbaren Angriffen zu schützen.

269 CSI/FBI, 2002 Survey (I), 8.

270 Thomas Eßer (Mummert Consulting), zitiert bei Lücke, Hayo: Studie: 60 Prozent der Firmen Opfer von Computer-Sabotage, Meldung des Internet-Portals teltarif.de vom 06.03.2003, www.teltarif.de/arch/2003/kw10/s10049.html.

271 Symantec, Symantec Internet Security Threat Report (I), 5.

272 CSI/FBI, 2002 Survey (I), 9.

273 Dietel, Innere Sicherheit, 63.

(v) Zwischenergebnis

Als Zwischenergebnis bleibt festzuhalten, dass eine Gefährdung der Allgemeinheit oder der physischen Sicherheit einzelner Bürger durch die Nutzung von Telekommunikationsnetzen kaum denkbar ist. Gefährdet ist vielmehr vorwiegend das Vermögen Einzelner, also ein Rechtsgut von vergleichsweise geringerem Gewicht. In wie vielen Fällen und in welchem Ausmaß durch die Nutzung von Telekommunikationsnetzen tatsächlich Rechtsgüter geschädigt werden, ist noch nicht empirisch untersucht worden. Wo Rechtsgüter anders als durch Nutzung von Telekommunikationsnetzen gefährdet werden, kann der Zugriff auf Telekommunikationsdaten in einzelnen Fällen der Abwendung von Gefahren für Rechtsgüter jeder Art dienen.

(bb) Maß an Eignung zur Begegnung der Gefahren

Nachdem festgestellt wurde, welche Rechtsgüter durch die Einführung einer generellen Vorratsspeicherung von Telekommunikationsdaten geschützt werden könnten, stellt sich die Frage nach dem praktischen Nutzen einer solchen Maßnahme. Bei der Untersuchung dieser Frage ist zweckmäßigerweise danach zu unterscheiden, zu welchem Zweck ein Zugriff auf Kommunikationsdaten erfolgt. Fraglich ist, in welchem Maße der Zugriff auf Kommunikationsdaten für die einzelnen Behördenzweige von Bedeutung ist.

Den Schwerpunkt wird man eindeutig im Bereich der Strafverfolgung sehen müssen[274]. Nicht umsonst hat schon § 142 der Paulskirchenversammlung von 1848 Ausnahmen von dem Briefgeheimnis nur und gerade für „strafgerichtliche Untersuchungen und in Kriegsfällen“ zugelassen. Auch auf der nationalen und internationalen Bühne – dort insbesondere im Rahmen des Europarats, der EU und der G8 – konzentrieren sich die Diskussionen und Anstrengungen auf das Gebiet der Strafverfolgung. Schließlich hat es der Polizeigesetzgeber – von Ausnahmen abgesehen – bisher nicht für erforderlich gehalten, die Gefahrenabwehrbehörden zu ermächtigen, auf Kommunikationsdaten zuzugreifen.

Zu beachten ist allerdings, dass sich die Bereiche der Gefahrenabwehr und der Strafverfolgung oft überschneiden, weil die Gefährdung von Rechtsgütern oft strafbar ist. Jedenfalls die vorsätzliche Gefährdung von Rechtsgütern wird durch das Strafrecht weitgehend abgedeckt, so dass eine „reine“ Gefahrenabwehr im Wesentlichen nur im Bereich fahrlässiges Verhaltens oder unverschuldeter Gefahren denkbar ist. Dass in diesen, schon für sich genommen wenig relevanten Bereichen ein Zugriff auf Kommunikationsdaten erforderlich werden könnte, ist kaum denkbar.

Im Bereich strafbarer Handlungen sind die praktischen Möglichkeiten der Gefahrenabwehrbehörden, die zukünftige Begehung einer Straftat zu verhindern, gering[275]. Eine Gefahrenabwehr wird daher in der Praxis ganz regelmäßig in der Form erfolgen, dass die weitere Begehung einer strafbaren Handlung unterbunden und in dieser Weise zugleich die dadurch verursachte Gefahr beseitigt wird. Beispielsweise könnte im Fall einer Entführung der Zugriff auf die Mobiltelefon-Positionsdaten des Opfers erforderlich werden, um das Opfer zu befreien und zugleich den Täter festzunehmen.

Der Zugriff auf Telekommunikationsdaten ist somit vor allem im Bereich strafbarer Handlungen erforderlich, so dass sich die folgenden Ausführungen auf dieses Feld konzentrieren.

Bei der Diskussion um erweiterte informationelle Eingriffsbefugnisse wird regelmäßig – meist unausgesprochen[276], manchmal ausdrücklich[277] – vorausgesetzt, dass eine verstärkte Strafverfolgung dem Rechtsgüterschutz dient. Nur selten wird problematisiert, ob dies überhaupt der Fall ist, in welchem Maße präventive Wirkungen infolge einer Eingriffsbefugnis zu erwarten sind und wie sich dieser Nutzen zu dem Ausmaß an unerwünschten Folgen der Befugnis verhält. Um diese Problematik näher zu beleuchten, soll an dieser Stelle zunächst näher auf kriminologische Erkenntnisse über die Wirksamkeit der Strafverfolgung eingegangen werden.

(i) Empirische Erkenntnisse über den Nutzen von Strafverfolgung

Präventive Wirkungen kann die Strafverfolgung einerseits dadurch entfalten, dass Straftäter an der Begehung weiterer Straftaten gehindert werden oder freiwillig davon absehen (Spezialprävention). Daneben könnten Strafverfahren auch Personen, die von Strafverfahren gegen andere Kenntnis erlangen, von der Begehung von Straftaten abhalten (Generalprävention).

274 L/D3-Bäumler, J 536 und 679.

275 L/D3-Bäumler, J 535; Kube, Edwin (BKA-Abteilungspräsident), zitiert bei Feltes, Fehlerquellen im Ermittlungsverfahren (I): Die Polizei sei nicht in der Lage, „einen nennenswerten Anteil der Gesamtkriminalität zu verhüten“.

276 Etwa Bayern und Thüringen in ihrem Gesetzesantrag, BR-Drs. 1014/01 (Entwurf eines Gesetzes zur Verbesserung des strafrechtlichen Instrumentariums für die Bekämpfung des Terrorismus und der Organisierten Kriminalität), 1.

277 Etwa LINX, Traceability (I), Punkt 1: „Of course, the ability to trace actions back to their source will, in itself, discourage unreasonable behaviour.“

Im Bereich der Spezialprävention kann das Strafverfahren zunächst im Wege unmittelbaren Zwangs präventiv wirken. So kann eine freiheitsentziehende Untersuchungsmaßnahme, Strafe oder Maßnahme der Besserung und Sicherung (§§ 61 ff. StGB) dem Täter bereits die Möglichkeit nehmen, in dieser Zeit fremde Rechtsgüter zu gefährden. Neben der Verhinderung zukünftiger Straftaten kann das Strafverfahren auch die weitere Begehung einer noch nicht vollendeten Straftat unterbinden (vgl. etwa §§ 23, 24, 30 Abs. 2, 127 ff. StGB) oder wenigstens den Eintritt weiterer Schäden und Gefahren infolge einer bereits vollendeten Straftat verhindern. Dies kann beispielsweise im Wege der Festnahme des Täters erfolgen. Auch eine Restitution des Geschädigten kann erfolgen, etwa durch die Rückgabe betrügerisch erlangter Gegenstände.

Während diese Aspekte des Rechtsgüterschutzes durch Strafverfolgung theoretisch auf der Hand liegen, ist für die verfassungsrechtliche Abwägung ihr tatsächliches Gewicht maßgeblich. Dieses bestimmt sich danach, ob und in welchem Maße die erwünschten präventiven Effekte tatsächlich eintreten. Was eine mögliche Restitution des Geschädigten anbelangt, so ist nicht bekannt, in wie vielen Fällen und in welchem Maße eine Restitution infolge eines strafrechtlichen Ermittlungsverfahrens gegenwärtig stattfindet. An den Geschädigten zurückgegeben werden kann jedenfalls nur Vermögen. Da strafbare Zugriffe auf fremdes Vermögen regelmäßig erfolgen werden, um das erlangte Vermögen zu eigenen Zwecken einzusetzen, wird dieses oft nicht mehr vorhanden sein. Da außerdem zu vermuten ist, dass Straftäter nur selten über nennenswertes eigenes Vermögen verfügen, wird auch eine Restitution im Wege des Schadensersatzes zumeist ausscheiden.

Weiterhin ist der Nutzen einer Inhaftierung von Straftätern zu betrachten. Dass eine eingesperrte Person während der Haftzeit regelmäßig keine Straftaten begehen kann, steht fest[278]. Dennoch sind Auswirkungen des amerikanischen Konzepts der „Incapacitation“ auf das allgemeine Kriminalitätsniveau nicht nachgewiesen[279]. Wegen der großen Zahl von Kleinkriminellen und der beschränkten Anzahl an Gefängnisplätzen ist der Nutzen einer „Verwahrung“ jedenfalls bei weniger schwer wiegenden Delikten gering[280]. Auch eine Beschränkung des Freiheitsentzugs auf besonders gefährliche Straftäter ist praktisch nicht durchführbar, weil sich die zukünftige Straffälligkeit von Straftätern nicht prognostizieren lässt[281]. Gegen jeden potenziell gefährlichen Straftäter eine Gefängnisstrafe zu verhängen, ist schon wegen der hohen Kosten der Vollstreckung von Freiheitsstrafen unmöglich.

Gerade auf dem Gebiet der organisierten Kriminalität ist außerdem die Annahme plausibel, dass es einen lukrativen Markt für bestimmte kriminelle Aktivitäten gibt und dass „unschädlich gemachte“ Straftäter alsbald durch andere Personen ersetzt werden. Hinzu kommen die kontraproduktiven Effekte des Freiheitsentzugs auf Insassen[282]: Die Vertrautheit mit dem Übel der Freiheitsstrafe kann deren abschreckende Wirkung für die Zukunft vermindern[283]. Gerade ein Aufenthalt in einer Justizvollzugsanstalt kann dazu führen, dass jemand zum Wiederholungstäter wird[284]. Überreaktionen von staatlichem Personal können auf Täter stigmatisierend wirken[285]. Die Erfahrung von Demütigung ist ein wichtiges Motiv gerade von Terroristen[286]. Im Übrigen spricht das Beispiel der USA gegen die Annahme, ein verstärkter Freiheitsentzug könne das Kriminalitätsniveau senken. Obwohl sich in den USA ein weltweit nahezu einmaliger Anteil der Bevölkerung im Freiheitsentzug befindet, ist die Kriminalität laut Statistik erheblich höher als in Deutschland[287].

Was die möglichen Auswirkungen des Strafverfahrens auf den freien Entschluss von Straftätern in Bezug auf die zukünftige Begehung weiterer Straftaten angeht, so gibt es trotz intensiver Forschung weltweit keinen empirischen Beleg für die Annahme, dass eine Verurteilung in spezialpräventiver Hinsicht einer Verfahrenseinstellung überlegen sein könnte[288]. Ebenso wenig erwiesen ist, dass die Bekanntgabe eines Ermittlungsverfahrens an eine Person spezialpräventiv wirken könnte.

Letztlich lässt sich also nicht feststellen, dass das Betreiben eines Ermittlungs-, Gerichts- oder Strafvollstreckungsverfahrens irgendeine spezialpräventive Wirkung auf den jeweiligen Beschuldigten,

278 BMI/BMJ, Sicherheitsbericht 2001, 381.
279 Sherman u.a.-Sherman, Preventing Crime, 44: „Recent reviews conclude there is very little evidence that increased incarceration has reduced crime“.
280 Diekmann, Die Befolgung von Gesetzen, 149.
281 Sherman u.a.-MacKenzie, Preventing Crime, 431.
282 BMI/BMJ, Sicherheitsbericht 2001, 381.
283 Kunz, Kriminologie, § 31, Rn. 17.
284 Kunz, Kriminologie, § 31, Rn. 17.
285 Schneider, Kriminologie, 324.
286 Limbach, Jutta: Ist die kollektive Sicherheit Feind der individuellen Freiheit? 10.05.2002, www.zeit.de/reden/-Deutsche%20Innenpolitik/200221_limbach_sicherheit.html; Rötzer, Florian: Armut ist keine Ursache für den Terrorismus, Telepolis, Heise-Verlag, 01.08.2002, www.heise.de/tp/deutsch/inhalt/co/13015/1.html.
287 Bottger/Pfeiffer, ZRP 1994, 7 (14).
288 BMI/BMJ, Sicherheitsbericht 2001, 382.

Angeklagten oder Verurteilten hat. Dass sich spezialpräventive Wirkungen der Strafverfolgung nicht empirisch belegen lassen, bedeutet zwar nicht zwangsläufig, dass sie nicht existieren[289]. Wenn sich für eine Theorie aber trotz beträchtlichen Aufwands über Jahrzehnte keine Belege haben finden lassen, dann muss diese Theorie als gescheitert bezeichnet werden[290].

Was eine mögliche generalpräventive Wirkung der Strafverfolgung anbelangt, so kommen einige der vielen empirischen Untersuchungen auf diesem Gebiet zu dem Ergebnis, dass ein gewisser Einfluss des subjektiv angenommenen Entdeckungsrisikos auf die Delinquenz nachweisbar sei[291]. Anerkannt ist dies jedoch nur bei einigen minder schweren Delikten[292]. Anderen einschlägigen Forschungsergebnissen zufolge sollen keinerlei generalpräventive Wirkungen der Erwartung, bei Begehung einer Straftat bestraft zu werden, feststellbar sein[293]. Die geringe oder fehlende Bedeutung des subjektiv angenommenen Entdeckungsrisikos lässt sich mit der empirisch gewonnenen Erkenntnis erklären, dass Straftäter das Entdeckungsrisiko bei ihrer Entschlussfassung nur selten berücksichtigen[294].

Den genannten Untersuchungen ist gemeinsam, dass eine generalpräventive Wirkung der wahrgenommenen Sanktionswahrscheinlichkeit, sofern sie überhaupt existiert, gering und im Vergleich zu anderen Faktoren minimal ist[295]. So spielt der Grad der Abweichung eines strafbaren Verhaltens von sozialen Normen sowie die soziale Integration einer Person eine erheblich größere Rolle für den Entschluss, eine Straftat zu begehen oder nicht, als die wahrgenommene Sanktionswahrscheinlichkeit[296]. Daneben gibt es eine Vielzahl weiterer Faktoren, die jeweils für sich genommen erheblich bedeutsamer für die Delinquenz sind als die Sanktionswahrscheinlichkeit, etwa der von dem Delikt erhoffte Nutzen, die soziale Bezugsgruppe einer Person, ihr Einkommen, ihre etwaige Arbeitslosigkeit[297], ihre Freizeittätigkeiten, ihre individuellen Moralvorstellungen[298], vermutete negative Reaktionen des Umfelds auf eine Straftat, die Delinquenz in der Vergangenheit, gerichtliche Vorverurteilungen und das Ausmaß der im Bekanntenkreis beobachteten Kriminalität[299]. Im Vergleich zur Bedeutung dieser Faktoren ist der Einfluss der empfundenen Sanktionswahrscheinlichkeit nicht nennenswert[300]. Dass ein potenzieller Straftäter von seinem Vorhaben absieht, weil er damit rechnet, dass ihn die Polizei überführen kann, ist mithin selten[301].

Überdies würde der Versuch, das subjektiv angenommene Entdeckungsrisiko durch eine verstärkte Strafverfolgung zu erhöhen, schon daran scheitern, dass potenzielle Straftäter das objektive Entdeckungsrisiko beziehungsweise die tatsächliche Aufklärungsrate nicht kennen[302] und ihr Verhalten folglich nicht daran ausrichten können. In den USA hat man etwa versucht, das subjektiv wahrgenommene Entdeckungsrisiko durch eine stete Ausweitung der Ermittlungsbefugnisse zu steigern[303]. Ein kriminalitätssenkender Einfluss dieser Strategie ist jedoch nicht zu erkennen. In der Bevölkerung wird das Entdeckungsrisiko ohnehin durchgehend weit überschätzt[304], so dass selbst ein objektiv gesteigertes Entdeckungsrisiko noch hinter dem subjektiv wahrgenommenen zurückbleiben würde[305].

Man muss danach annehmen, dass die generalpräventive Abschreckungswirkung der Strafverfolgung im Wesentlichen dadurch ausgeschöpft wird, dass sich potenzielle Straftäter einem gewissen Entdeckungsrisiko ausgesetzt sehen. Solange die Bevölkerung nicht den Eindruck hat, eine Strafverfolgung sei in bestimmten Bereichen generell ausgeschlossen, kommt es auf das tatsächliche Ausmaß an Strafverfolgung für das allgemeine Kriminalitätsniveau also nicht an. Dass die Entscheidung einer Person für oder gegen eine Straftat von einer um einige Prozentpunkte höheren oder niedrigeren Entdeckungswahrscheinlichkeit abhängen könnte, ist nicht plausibel. Ob die Aufklärungsrate 10 oder 20%

289 Göppinger, Kriminologie, 179.
290 Niggli, Kriminologische Überlegungen zur Strafzumessung (I), 8 für die negative Spezial- und Generalprävention.
291 Diekmann, Die Befolgung von Gesetzen, 129 und 133.
292 BMI/BMJ, Sicherheitsbericht 2001, 382.
293 Kunz, Kriminologie, § 30, Rn. 15; Eisenberg, Kriminologie, § 41, Rn. 6; Diekmann, Die Befolgung von Gesetzen, 131; Bönitz, Strafgesetze und Verhaltenssteuerung, 329.
294 Kunz, Kriminologie, § 30, Rn. 19; Niggli, Kriminologische Überlegungen zur Strafzumessung (I), 9.
295 Feltes, MschrKrim 1993, 341 (344 f.); Bönitz, Strafgesetze und Verhaltenssteuerung, 329.
296 Diekmann, Die Befolgung von Gesetzen, 133; Feltes, MschrKrim 1993, 341 (344 f.).
297 Diekmann, Die Befolgung von Gesetzen, 133.
298 Feltes, MschrKrim 1993, 341 (344 f.).
299 Bönitz, Strafgesetze und Verhaltenssteuerung, 329.
300 Bönitz, Strafgesetze und Verhaltenssteuerung, 329.
301 L/D3-Bäumler, J 535.
302 Kunz, Kriminologie, § 30, Rn. 20; Eisenberg, Kriminologie, § 41, Rn. 9; Niggli, Kriminologische Überlegungen zur Strafzumessung (I), 9.
303 Rohe, Verdeckte Informationsgewinnung mit technischen Hilfsmitteln zur Bekämpfung der Organisierten Kriminalität, 47.
304 Kunz, Kriminologie, § 30, Rn. 20; Bönitz, Strafgesetze und Verhaltenssteuerung, 329.
305 Kunz, Kriminologie, § 30, Rn. 20.

beträgt, wird für den Entschluss einer Person, eine Straftat zu begehen, keine Rolle spielen. In höherem Maße als um einige Prozentpunkte ließe sich die Ermittlungserfolgsrate realistischerweise nicht steigern. In Übrigen werden die Kosten einer Steigerung der Aufklärungsrate um nur 1% auf eine halbe Milliarde Euro geschätzt[306].

Gemessen an dem genannten Maßstab ist es auf dem Gebiet des Zugriffs auf Telekommunikationsdaten vollkommen ausreichend, wenn in einzelnen Fällen die Aufbewahrung von Telekommunikationsdaten zur Strafverfolgung angeordnet werden kann, wie es in der Cybercrime-Konvention des Europarates für Verbindungen zum Datenaustausch vorgesehen ist und in den USA allgemein praktiziert wird. Bereits dadurch können sich potenzielle Straftäter vor einer Entdeckung nicht sicher fühlen. Darüber hinaus gehende generalpräventive Wirkungen durch eine generelle Vorratsspeicherung aller Kommunikationsdaten sind nach dem Gesagten nicht ernsthaft zu erwarten, zumal jeder rational planende Kriminelle eine solche Maßnahme leicht umgehen könnte[307].

Fasst man die Forschungsergebnisse bezüglich möglicher präventiver Wirkungen des Strafrechts zusammen, so ist festzuhalten, dass solche Wirkungen auf keinem Gebiet zweifelsfrei empirisch belegbar sind[308]. Ob man daraus den Schluss ziehen kann, das Strafrecht sei überhaupt sinnlos[309], kann dahinstehen. Jedenfalls sind im Bereich der Strafverfolgung angesichts der genannten Erkenntnisse nur entschieden mildere Eingriffsbefugnisse angemessen als bei der Abwehr konkreter Gefahren[310]. Der Gesetzgeber muss diese Abstufung auch abstrakt nachvollziehen. Bei der Einräumung von Befugnissen darf er nicht allzu sehr generalisieren, sondern muss bereichsspezifisch unterschiedliche Eingriffsschwellen vorsehen.

Die unterschiedlichen Anforderungen dürfen auch nicht dadurch umgangen werden, dass die Verwendung von Erkenntnissen, die im Rahmen der Gefahrenabwehr gewonnen wurden, ohne Weiteres auch für Zwecke der Strafverfolgung erlaubt wird[311]. Es ist ein Wertungswiderspruch, wenn die Kenntnisnahme personenbezogener Informationen mit Gefahren für höchste Rechtsgüter legitimiert wird, die Verwendung der Kenntnisse aber dann schon zur Verfolgung von geringwertigen Zwecken zulässig sein soll[312]. Aus Sicht der Betroffenen macht es keinen Unterschied, ob bereits erhobene Daten zu einem „Sekundärzweck“ verwertet werden oder ob die Daten überhaupt erst zu diesem Zweck erhoben werden („Primärzweck“). In beiden Fällen ist der Betroffene gleichermaßen belastet, beispielsweise durch Verwicklung in ein strafrechtliches Ermittlungsverfahren, möglicherweise auch zu Unrecht. Die Sicht des Betroffenen ist die maßgebliche, wenn es um die Beurteilung der Verhältnismäßigkeit einer Maßnahme geht, denn dabei ist die Belastung der Betroffenen gegen den Nutzen der Maßnahme abzuwägen. Das wiederum zwingt zu dem Schluss, dass ein Eingriff in Art. 10 Abs. 1 Var. 3 GG durch Zweitverwertung von Daten nur zulässig ist, wenn auch die erstmalige Erhebung der Daten allein zu diesem Zweck und auf dieselbe Weise verhältnismäßig gewesen wäre[313]. Dem tragen bestehende Normen bisher keine Rechnung.

(ii) Möglicher Nutzen einer Erweiterung der Befugnisse der Strafverfolgungsbehörden

Fraglich ist, ob und in welchem Maße erweiterte informationelle Eingriffsbefugnisse in Strafverfahren den Rechtsgüterschutz stärken können. Vorab ist festzuhalten, dass eine Ausweitung informationeller Eingriffsbefugnisse hohe Kosten verursachen kann, etwa Fortbildungskosten oder Kosten für die Anschaffung technischer Einrichtungen. Soweit der Staat die Kosten trägt, können der originären Kriminalpräventionsarbeit auf diese Weise Mittel vorenthalten werden. Weil die Bekämpfung der Ursachen von Kriminalität vielversprechender ist als Maßnahmen der Strafverfolgung[314], sind Mittelverlagerungen in den Bereich der Strafverfolgung kontraproduktiv. Zwar lässt sich vortragen, ohne die Möglichkeit einer Bestrafung könne keine alternative Vorbeugungsstrategie auskommen[315]. Die Strafverfolgung kann aber stets nur das letzte Mittel der Kriminalitätskontrolle sein[316]. Alles andere wäre eine Überschätzung ihrer präventiven Wirkungen, denn Strafverfolgung ist per definitionem primär auf

306 Feltes, MschrKrim 1993, 341 (350); vgl. auch Sherman u.a.-MacKenzie, Preventing Crime, 430 f.
307 Eckhardt, CR 2002, 770 (774).
308 Niggli, Kriminologische Überlegungen zur Strafzumessung (I), 7.
309 Nachweise bei Kaiser, Kriminologie, 103; Eisenberg, Kriminologie, § 41, Rn. 17 und § 42, Rn. 11.
310 Vgl. BVerfGE 100, 313 (394 ff.); vgl. auch Art. 13 Abs. 3 und 4 GG; ebenso Schenke, AöR 125 (2000), 1 (29); Schenke, JZ 2001, 997 (997); dagegen AK-GG-Bizer, Art. 10, Rn. 95.
311 BVerfGE 100, 313 (389 f.).
312 So aber das BVerfG in E 100, 313 (373 ff.); vgl. auch Art. 13 Abs. 5 S. 2 GG.
313 Gusy, KritV 2000, 52 (63); L/D3-Bäumler, J 719; so jetzt auch BVerfGE 109, 279 (377) und BVerfG, NJW 2004, 2213 (2221).
314 Travis Hirschi, zitiert bei Kunz, Kriminologie, § 34, Rn. 3; Schneider, Kriminologie, 325; Diekmann, Die Befolgung von Gesetzen, 151.
315 Schneider, Kriminologie, 336.
316 Schneider, Kriminologie, 336.

nachträgliche Repression in einzelnen Fällen angelegt[317]. Dies wird etwa an den Vorschriften des Strafgesetzbuches über die Strafzumessung deutlich, die in erster Linie auf die Schuld des Täters abstellen (§ 46 Abs. 1 S. 1 StGB) und erst in zweiter Linie auf die Auswirkungen der Strafe (§ 46 Abs. 1 S. 2 StGB).

Gegen die Annahme, dass eine Erweiterung der Eingriffsbefugnisse im Strafverfahren eine kriminalitätssenkende Wirkung haben könnte, sprechen zunächst die in Deutschland auf politischer Ebene gemachten Erfahrungen. Nach der Auflösung des Polizeistaates des Dritten Reiches wurden in Deutschland vorhandene Überwachungsstrukturen zunächst zerschlagen. Seit 1968 wurde das Maß an informationellen Eingriffsbefugnissen wieder zusehends gesteigert, unter anderem um die Durchsetzung des Strafrechts zu erleichtern. Fundamentale Prinzipien wie die Unschuldsvermutung, das Trennungsprinzip, die Offenheit staatlicher Ermittlungen und die Konzentration von Maßnahmen auf Verdächtige sind immer weiter eingeschränkt worden[318], ohne dass jedoch ein Einfluss dieser Änderungen auf das Kriminalitätsniveau feststellbar wäre. Strafverfolgungsbehörden verweisen zwar auf – teilweise spektakuläre – Einzelfälle, die mit Hilfe der verschiedenen Befugnisse gelöst worden seien. Jedoch können solche Einzelfälle oder Erledigungsstatistiken nichts über die Frage aussagen, ob Auswirkungen von Befugniserweiterungen auf das Kriminalitätsniveau spürbar sind.

Dies ist, soweit ersichtlich, nicht der Fall. Trotz aller bisher erfolgten Befugniserweiterungen bestehen die gravierenden Strafverfolgungsdefizite, die allseits beklagt werden, unverändert fort. Als chronische Strafverfolgungsdefizite sind die großen Dunkelfelder und die geringen Aufklärungsquoten zu nennen, besonders auf den zentralen Gebieten modernen Strafrechts wie in den Bereichen der organisierten Kriminalität und Wirtschaftskriminalität[319]. Gerade Fälle der schwersten und folgenreichsten Kriminalität kommen höchst selten zur Anklage und zur Verurteilung, obwohl sie am sozialschädlichsten sind[320]. Selbst wenn es zu einer Anklage kommt, dauern Prozesse oft jahrelang und ziehen in den allermeisten Fällen allenfalls Geld- oder Bewährungsstrafen nach sich[321]. Auf dem Gebiet der Betäubungsmittelkriminalität ist es der Strafverfolgung offensichtlich nicht gelungen, eine merkliche Eindämmung des Drogenhandels und damit auch der Begehung entsprechender Straftaten zu erreichen. Im Bereich der Computerkriminalität kommt ein deutsches Gutachten zum Thema Datenpiraterie zu dem Ergebnis, „dass rechtliche Instrumentarien die Verbreitung der Raubkopien [...] nicht nennenswert verhindern. Das Ausmaß der in der Praxis festzustellenden Raubkopien steht in eklatantem Widerspruch zu den bisherigen rechtlichen Erfolgen“[322].

Eine Ursache für die Vollzugsdefizite kann darin liegen, dass die Strafverfolgung aus politischen Gründen auf vorweisbare Erfolge angewiesen ist, wobei in der Statistik jeder erledigte Fall gleich viel zählt. Dadurch kann es zu einer Konzentration auf leicht zu erledigende Kleinkriminalität kommen, wohingegen Fälle der schwersten, folgenreichsten und sozial schädlichsten Kriminalität nur höchst selten zur Anklage und Verurteilung gebracht werden[323].

Als weitere Ursache für die Vollzugsdefizite kommt die ständige Ausdehnung des Strafrechts in Betracht. Das Strafrecht beschränkt sich nicht mehr auf die klassische Sicherung eines „ethischen Minimums“[324], also den Schutz konkreter Rechtsgüter. Es soll Rechtsgüter vielmehr bereits im Vorfeld vor vielfältigen Gefahren schützen und wird damit zu einem politischen Steuerungsinstrument auf nahezu allen Gebieten, etwa der Subventions- und Umweltpolitik, der Gesundheits- und Außenpolitik[325]. Kaum ein neues Gesetz kommt ohne einen Annex von Strafnormen zu seiner Durchsetzung aus. Dabei wird das Strafrecht oft nicht als letztes Mittel, sondern häufig als erstes oder sogar einziges Mittel zur Durchsetzung von Normen vorgesehen[326]. Obwohl den Ermittlungsbehörden, denen oft keine ausreichende Sachkenntnis und keine hinreichenden Mittel zur Verfügung stehen, Straftaten auf solchen Nebengebieten nur ganz ausnahmsweise bekannt werden und diese damit nur selten verfolgt werden können, scheint der Glaube an das Strafrecht als „Allzweckwaffe“[327] zur Lösung gesellschaftlicher Konflikte fortzubestehen und die Flut neuer Strafnormen nicht nachzulassen. Unter dem Aspekt des Grundsatzes der Gleichmäßigkeit der Strafverfolgung kann es nicht angehen, dass unter einer Masse

317 Kunz, Kriminologie, § 31, Rn. 41; Hassemer, Strafen im Rechtsstaat, 277.
318 Hassemer, Strafen im Rechtsstaat, 255.
319 Hassemer, Freiheitliches Strafrecht, 226 f.
320 Kunz, Kriminologie, § 35, Rn. 2; Hassemer, Freiheitliches Strafrecht, 226 f.
321 Albrecht, Die vergessene Freiheit, 168.
322 Sieber, Gutachten zum Thema Datenpiraterie (I).
323 Kunz, Kriminologie, § 35, Rn. 2 ff.; DG Research, Economic risks arising from the potenzial vulnerability of electronic commercial media to interception (I); Hassemer, Freiheitliches Strafrecht, 226 f.
324 Hassemer, Strafen im Rechtsstaat, 185.
325 Hassemer, Strafen im Rechtsstaat, 185.
326 Hassemer, Strafen im Rechtsstaat, 197.
327 Hassemer, Strafen im Rechtsstaat, 197.

rechtswidrig handelnder Personen nur wenige exemplarisch abgestraft werden, die übrigen dagegen nicht erreichbar sind.

Die Folgerung liegt nahe, dass das Strafrecht schlicht nicht in der Lage ist, in großflächigen Problemlagen Abhilfe zu schaffen, wie sie beispielsweise auf den Gebieten Drogen, Wirtschaft und Umwelt existieren[328]. Es ist als Instrument insoweit vergleichsweise schlecht geeignet[329]: Das Strafrecht ist vergangenheitsgerichtet und erlaubt keine konkreten Maßnahmen zur Vorbeugung von Schäden. Es ist auf die Bestrafung einzelner Täter gerichtet und in seinen Wirkungen entsprechend beschränkt. Das Strafverfahren braucht Zeit; rasche Reaktionen sind kaum möglich. Vielfältige Beschränkungen bei der Sachverhaltsermittlung und die Unschuldsvermutung führen dazu, dass das strafrechtliche Instrumentarium in den weitaus meisten Fällen nicht zum Zug kommt.

Das Strafrecht kann die hohen Erwartungen an seine Wirksamkeit daher zwangsläufig nicht erfüllen. Zur Prävention ist es schon seiner Eigenart nach – wenn überhaupt – nur sehr beschränkt und mittelbar in der Lage. Die meisten Faktoren, die in der Wissenschaft als mögliche Entstehungsgründe für Kriminalität diskutiert werden, sind in Strafverfahren nicht oder kaum beeinflussbar[330], und entsprechend der oben genannten Forschungsergebnisse verspricht eine gegenüber dem bestehenden Maß verschärfte Strafverfolgung weder in general- noch in spezialpräventiver Hinsicht nennenswerten Erfolg[331].

Dieser Befund steht nicht im Widerspruch zu der Annahme, dass die völlige Entkriminalisierung eines sozial schädlichen Verhaltens dessen Ausweitung zur Folge hätte. Diese Hypothese lässt ebenso wenig auf die Wirkung erweiterter Ermittlungsbefugnisse schließen wie auf den Nutzen härterer Strafen: Empirisch widerlegt ist bekanntlich der – von der Alltags- und Lebenserfahrung nahe gelegte und von vielen Bürgern als richtig unterstellte – Schluss, dass eine härtere Bestrafung das Kriminalitätsniveau senken könnte. Wenn zum Beleg für die Behauptung, dass die Einführung neuer Ermittlungsbefugnisse typischerweise einen positiven Einfluss auf die Aufklärungsquote habe, auf die Erfahrungen der Eingriffsbehörden verwiesen wird, ist daher zu entgegnen, dass subjektive Einschätzungen keine zuverlässige Beurteilungsgrundlage darstellen. Überdies hat ein internationaler Vergleich der Telekommunikationsüberwachung ergeben, dass „Struktur und Entwicklungen der von der Überwachung der Telekommunikation besonders betroffenen Kriminalitätsbereiche [...] im Vergleich der Länder keine Rückschlüsse darauf [zulassen], dass die Häufigkeit der Anordnung der Überwachung der Telekommunikation mit einer effizienteren Kontrolle der davon erfassten Kriminalitätsbereiche korreliert."[332]

Dieses Ergebnis widerlegt auch die Annahme, dass Ermittlungsbefugnisse, wenn sie die Kriminalität schon nicht eindämmen, wenigstens ihre Ausweitung verhinderten. Im zeitlichen und internationalen Vergleich ist nicht feststellbar, dass geringere Ermittlungsbefugnisse ein höheres Kriminalitätsniveau zur Folge haben. Plausibel – wenn auch mangels praktischer Beispiele nicht erwiesen – ist lediglich die Annahme, dass ein höheres Kriminalitätsniveau zu befürchten wäre, wenn potenzielle Straftäter den Eindruck hätten, eine Strafverfolgung sei in bestimmten Bereichen generell ausgeschlossen[333]. Mehr als ein Mindestmaß an Eingriffsbefugnissen lässt sich damit aber nicht legitimieren.

Soweit ersichtlich hat noch niemand auch nur einen Einfluss der Aufklärungsquote auf die Anzahl der registrierten Straftaten feststellen können. Das bedeutet, dass man selbst dann nicht selbstverständlich von einem Nutzen zusätzlicher Ermittlungsbefugnisse ausgehen könnte, wenn fest stünde, dass diese die Aufklärungsquote erhöhten. Ist schon eine Korrelation zwischen der Aufklärungsquote in Bezug auf eine Straftat und der registrierten Anzahl ihrer Begehung nicht festzustellen, dann kann erst recht nicht davon ausgegangen werden, dass weiter gehende Ermittlungsbefugnisse das tatsächliche Kriminalitätsniveau senken könnten, obwohl gerade dies von Politikern und Bürgern verbreitet angenommen wird.

Realistischerweise können neue Ermittlungsbefugnisse die Aufklärungsquote bestenfalls um einige Prozentpunkte steigern. Ob eine Steigerung der Aufklärungsquote in dieser Größenordnung einen negativen Einfluss auf das Kriminalitätsniveau haben könnte, ist – auch angesichts des großen Dunkelfeldes von staatlich nicht registrierten Straftaten – äußerst fragwürdig. Gerade bei rational geplanten und auf dauernde Gewinnerzielung gerichteten Straftaten wie der Wirtschaftskriminalität und der organisierten Vermögenskriminalität, bei denen ein Einfluss des Entdeckungsrisikos auf den Tatentschluss noch am ehesten zu erwarten wäre, ist anzunehmen, dass die Inhaftierung einiger der Straftäter lediglich dazu führt, dass andere Bandenmitglieder ihr Werk fortführen, dass nicht inhaftierte Straftä-

328 Albrecht, Die vergessene Freiheit, 74 und 168.
329 Zum Folgenden Hassemer, Strafen im Rechtsstaat, 185 f. und 275 ff.
330 BMI/BMJ, Sicherheitsbericht 2001, 462.
331 Travis Hirschi, zitiert bei Kunz, Kriminologie, § 34, Rn. 3; Feltes, Fehlerquellen im Ermittlungsverfahren (I).
332 Albrecht/Arnold/Demko/Braun, Rechtswirklichkeit und Effizienz der Telekommunikationsüberwachung, 437.
333 Seiten 44-46.

ter infolge der mangelnden Konkurrenz vermehrt Straftaten begehen oder dass Personen die lukrative Begehung der Straftaten neu aufnehmen.

Angesichts dessen spricht viel für die Annahme, dass Befugniserweiterungen – „more of the same" – keinen merklichen Einfluss auf die Kriminalität haben. Soweit die Kriminalität eine Ausprägung struktureller sozialer Probleme wie etwa von Arbeitslosigkeit oder übergreifender Entwicklungen wie der Globalisierung ist, ist anzunehmen, dass sie sich durch politische und erst recht durch lediglich kriminalpolitische Maßnahmen nicht merklich beeinflussen lassen wird[334]. Noch weniger als das Kriminalitätsniveau von Entdeckungsrisiko oder Strafhöhe abhängt, kann es vom Ausmaß abstrakter Eingriffsbefugnisse abhängen. Auf dem Gebiet der Telekommunikationsüberwachung hat eine internationale Untersuchung ergeben, dass ein Einfluss der rechtlichen Ausgestaltung der Eingriffsbefugnisse auf das Kriminalitätsniveau nicht erkennbar sei[335]. Auch Vergleichsuntersuchungen zwischen den einzelnen Bundesstaaten der USA konnten keinen Zusammenhang zwischen den – je nach Staat unterschiedlichen – Ermittlungsbefugnissen und der Kriminalitätsentwicklung feststellen[336]. Im Vergleich zu Deutschland zeigen die Beispiele anderer Staaten, dass das Instrument der Telekommunikationsüberwachung erheblich seltener[337] oder – wie etwa in Japan – überhaupt nicht zum Einsatz kommen kann[338], ohne dass die Sicherheit dieser Staaten unter diesem Umstand erkennbar leiden würde.

Generell weisen Staaten mit erheblich weiter gehenden Eingriffsbefugnissen, Diktaturen aber auch Demokratien wie die USA[339], im Vergleich zu Deutschland keineswegs eine niedrigere Kriminalitätsrate auf. Wenn selbst totalitäre Staaten, in denen der Überwachung keine Grenzen gesetzt sind, die Kriminalität durch Kontrollmaßnahmen nicht spürbar senken können, dann scheint dies in einem Rechtsstaat erst recht nicht möglich zu sein. Aus den genannten Gründen ist anzunehmen, dass erweiterte informationelle Eingriffsbefugnisse keinen nennenswerten Beitrag zum Rechtsgüterschutz erwarten lassen.

(iii) Nutzen einer Vorratsspeicherung im Speziellen

Im vorliegenden Zusammenhang ist von Bedeutung, in welchem Maße gerade eine generelle Vorratsspeicherung von Telekommunikationsdaten zum Rechtsgüterschutz geeignet ist. Zunächst lässt sich daran denken, dass gespeicherte Kommunikationsdaten dazu verwendet werden könnten, noch unbekannte Straftaten oder Gefahren aufzudecken. Insoweit kommt etwa eine automatische Durchsuchung und Analyse der Datenbestände auf bestimmte Merkmale hin in Betracht, die geeignet sind, das Vorliegen einer Straftat oder Gefahr zu indizieren. Allerdings erscheint es aufgrund des Aussagegehalts von Kommunikationsdaten unwahrscheinlich, dass aus deren Analyse gänzlich neue Anhaltspunkte für Gefahren gewonnen werden könnten. Solche Projekte, die manchmal als „fishing expeditions"[340] oder als „Stochern im Nebel"[341] bezeichnet werden, sind ohne vorherige Anhaltspunkte rechtsstaatlich bedenklich, erfordern ein großes Maß an Ressourcen und versprechen kaum Erfolg. Gerade die Bekämpfung organisierter Kriminalität erfordert stattdessen gezielte kriminalistische Arbeit[342].

Dies bestätigt die mit großem Aufwand im Jahre 2002 durchgeführte Rasterfahndung, deren Ziel einer Identifizierung potenzieller Terroristen verfehlt wurde. Die Rasterfahndung hat im Wesentlichen lediglich zur Aufdeckung einiger Fälle von Sozialhilfebetrug geführt[343]. Auch die Initiatoren der Rasterfahndung mussten schließlich eingestehen, dass sich „Schläfer" gerade dadurch auszeichnen, dass sie ein äußerlich vollkommen normales Leben führen[344]. Viele Terroristen leben über Jahre hinweg in westlichen Ländern und sind dort vollständig integriert. Eine der zentralen Figuren der al-Quaida war beispielsweise Sergeant bei der US-Armee und hatte in dieser Funktion sogar Zugang zu Geheimdokumenten[345]. Führen Terroristen aber ein äußerlich normales Leben, dann ist es aussichtslos, sie anhand äußerlicher Merkmale identifizieren zu wollen – so das Ergebnis einer wissenschaftlichen Ver-

334 Hassemer, Strafen im Rechtsstaat, 261.
335 Albrecht/Arnold/Demko/Braun, Rechtswirklichkeit und Effizienz der Telekommunikationsüberwachung, 437.
336 Rohe, Verdeckte Informationsgewinnung mit technischen Hilfsmitteln zur Bekämpfung der Organisierten Kriminalität, 47.
337 Breyer, Vorratsspeicherung, 23 ff.
338 Für Japan wik-Consult, Studie (I), 103 f. und 110.
339 Vgl. Bottger/Pfeiffer, ZRP 1994, 7 (14): Die Kriminalität in den USA sei laut Statistik erheblich höher als in Deutschland.
340 GILC, Global Internet Liberty Coalition u.a.: Open letter to the European Parliament, gilc.org/cox_en.html.
341 Weichert, Terror und Informationsgesellschaft (I); ähnlich L/D3-Lisken, C 83: „Suchen im Nebel"; Schütte, ZRP 2002, 393 (397) zur Schleierfahndung spricht von einem Stochern „mit der Nadel im Heuhaufen".
342 Weichert, Terror und Informationsgesellschaft (I).
343 Weichert, Thilo: Beängstigende Bilanz der Terrorismusbekämpfung, 10.09.2002, www.datenschutzverein.de/-Pressemitteilungen/2002_07.html.
344 Krischer, Markus: In den Köpfen der Krieger Allahs, FOCUS 37/2002, S. 52-58, 52 (54).
345 Krischer, Markus: In den Köpfen der Krieger Allahs, FOCUS 37/2002, S. 52-58, 52 (61).

gleichsstudie zu Soziologie und Psychologie des Terrorismus[346]. Dies aber entzieht Verfahren, die – wie die Rasterfahndung – erst der Verdachtsgewinnung dienen sollen, den Boden. Gründe für die Annahme, dass dies bei anderen Kriminalitätszweigen oder speziell im Bereich von Telekommunikationsdaten substanziell anders sein könnte, sind nicht ersichtlich. Eine hinreichende Eignung solcher Filterverfahren zur Verdachtsgewinnung kann somit nicht angenommen werden.

Von Bedeutung können angesichts dessen vor allem Fälle sein, in denen ein Verdacht bezüglich des Vorliegens einer bestimmten Straftat oder Gefahr bereits besteht oder das Vorliegen einer Straftat oder Gefahr bereits gewiss ist. Hier könnten Strafverfolgungsbehörden beispielsweise versuchen, anhand von Telekommunikationsdaten zu klären, ob eine vermutete Straftat begangen wurde und wenn ja, an welchem Ort und durch wen sie begangen wurde. Gefahrenabwehrbehörden könnten versuchen, mit Hilfe von Telekommunikationsdaten zu klären, ob eine vermutete Gefahr besteht und welche Rechtsgüter an welchem Ort durch wen gefährdet sind.

Die Einführung einer obligatorischen Vorratsspeicherung von Telekommunikationsdaten ist grundsätzlich geeignet, die Verdachtssteuerung und Verdachtsverdichtung zu erleichtern. Durch eine Vorratsspeicherung wird vermieden, dass sich Kommunikationsvorgänge nicht nachvollziehen lassen, weil ihre Umstände nicht aufgezeichnet wurden oder die Aufzeichnungen gelöscht wurden. Allerdings ist nicht bekannt, in wie vielen und in welchen Fällen tatsächlich ein Bedarf nach Kommunikationsdaten besteht, die gegenwärtig nicht gespeichert oder gelöscht werden und die im Fall einer Vorratsspeicherung verfügbar wären. Zu beachten ist nämlich, dass eine Vorratsspeicherung die Quantität der zu staatlichen Zwecken verfügbaren Kommunikationsdaten nur in begrenztem Maße steigern würde: Schon bisher kann die Aufzeichnung von Telekommunikationsdaten in Einzelfällen angeordnet werden (§ 100g Abs. 1 S. 3 StPO bzw. §§ 100a, 100b StPO). Was Kommunikationsdaten aus der Vergangenheit angeht, so wird schon bisher eine Vielzahl von Kommunikationsdaten zu Abrechnungs- und Beweiszwecken bis zu sechs Monate lang gespeichert.

Angesichts dessen wird teilweise bezweifelt, ob eine generelle Vorratsspeicherung von Telekommunikationsdaten nennenswerten Nutzen für die staatliche Aufgabenerfüllung entfalten kann, und es werden nähere Untersuchungen über den Bedarf danach gefordert[347]. In der Praxis gebe es nur sehr wenige Fälle, in denen ein Auskunftverlangen daran scheitere, dass die Daten bereits gelöscht wurden[348]. Auf die meisten dieser Fälle wiederum seien die Sicherheitsbehörden erst nach so langer Zeit aufmerksam geworden, dass selbst nach den aktuellen Plänen für eine Vorratsspeicherung, die eine Speicherungsdauer von ein bis zwei Jahren vorsehen, die Daten bereits gelöscht worden wären[349].

Vertreter italienischer Sicherheitsbehörden sind der Ansicht, Untersuchungen im Bereich der Netzkriminalität begönnen nur selten vor Ablauf eines Jahres nach Begehung der Straftat[350]. Ihnen sind keine oder nur wenige Fälle bekannt, in denen eine Ermittlung an der fehlenden Vorratsspeicherung von Telekommunikationsdaten scheiterte[351]. Auch die schwedischen Strafverfolger sehen insoweit keinen Handlungsbedarf[352], wohingegen die britischen Behörden eine „zunehmende Anzahl" von Fällen vermelden, in denen es an Kommunikationsdaten mangele[353]. Deutsche Stimmen behaupten, dass die Zuordnung von IP-Adressen zu einer Person im Internet „oftmals" scheitere, wenn nicht zeitnah ermittelt werde[354]. Die Bundesregierung sah im Jahr 2002 dagegen noch keine Notwendigkeit einer generellen Vorratsspeicherung von Telekommunikationsdaten[355].

346 Krischer, Markus: In den Köpfen der Krieger Allahs, FOCUS 37/2002, S. 52-58, 52 (54); vgl. auch AG Wiesbaden, DuD 2003, 375 (375 ff.).

347 ISPA, Internet Service Providers' Association (UK): Memorandum by the Internet Services Providers' Association (ISPA), 19 November 2001, www.parliament.the-stationery-office.co.uk/pa/cm200102/cmselect/cmhaff/351/-351ap10.htm; eco, Electronic Commerce Forum e.V., Verband der deutschen Internetwirtschaft: Vorratsdatenspeicherung ist verfassungswidrig! Pressemitteilung vom 17.12.2003, www.eco.de/servlet/PB/menu/1236462_pcontent_l1/-content.html.

348 ECTA, European Competitive Telecommunications Association: ECTA position on data retention in the EU, August 2002, https://www.ectaportal.com/uploads/1412ECTAdataretentionstatement.DOC.

349 APIG, Communications Data, 25; vgl. auch Uhe/Herrmann, Überwachung im Internet (I), 111, wonach die vollständige Auswertung einer Computerausrüstung in einem deutschen Bundesland im Schnitt ein bis zwei Jahre dauere; a.A. Finnland in MDG, EU-Questionnaire (I), 24: In den meisten Fällen sei eine zweijährige Speicherung ausreichend.

350 Italien in MDG, EU-Questionnaire (I), 8.

351 Italien in MDG, EU-Questionnaire (I), 19.

352 Schweden in MDG, EU-Questionnaire (I), 19.

353 Großbritannien in MDG, EU-Questionnaire (I), 19.

354 BMI/BMJ, Sicherheitsbericht 2001, 203 f.

355 Deutschland in MDG, EU-Questionnaire (I), 24. Schon in BT-Drs. 13/4438, 39 sah die Bundesregierung keinen „aktuellen Bedarf" für eine Vorratsspeicherung.

Der Internet-Access-Provider AOL Großbritannien gibt an, 99,9% der an Sicherheitsbehörden erteilten Auskünfte hätten ausschließlich Bestandsdaten zum Gegenstand[356]. Verkehrsdaten sind also in weniger als 0,1% der Fälle erfragt worden, was gegen die Bedeutung speziell von Internet-Verkehrsdaten für die Sicherheitsbehörden spricht. Es ist bekannt, dass die meisten Auskunftsersuchen Telefon-Verbindungsdaten zum Gegenstand haben und dass Internet-Kommunikationsdaten eher selten angefordert werden[357]. In Deutschland sollen Internet-Daten nur in etwa 0,5-1% der Fälle von Telekommunikationsüberwachung betroffen sein[358]. Ähnliche Zahlen sind aus den Niederlanden bekannt, wo Internet-Provider zu Investitionen in dreistelliger Millionenhöhe verpflichtet wurden, um die Telekommunikationsüberwachung im Internet sicher zu stellen, wo aber seit 1998 nicht mehr als fünf Internet-Überwachungsmaßnahmen angeordnet wurden[359].

Der mögliche Zusatznutzen einer generellen Vorratsspeicherung von Telekommunikationsdaten reduziert sich weiter dadurch, dass eine Vorratsspeicherung nur die Quantität, nicht aber die Qualität von Kommunikationsdaten verbessern würde. Telekommunikationsdaten sind bedeutungslos, sobald die Kommunikationsnetze anonym genutzt werden[360]. Verhalten in den Kommunikationsnetzen nachvollziehen zu können, ist weitgehend sinnlos, wenn es sich nicht auch den jeweiligen Personen zuordnen lässt. Gerade dies ist heutzutage aber nicht gewährleistet; es gibt kostengünstige, leicht erreichbare und effektive Mittel zur anonymen Nutzung der Kommunikationsnetze[361]. Dies führt dazu, dass aus technischer Sicht nahezu jede behördliche Maßnahme unter dem Vorbehalt steht, dass der jeweilige Täter nicht das gewisse Maß an krimineller Energie und technischem Geschick aufwendet, das erforderlich ist, um sich einer Identifizierung zu entziehen[362].

Für die Zukunft ist mit der Neu- und Fortentwicklung von Möglichkeiten zur anonymen Telekommunikation zu rechnen[363], was deren Verbreitung weiter fördern wird. Es ist anzunehmen, dass zunehmend komfortable und preisgünstige Lösungen auf den Markt kommen werden oder dass Anonymisierungstechniken sogar standardmäßig angeboten werden, besonders im Internet. Es dauert erfahrungsgemäß nur drei bis vier Jahre, bis sich neue Technik im Bereich von Endgeräten durchsetzt[364]. Vertreter von Sicherheitsbehörden erkennen an, dass sich die Verbreitung von Datenverschlüsselung im Zusammenhang mit Internetanwendungen weder aufhalten noch nationalstaatlich begrenzen lässt[365]. Nicht anders verhält es sich auf dem Gebiet von Anonymisierungstechniken.

Die anonyme Nutzung von Kommunikationsnetzen lässt sich in weiten Bereichen nicht verhindern. Zwar muss nach § 111 TKG seine Identität angeben, wer einen Telefon- oder Mobiltelefonanschluss anmeldet. Dies gewährleistet jedoch keine effektive Zuordnung, weil die Anbieter zur Überprüfung der Angaben nicht verpflichtet sind. Denkbar wäre es zwar, in Deutschland oder vielleicht sogar Europa noch weiter gehend vorzusehen, dass sich jeder Käufer einer Telefonkarte, jeder Benutzer eines Hoteltelefons oder Internet-Cafés mit einem Ausweis identifizieren muss. Abgesehen von den damit verbundenen Freiheitseinbußen, die bisher nur totalitäre Staaten wie China und Pakistan[366] in Kauf nehmen, würde der Versuch der Abschaffung anonymer Telekommunikation spätestens an den Grenzen Europas scheitern. Der Umweg über Drittstaaten würde es weiterhin ohne größere Schwierigkeiten ermöglichen, sich anonym ein Mobiltelefon zu kaufen, Callback-Dienste zu nutzen, E-Mail-Konten einzurichten und Proxies zu verwenden, auch von Ländern aus, in denen eine Identifizierungspflicht existiert. Gerade die Divergenzen der nationalen Rechtsordnungen werden von Straftätern häufig ausgenutzt, um einer Strafverfolgung zu entgehen[367]. So haben Terroristen aus dem Umfeld der Anschläge auf das World Trade Center am 11. September 2001 unter anderem mit Schweizer SIM-Karten in

356 De Stempel, Camille in APIG, All Party Parliamentary Internet Group (UK): Internet Service Providers Association (UK), APIG Communications Data Inquiry Oral Evidence, 11.12.2002, www.apig.org.uk/ispa_oral_evidence.htm.

357 NCIS Submission (I), Punkt 6.1.1.

358 Schulzki-Haddouti, Lauscher unter Beschuss, c't 09/2001, 24 ff.; Welp, TKÜV, 3 (4).

359 Ermert, Monika: Jedem Bundesland sein Lauschgesetz, 23.11.2002, Heise Newsticker, www.heise.de/newsticker/data/-gr-23.11.02-001/.

360 Lenz, Karl-Friedrich: Stellungnahme zur Anhörung der Kommission über die Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität, europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/Comments/kf_lenz.html.

361 Breyer, Vorratsspeicherung, 12 ff.

362 Germann, 325 für das Internet.

363 Hamm, NJW 2001, 3100 (3101).

364 Pfitzmann, Andreas in Bundestag, Öffentliche Anhörung zum Thema Cyber-Crime/TKÜV (I), 40.

365 Zwingel (Leiter des BKA-Referates IT-Nutzung und Telekommunikationsüberwachung), Technische Überwachungsmaßnahmen aus Sicht der Polizei, 37 (42).

366 Dazu Rötzer, Florian: Pakistan: Ausweis für Benutzung von Internetcafés, Telepolis, Heise-Verlag, 05.08.2002, www.heise.de/tp/deutsch/inhalt/te/13040/1.html.

367 BMI/BMJ, Sicherheitsbericht 2001, 204.

ihren Handys telefoniert[368], weil bei dem Kauf von Schweizer SIM-Karten keine Personalien angegeben werden mussten. In vielen Staaten werden international einsetzbare SIM-Karten anonym verkauft[369].

Die vorliegenden Vorschläge zur Einführung einer Vorratsspeicherung sehen keine wirksamen Einschränkungen der anonymen Nutzung der Netze vor. Sich der verfügbaren Möglichkeiten zur anonymen Nutzung der Netze nicht zu bedienen, wäre für einen Kriminellen aber so leichtsinnig wie eine Erpressung unter Benutzung des eigenen Telefonanschlusses oder wie ein Bankraub mit dem eigenen Nummernschild am Fluchtwagen[370]. Bekannt ist, dass sich die Nutzung von Möglichkeiten anonymer Telekommunikation in kriminellen Kreisen immer weiter durchsetzt[371]. Die Verwendung einer Vielzahl von anonym oder unter falschem Namen angemeldeten Mobiltelefonkarten sowie mehrerer Mobiltelefone abwechselnd ist heute bereits unter Kleinkriminellen verbreitet[372]. Die sicherheitsbewusstesten Großkriminellen sollen jedes Mobiltelefon und jede Mobiltelefonkarte gar nur einmal benutzen[373]. Selbst im Bereich redlicher Kunden werden etwa 50% der Mobiltelefonkarten innerhalb eines Jahres verschenkt[374], was eine Identifizierung des jeweiligen Nutzers vereiteln kann. Im Bereich der Internetkriminalität ist bekannt, dass in vielen Fällen gestohlene Internet-Zugangsdaten eines Dritten genutzt werden[375]. Auch die übrigen Möglichkeiten des Internet zur Wahrung der Anonymität und zur Erschwerung der Nachvollziehbarkeit von Absenderadressen werden nach Einschätzung des Ersten Sicherheitsberichts der Bundesregierung ausgenutzt[376]. Nach Angaben des Bayerischen Landeskriminalamts wurden bei 7-8% der dort durchgeführten Untersuchungen mit Internetrelevanz Anonymisierungsdienste eingesetzt[377].

Darüber hinaus ist anzunehmen, dass eine Vorratsspeicherung zu einer erheblich höheren Verbreitung anonymer Telekommunikation als bisher führen würde, weil dadurch ein konkreter Bedarf nach diesen Techniken entstünde[378]. Dieser kontraproduktive Effekt schlägt im Rahmen der Verhältnismäßigkeitsprüfung negativ zu Buche.

Angesichts der vielfältigen Möglichkeiten anonymer Telekommunikation ist fraglich, ob gerade gegen besonders gefährliche Personen wie Hintermänner organisierter Kriminalität effektiv im Wege des Zugriffs auf Telekommunikationsdaten vorgegangen werden kann. Teilweise wird vorgetragen, dass selbst professionelle Zielpersonen immer einmal wieder auch identifizierbare Anschlüsse benutzten[379]. Viele Straftäter seien zu bequem, um verfügbare Möglichkeiten anonymer Telekommunikation zu nutzen. Dies gelte jedenfalls außerhalb des Internetbereichs, in dem die Sicherheitsbehörden – wohl wegen der zahlenmäßig seltenen Überwachung in diesem Feld – noch keine Erfahrungen sammeln konnten[380].

Inwieweit die Hoffnung der Strafverfolgungsbehörden, auch Großkriminelle gelegentlich identifizieren zu können, berechtigt ist, lässt sich nicht sicher sagen. Immerhin steht fest, dass sich die Erfahrungswerte der Strafverfolgungsbehörden[381] nur auf die von ihnen tatsächlich erfassten Kommunikationsdaten und nur auf ihnen bekannte Täter beziehen können. Wie viel Telekommunikation und wie viele Personen ihnen dagegen entgehen, können sie kaum beurteilen. Es ist eine allgemeine Erkenntnis

368 taz, Die Tageszeitung: Terroristen nutzten SIM-cards, 09.08.2002, www.taz.de/pt/2002/08/09/a0131.nf/-text.name,askeVQpje.n,66.

369 taz, Die Tageszeitung: Terroristen nutzten SIM-cards, 09.08.2002, www.taz.de/pt/2002/08/09/a0131.nf/-text.name,askeVQpje.n,66; Spanische Delegation in der Gruppe „Drogenhandel“ des Rates der Europäischen Union: Entwurf von Schlussfolgerungen des Rates zur Notwendigkeit der Einführung einer gemeinsamen Regelung auf EU-Ebene für die Identifizierung von Guthabenkartenbenutzern zur Erleichterung der Ermittlungen im Bereich der organisierten Kriminalität insbesondere mit Blick auf den illegalen Drogenhandel, 05.06.2002, register.consilium.eu.int/pdf/-de/02/st05/05157-r2d2.pdf.

370 Lenz, Karl-Friedrich: Stellungnahme zur Anhörung der Kommission über die Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität, europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/Comments/kf_lenz.html.

371 Jeserich (Leitender Oberstaatsanwalt bei der Generalstaatsanwaltschaft in Celle), TK-Überwachung, 63 (69).

372 Heise Verlag: IMSI-Catcher zur Mobilfunküberwachung bald legal, Meldung vom 30.11.2001, www.heise.de/-newsticker/data/hod-30.11.01-000/.

373 Fairbrother, Peter: Defeating traffic analysis, www.apig.org.uk/fairbrother.pdf.

374 BMWi-Ressortarbeitsgruppe, Eckpunkte zur Anpassung der Regelungen des § 90 TKG (I), 7.

375 Hong Kong Inter-departmental Working Group on Computer Related Crime, Report (I), 61.

376 BMI/BMJ, Sicherheitsbericht 2001, 205.

377 Gerling/Tinnefeld, DuD 2003, 305 (305).

378 Fairbrother, Peter: Defeating traffic analysis, www.apig.org.uk/fairbrother.pdf.

379 Jeserich (Leitender Oberstaatsanwalt bei der Generalstaatsanwaltschaft in Celle), TK-Überwachung, 63 (68); so zu den Möglichkeiten der Verschlüsselung auch Graf, Jürgen (Generalbundesanwalt) in Bundestag, Öffentliche Anhörung zum Thema Cyber-Crime/TKÜV (I), 12 f.; Lorenz, GA 97, 51 (69).

380 Graf, Jürgen (Generalbundesanwalt) in Bundestag, Öffentliche Anhörung zum Thema Cyber-Crime/TKÜV (I), 14.

381 Zu deren Maßgeblichkeit BVerfGE 100, 313 (374 f.).

moderner Kriminologie, dass das Dunkelfeld unerkannter Straftaten allgemein sehr groß ist und dass, wenn eine Straftat einmal entdeckt und aufgeklärt wird, meistens nur „kleine Fische“ überführt werden können[382].

Auch auf dem Gebiet der Telekommunikationsüberwachung konzedieren Vertreter der Sicherheitsbehörden, dass in den Kreisen wirklich gefährlicher Personen „gewichtige Überwachungsdefizite“ bestehen und dass sich gerade besonders gefährliche Personen die Möglichkeiten der anonymen Telekommunikationsnutzung in hohem Maße zunutze machen[383]. Wirklich gefährliche Kriminelle suchten immer nach Wegen, um einer Überwachung vorzubeugen, beispielsweise durch die Benutzung vorausbezahlter Handys, von Internet-Cafés oder von pauschalen Abrechnungsmodellen[384]. Wenn einige Telekommunikationsunternehmen Kommunikationsdaten freiwillig speichern, dann würden organisierte Kriminelle andere Unternehmen nutzen[385]. Im Falle einer generellen Vorratsspeicherung von Telekommunikationsdaten würde diese Gruppe von Kriminellen sofort Gegenmaßnahmen ergreifen, um einer Überwachung zu entgehen[386].

Da es für professionelle Kriminelle, die viel zu verlieren haben, geradezu leichtsinnig wäre, sich vorhandener Möglichkeiten anonymer Kommunikation nicht zu bedienen, spricht viel dafür, dass sich der unsichere Gebrauch von Mobiltelefonen im Wesentlichen auf Kleinkriminalität beschränkt[387]. Organisierte Täterkreise sind demgegenüber bekannt dafür, mit äußerster Professionalität vorzugehen. Sie werden daher selbst hohe Kosten und Unbequemlichkeiten in Kauf nehmen, um ihre lukrativen und oft langfristig aufgebauten Geschäfte nicht zu gefährden. Aus diesen Gründen ist anzunehmen, dass sich ernsthafte Kriminelle regelmäßig einer Identifizierung entziehen werden[388] und dass der Zugriff auf Telekommunikationsdaten daher kein geeignetes Mittel ist, gegen diese Täterkreise effektiv vorzugehen[389].

Angesichts dieser Situation ist zwar ein kurzfristiger Handlungsvorteil der Behörden nach Einführung einer Vorratsspeicherung denkbar[390]. Dieser kann aber durch Probleme in der Einführungsphase der Technik gemindert werden[391]. Nach einigen Monaten wird sich überdies jedenfalls ein großer Teil der gefährlichen Kriminellen auf die neue Situation eingestellt haben und von den Möglichkeiten anonymer Telekommunikation Gebrauch machen[392]. Es liegt daher nahe, dass eine Vorratsspeicherung zur Überführung einiger Unachtsamer führen könnte und Kleinkriminelle wie schon bisher überführt werden könnten, dass sie gegen umsichtige und ernsthafte Kriminelle aber nahezu gänzlich wirkungslos wäre[393] und dass insoweit nach wie vor nur in Einzelfällen Erfolge erzielt werden könnten.

Angesichts der Möglichkeiten zur anonymen Nutzung der Telekommunikationsnetze muss man daher davon ausgehen, dass eine Vorratsspeicherung von Kommunikationsdaten regelmäßig allenfalls

---

382 Hassemer, Strafen im Rechtsstaat, 278.

383 Jeserich (Leitender Oberstaatsanwalt bei der Generalstaatsanwaltschaft in Celle), TK-Überwachung, 63 (71); für den Internetbereich auch Gehde (LKA Berlin), c’t 19/2002, 127.

384 Gamble, Jim (Assistant Chief Constable in the UK National Crime Squad) in APIG, All Party Parliamentary Internet Group (UK): UK Law Enforcement, APIG Communications Data Inquiry Oral Evidence, 18.12.2002, www.apig.org.uk/law_enforcement_oral_evidence.htm.

385 Gamble, Jim (Assistant Chief Constable in the UK National Crime Squad) in APIG, All Party Parliamentary Internet Group (UK): UK Law Enforcement, APIG Communications Data Inquiry Oral Evidence, 18.12.2002, www.apig.org.uk/law_enforcement_oral_evidence.htm.

386 Gamble, Jim (Assistant Chief Constable in the UK National Crime Squad) in APIG, All Party Parliamentary Internet Group (UK): UK Law Enforcement, APIG Communications Data Inquiry Oral Evidence, 18.12.2002, www.apig.org.uk/law_enforcement_ oral_evidence.htm.

387 Fairbrother, Peter: Defeating traffic analysis, www.apig.org.uk/fairbrother.pdf.

388 Snape, Tim (Managing Director des britischen ISP West Dorset Internet), zitiert bei McCue, Andy: Government rethinks data policy, 10.10.2001, www.vnunet.com/News/1126012: „Any competent technician can bypass logging procedures“; Robinson, James K.: Vortrag auf der International Computer Crime Conference „Internet as the Scene of Crime“ in Oslo, Norwegen, 29.-31.05.2000, www.usdoj.gov/criminal/cybercrime/roboslo.htm: „While less sophisticated cybercriminals may leave electronic ‚fingerprints,‘ more experienced criminals know how to conceal their tracks in cyberspace.“

389 So Pfitzmann, Andreas in Bundestag, Öffentliche Anhörung zum Thema Cyber-Crime/TKÜV (I), 10 angesichts von Verschlüsselungsmöglichkeiten: eher zweifelhaft; a.A. Graf, Jürgen (Generalbundesanwalt) in Bundestag, Öffentliche Anhörung zum Thema Cyber-Crime/TKÜV (I), 12 f. und 44.

390 Fairbrother, Peter: Defeating traffic analysis, www.apig.org.uk/fairbrother.pdf.

391 Fairbrother, Peter: Defeating traffic analysis, www.apig.org.uk/fairbrother.pdf.

392 Fairbrother, Peter: Defeating traffic analysis, www.apig.org.uk/fairbrother.pdf.

393 Fairbrother, Peter: Defeating traffic analysis, www.apig.org.uk/fairbrother.pdf; BITKOM: Stellungnahme zur Gesetzesinitiative des Bundesrates vom 31.05.2002 (BR-Drs. 275/02), 12.08.2002, www.bitkom.org/files/documents/-Position_BITKOM_Vorratsdatenspeicherung_u.a._12.08.2002.pdf, 9; o2 (Germany): Schriftliche Stellungnahme zur öffentlichen Anhörung am 09.02.2004 in Berlin zum Entwurf eines Telekommunikationsgesetzes (TKG), in Ausschussdrucksache 15(9)961, www.bitkom.org/files/documents/StN_BITKOM_TKG_Wirtschaftsausschuss_03.02.04.pdf, 140 (146).

bei geringen Gefahren Abhilfe schaffen kann[394]. Die Eignung zur Bekämpfung organisierter Kriminalität oder zur Verhütung terroristischer Anschläge ist demgegenüber als gering einzuschätzen. Die Schaffung besonders eingriffsintensiver Befugnisse, die regelmäßig nur im Bereich der kleinen und mittleren Kriminalität Nutzen entfalten können, steht im Widerspruch zu dem Grundsatz der gleichmäßigen Strafverfolgung und führt zu einer weiteren Konzentration der Strafverfolgung auf die Bekämpfung der „kleinen Fische".

Die Bedeutung des Zugriffs auf Kommunikationsdaten im Rahmen von Ermittlungsverfahren darf auch nicht überschätzt werden: Zu Recht warnen Behördenvertreter, dass es eine Überschätzung der Möglichkeiten der Telekommunikationsüberwachung wäre, diese allein als „Schlüssel zur inneren Sicherheit" anzusehen[395]. Während plausibel ist, dass der Zugriff auf Kommunikationsdaten im Rahmen von Ermittlungsverfahren nützlich sein kann, bedeutet das noch nicht, dass Kommunikationsdaten das entscheidende, zur Aufklärung der Straftat führende Element darstellen[396]. Außerhalb des Gebiets der Netzkriminalität stellen Kommunikationsdaten nur einen kleinen Teil des Puzzles dar, welches die Ermittler zusammen setzen müssen[397]. Ein Fehlen von Kommunikationsdaten kann oft durch andere Informationsquellen ausgeglichen werden[398], deren Erschließung zwar aufwändiger sein kann, dafür aber zielgerichteter erfolgen und infolgedessen effektiver sein kann[399]. Selbst wenn die erforderlichen Kommunikationsdaten zur Verfügung stehen, kann die Aufklärung einer Straftat immer noch aus einer Vielzahl von anderen Gründen scheitern.

Es ist daher nicht klar, ob eine generelle Vorratsspeicherung von Telekommunikationsdaten einen merklichen Einfluss auf die Aufklärungsrate oder gar das Kriminalitätsniveau haben könnte. Angesichts der beschriebenen Bedenken gegen die präventive Wirksamkeit der Strafverfolgung allgemein, besonders gegen den Nutzen der Erweiterung ihrer Befugnisse, sowie gegen die Wirksamkeit gerade einer Vorratsspeicherung von Kommunikationsdaten ist ein merklicher Einfluss dieser Maßnahme auf die Kriminalitätsrate nicht anzunehmen.

Im Übrigen sollte auch die Bedeutung des Arguments nicht überschätzt werden, dass der verstärkte Zugriff auf Kommunikationsdaten dazu dienen könnte, Unschuldige von falschen Verdachtsmomenten zu entlasten[400]. Nur in Einzelfällen kann davon ausgegangen werden, dass Kommunikationsdaten mit Hilfe von anderen Ermittlungsmethoden gewonnene Verdachtsmomente entkräften können. Ihre Aussagekraft ist wegen der vielen Manipulationsmöglichkeiten zu gering. Demgegenüber ist mit einer Vielzahl von Massenverdächtigungen durch Kommunikationsdaten-Rasterung der oben genannten Art zu rechnen, was den möglichen Entlastungseffekt bei Weitem überwiegt. Als konkretes Beispiel lässt sich der Fall eines Nigerianers in Österreich anführen, der mehrere Monate lang in Untersuchungshaft genommen wurde, weil er wegen seiner zahlreichen Telefonkontakte als Führer einer Rauschgiftbande in Verdacht geraten ist[401]. Später stellte sich der Verdacht als unbegründet und der Nigerianer einfach als gefragter Ratgeber für die schwarze Gemeinschaft in Wien heraus[402]. In den USA sollen 800 Personen nur deshalb in Untersuchungshaft sitzen, weil sie im Vorfeld des 11. September besonders viel kommuniziert haben[403].

(cc) Zusammenfassung: Nutzen einer Vorratsspeicherung von Telekommunikationsdaten

Festzuhalten ist, dass eine vorsorgliche, generelle Speicherung von Telekommunikationsdaten notwendig vergangenheitsbezogen ist und daher im Wesentlichen nur der Aufklärung bereits begangener Straftaten dienen kann. Nach den obigen Ausführungen kann nicht davon ausgegangen werden, dass Strafverfahren den Entschluss von Personen zur Begehung von Straftaten beeinflussen können. Der

394 Fairbrother, Peter: Defeating traffic analysis, www.apig.org.uk/fairbrother.pdf; BITKOM: Stellungnahme zur Gesetzesinitiative des Bundesrates vom 31.05.2002 (BR-Drs. 275/02), 12.08.2002, www.bitkom.org/files/documents/Position_BITKOM_Vorratsdatenspeicherung_u.a._12.08.2002.pdf, 9.

395 Bansberg (Abteilung Grundsatzangelegenheiten des Bundesamtes für Verfassungsschutz), Staatsschutz im Internet, 48 (54).

396 De Stempel, Camille in APIG, All Party Parliamentary Internet Group (UK): Internet Service Providers Association (UK), APIG Communications Data Inquiry Oral Evidence, 11.12.2002, www.apig.org.uk/ispa_oral_evidence.htm.

397 De Stempel, Camille in APIG, All Party Parliamentary Internet Group (UK): Internet Service Providers Association (UK), APIG Communications Data Inquiry Oral Evidence, 11.12.2002, www.apig.org.uk/ispa_oral_evidence.htm.

398 Bansberg (Abteilung Grundsatzangelegenheiten des Bundesamtes für Verfassungsschutz), Staatsschutz im Internet, 48 (54).

399 Weichert, DuD 2001, 694 (694).

400 So NCIS, APIG-Submission (I), Punkt 3.0; zu diesem Argument ausführlich Seiten 35-36.

401 Krempl, Stefan: Die totale Informationsüberwachung, die Demokratie und die Hacker, Telepolis, Heise-Verlag, 28.12.2002, www.heise.de/tp/deutsch/inhalt/te/13870/1.html.

402 Krempl, Stefan: Die totale Informationsüberwachung, die Demokratie und die Hacker, Telepolis, Heise-Verlag, 28.12.2002, www.heise.de/tp/deutsch/inhalt/te/13870/1.html.

403 Krempl, Stefan: Die totale Informationsüberwachung, die Demokratie und die Hacker, Telepolis, Heise-Verlag, 28.12.2002, www.heise.de/tp/deutsch/inhalt/te/13870/1.html.

Verfolgung bereits begangener Straftaten können präventive Effekte nur insoweit zugeschrieben werden, als Straftäter im Wege des Freiheitsentzugs von der Gefährdung von Rechtsgütern abgehalten werden oder als infolge eines Strafverfahrens eine Restitution oder Entschädigung der Opfer einer Straftat erfolgen kann. In wie vielen Fällen gerade eine generelle Vorratsspeicherung von Telekommunikationsdaten dabei von Nutzen wäre, ist nicht bekannt. Die vielfältigen Möglichkeiten zur anonymen Telekommunikation, von denen bei Einführung einer generellen Vorratsspeicherung von Telekommunikationsdaten vermutlich verstärkt Gebrauch gemacht würde, stellen den möglichen Nutzen der Maßnahme allerdings grundlegend in Frage.

Insgesamt ist anzunehmen, dass eine generelle Vorratsspeicherung von Telekommunikationsdaten nur in wenigen und regelmäßig wenig bedeutenden Einzelfällen den Schutz von Rechtsgütern fördern könnte[404]. Ein dauerhafter, negativer Effekt auf das Kriminalitätsniveau ist selbst im Bereich der Netzkriminalität nicht zu erwarten. Die Eignung einer Vorratsspeicherung zur Bekämpfung organisierter Kriminalität oder zur Verhütung terroristischer Anschläge ist als äußerst gering bis nicht gegeben einzuschätzen.

(dd) Betroffene Grundrechtsträger nach Art und Zahl, Identifizierbarkeit der Betroffenen, Eingriffsvoraussetzungen

Für die Bemessung des Verlusts an grundrechtlich geschützter Freiheit infolge einer generellen Speicherung von Kommunikationsdaten ist zunächst maßgeblich, welche und wie viele Grundrechtsträger von einer solchen Maßnahme negativ betroffen wären. Während konkrete Nachteile von staatlicher Seite regelmäßig erst durch den staatlichen Zugriff auf die gespeicherten Daten drohen, ist bereits die vorbereitende Erfassung der Kommunikationsdaten durch die Telekommunikationsunternehmen als Eingriff in Art. 10 Abs. 1 Var. 3 GG zu qualifizieren[405], von dem, wie auszuführen sein wird, auch ohne späteren staatlichen Zugriff auf die Daten erhebliche Gefahren ausgehen können.

Von einer Vorratsspeicherung betroffen wären daher alle Personen, die sich der Fernmeldetechnik bedienen. Eine größere Zahl betroffener Grundrechtsträger infolge einer Grundrechtsbeschränkung ist kaum denkbar. Es gäbe praktisch keine unbeeinträchtigte Telekommunikation mehr[406]. § 110a TKG ist zwar insoweit eingeschränkt, wie er nur auf Telekommunikationsdienste für die Öffentlichkeit Anwendung findet, während Kommunikationsvorgänge, die beispielsweise über Firmennetzwerke oder Nebenstellenanlagen abgewickelt werden, nicht erfasst sein sollen. Diese Einschränkung kann im Rahmen des Art. 10 Abs. 1 Var. 3 GG aber nicht von großem Gewicht sein, weil die Betroffenen regelmäßig keine Wahl zwischen dem Einsatz öffentlicher und privater Kommunikationsnetze haben.

Als weiteres Kriterium für die Verhältnismäßigkeitsprüfung fragt das Bundesverfassungsgericht nach der Identifizierbarkeit der Betroffenen. Werden Daten anonym erhoben, so ist der Eingriff nämlich von geringerem Gewicht. Entsprechend dem Zweck einer Vorratsspeicherung müssen die gespeicherten Telekommunikationsdaten jedoch in jedem Fall personenbezogen sein, um der Gefahrenabwehr oder Strafverfolgung förderlich sein zu können. Bei der gewöhnlichen Telekommunikationsnutzung besteht ein Personenbezug regelmäßig insoweit, als sich der Inhaber des genutzten Telekommunikationsanschlusses anhand von Auskünften des jeweiligen Telekommunikationsunternehmens feststellen lässt. Zwar gibt es vielfältige Möglichkeiten der anonymen Telekommunikation, welche die Herstellung eines Personenbezugs verhindern können[407] und deren Einsatz sich für Kriminelle lohnen mag. Dem Normalbürger ist die ausschließliche Nutzung anonymer Formen von Telekommunikation aber wegen des damit verbundenen Aufwands auf Dauer nicht möglich oder jedenfalls unzumutbar. Die Möglichkeiten anonymer Telekommunikation bewirken daher nur eine geringfügige Minderung der Eingriffsintensität einer generellen Vorratsspeicherung von Telekommunikationsdaten.

Für die Verhältnismäßigkeit einer Grundrechtsbeschränkung sind weiterhin die Voraussetzungen, unter denen ein Eingriff zulässig ist, von Bedeutung. Je niedriger die Eingriffsschwelle, desto höher ist die Intensität des Eingriffs. Im vorliegenden Zusammenhang ist bereits die staatlich angeordnete Speicherung oder Aufbewahrung von Kommunikationsdaten durch Telekommunikationsunternehmen als Eingriff in Art. 10 Abs. 1 Var. 3 GG anzusehen, soweit sie nicht für Zwecke der Vertragsabwicklung erforderlich ist[408]. Für diesen Eingriff sind im Rahmen der Pläne zur Einführung einer generellen Vorratsspeicherung von Telekommunikationsdaten keine Voraussetzungen vorgesehen. Vielmehr sollen

404 Earl of Northesk: Debatte im House of Lords, 27.11.2001, www.parliament.the-stationery-office.co.uk/pa/ld199900/-ldhansrd/pdvn/lds01/text/11127-13.htm; vgl. auch BVerfGE 103, 21 (31) zu vorsorglich gespeicherten DNA-Profilen: „Künftige Straftaten können sie im Regelfall auch tatsächlich nicht verhindern".

405 Breyer, Vorratsspeicherung, 90 ff.

406 So auch Bäumler, Helmut, zitiert bei Wagner, Marita: Intimsphäre - lückenlos überwacht? Telepolis, Heise-Verlag, 28.06.2002, www.heise.de/tp/deutsch/inhalt/te/12813/1.html.

407 Breyer, Vorratsspeicherung, 14 ff.

408 Seite 25.

unterschiedslos und unabhängig vom Bestehen eines Verdachts Kommunikationsdaten aller Nutzer von Kommunikationsnetzen gespeichert werden. Fast durchgängig betrifft der Eingriff dabei Personen, die sich nichts zuschulden kommen lassen haben. Der Eingriff könnte daher kaum schwerwiegender sein.

(ee) Gefahrennähe

Maßnahmen wie eine generelle Vorratsspeicherung von Telekommunikationsdaten, die bereits im Vorfeld einer konkreten Gefahr oder eines Verdachts wegen einer Straftat getroffen werden, werden als Vorfeldmaßnahmen bezeichnet. In der Sache handelt es sich um Eingriffe in die Grundrechte von Personen, die nicht aufgrund bestimmter Anhaltspunkte verdächtig sind, Rechtsgüter zu gefährden oder eine Straftat begangen zu haben. Letztlich geht es also um verdachtsunabhängige Eingriffe.

Dass allein der Rechtsgüterschutz Grundrechtseingriffe legitimieren kann, wurde bereits ausgeführt[409]. Dass ein Eingriff potenziell geeignet ist, Rechtsgüter zu schützen, kann ihn aber nicht in jedem Fall legitimieren. Ansonsten wäre zur Aufdeckung von Gefahren und Straftaten eine allgemeine Überwachung und Kontrolle der Bürger zulässig und die Grundrechte obsolet. Das Bundesverwaltungsgericht formuliert diesen Gedanken in einer Entscheidung auf dem Gebiet des Strafprozessrechts wie folgt: „Ausgangspunkt hat die Feststellung zu sein, daß nach dem Menschenbild des Grundgesetzes die Polizeibehörde nicht jedermann als potenziellen Rechtsbrecher betrachten und auch nicht jeden, der sich irgendwie verdächtig gemacht hat (‚aufgefallen ist') oder bei der Polizei angezeigt worden ist, ohne weiteres ‚erkennungsdienstlich behandeln' darf. Eine derart weitgehende Registrierung der Bürger aus dem Bestreben nach möglichst großer Effektivität der Polizeigewalt und Erleichterung der polizeilichen Überwachung der Bevölkerung widerspräche den Prinzipien des freiheitlichen Rechtsstaates."[410]

Gerade Vorfeldmaßnahmen sind daher nicht uneingeschränkt zulässig[411]. Der grundsätzliche Freiheitsanspruch des Einzelnen verlangt, dass der Einzelne von solchen Eingriffen verschont bleibt, die nicht durch eine hinreichende Beziehung oder Nähe zwischen ihm und einer Gefahr legitimiert sind[412]. Ob der insoweit erforderliche „Zurechnungszusammenhang"[413] gegeben ist, ist im Wege einer Abwägung der einschlägigen Interessen zu entscheiden. Letztlich handelt es sich um nichts anderes als die Prüfung der Verhältnismäßigkeit im engeren Sinne. Im Rahmen der Verhältnismäßigkeitsprüfung ist also die Gefahrennähe der betroffenen Grundrechtsträger zu berücksichtigen, so dass im vorliegenden Zusammenhang fraglich ist, welche Nähe zwischen den von einer generellen Vorratsspeicherung von Telekommunikationsdaten betroffenen Personen und den Gefahren, denen mit Hilfe der Vorratsspeicherung begegnet werden soll, besteht.

Wie gezeigt, kann man diese Gefahren in zwei Gruppen einteilen, nämlich in Gefahren, die aus der rechtswidrigen Nutzung von Telekommunikationsnetzen resultieren einerseits und in sonstige Gefahren, denen mit Hilfe einer Überwachung der Telekommunikation begegnet werden kann, andererseits. Fraglich ist zunächst, welche Nähe zwischen den von einer generellen Vorratsspeicherung von Telekommunikationsdaten betroffenen Personen und den Gefahren infolge von Netzkriminalität besteht.

Eine hinreichende Gefahrennähe liegt grundsätzlich dann vor, wenn eine Person aufgrund konkreter Umstände im Einzelfall im Verdacht steht, Rechtsgüter zu verletzen oder eine strafbare Handlung begangen zu haben[414]. Allgemeines Erfahrungswissen und Vermutungen genügen zur Begründung eines Verdachts nicht[415]. Dementsprechend hat das Bundesverwaltungsgericht in der oben zitierten Entscheidung geurteilt, dass angesichts des Menschenbildes des Grundgesetzes erkennungsdienstliche Unterlagen nur von Beschuldigten angefertigt und aufbewahrt werden dürfen und auch nur von sol-

409 Seite 34.

410 BVerwGE 26, 169 (170 f.); vgl. dazu Hohmann-Schwan, Freiheitssicherung durch Datenschutz, 276 (298): „Dies gilt selbstverständlich nicht nur für die Aufbewahrung erkennungsdienstlicher Unterlagen, sondern auch für die Speicherung aller anderen personenbezogenen Daten"; ähnlich wie das BVerwG die abweichende Meinung in BVerfGE 109, 279 (391).

411 SächsVerfGH, DuD 1996, 429 (436): informationelle Vorfeldmaßnahmen seien nur ausnahmsweise zulässig; Hohmann-Schwan, Freiheitssicherung durch Datenschutz, 276 (300): Vorfeldbefugnisse seien nur punktuell und in besonderen Gefährdungslagen zulässig.

412 Für gesetzliche Eingriffe auf dem Gebiet des Polizeirechts MVVerfG, LKV 2000, 149 (153); VG Trier, MMR 2002, 698 (699); vgl. auch Lisken, NVwZ 2002, 513 (515). Für das Gebiet der Straftatenverhütung vgl. BVerfG, NJW 2004, 2213 (2216), wonach das „Risiko einer Fehlprognose" „hinnehmbar" erscheinen müsse. Ähnliche Kriterien leitet Waechter, DÖV 1999, 138 (145) aus dem Gesichtspunkt der Indienstnahme Privater zu öffentlichen Zwecken ab, die nur bei deren besonderer Sachnähe zulässig sei.

413 Für gesetzliche Eingriffe auf dem Gebiet des Polizeirechts MVVerfG, LKV 2000, 149 (153); VG Trier, MMR 2002, 698 (699).

414 Vgl. etwa SächsVerfGH, DuD 1996, 429 (437).

415 SächsVerfGH, DuD 1996, 429 (437).

chen Beschuldigten, bei denen „nach der konkreten Sachlage [...] Anhaltspunkte dafür vor[liegen], daß die erkennungsdienstlich behandelte Person zukünftig strafrechtlich in Erscheinung treten [wird]“[416]. Demnach genügt es beispielsweise nicht, wenn sich die Polizeibehörden auf die generelle Wiedereinlieferungsquote in den Strafvollzug berufen, selbst wenn diese mit 50%[417] außerordentlich hoch liegt.

In die gleiche Richtung geht eine Entscheidung des Bundesverfassungsgerichts über einen Fall, in dem zur Aufklärung einer Straftat angeordnet worden war, dass allen männlichen Porschefahrern mit Münchener Kennzeichen eine Blutprobe zu entnehmen sei, um die Proben mit am Tatort gefundenen Spuren vergleichen zu können. Diese Vorgehensweise sah das Gericht trotz des großen Adressatenkreises als verhältnismäßig an, führte aber aus, die Grenze der Zumutbarkeit sei überschritten, wenn die Ermittlungsmaßnahme gegen so viele Personen angeordnet werde, dass ein konkreter Tatverdacht im Sinne des § 152 Abs. 2 StPO gegen die von der Anordnung Betroffenen nicht mehr bestehe[418]. Sobald jemand also nicht aufgrund besonderer Merkmale verdächtiger ist als sonstige Personen, hat er Eingriffe grundsätzlich nicht hinzunehmen. Die bloße allgemeine Möglichkeit, dass Daten einmal zu Zwecken der Strafverfolgung oder der Gefahrenabwehr benötigt werden könnten, begründet danach grundsätzlich nicht die von Verfassungs wegen zur Rechtfertigung von Eingriffen erforderliche Gefahrennähe.

Auch für den Zugriff auf Kommunikationsdaten zu Strafverfolgungszwecken hat das Bundesverfassungsgericht in einem neueren Urteil einen konkreten Tatverdacht gegen die betroffene Person oder eine hinreichend sichere Tatsachenbasis für die Annahme, dass die Person als Nachrichtenmittler für einen Straftäter tätig wird, gefordert[419]. Das Urteil betraf zwar nicht die generelle Vorratsspeicherung von Kommunikationsdaten, sondern die Übermittlung bestimmter Kommunikationsdaten an Strafverfolgungsbehörden im Einzelfall. Das Gericht spricht in diesem Zusammenhang aber allgemein von der „Erfassung der Verbindungsdaten“[420] und stellt ausdrücklich fest: „Voraussetzung der Erhebung von Verbindungsdaten ist ein konkreter Tatverdacht.“[421] Dies spricht für die Annahme, dass die Verdachtsschwelle für jede dem Staat als Eingriff zuzurechnende Erfassung und Speicherung von Kommunikationsdaten gelten soll.

Eine generelle Vorratsspeicherung von Telekommunikationsdaten würde verdachtsunabhängig erfolgen, so dass sich eine Gefahrennähe der Betroffenen nicht über einen konkreten Verdacht gegen sie herleiten lässt. Allerdings hat der Gesetzgeber in bestimmten Bereichen schon bisher zu Vorfeldeingriffen ermächtigt. Dies gilt etwa für die Einrichtung des Bundeszentralregisters, die Daten über Straftäter speichert. Immerhin setzt eine Eintragung in dieses Register, ebenso wie die meisten anderen strafprozessualen Eingriffe, voraus, dass gegen den Betroffenen zu einem früheren Zeitpunkt einmal ein Tatverdacht vorgelegen hat. Diese Voraussetzung ist bei einer generellen Kommunikationsdatenspeicherung nicht gegeben, so dass sich auch hieraus keine Gefahrennähe herleiten lässt.

Weiterhin können diejenigen Personen, die eine besondere Gefahrenquelle in ihrer Obhut haben, besonderen Kontrollen unterworfen sein, etwa Kraftfahrzeugführer (§ 36 Abs. 5 StVO) oder Betreiber emittierender Anlagen (§ 52 Abs. 2 BImSchG). Noch einen Schritt weiter geht der Gesetzgeber, wenn er Personen allein schon deshalb Kontrollen unterwirft, weil sie sich an Orten aufhalten, an denen typischerweise Gefahren auftauchen sollen, etwa an Grenzen (§ 2 BGSG; vgl. auch die Landespolizeigesetze). Darüber hinaus muss der Bürger an allen öffentlichen Orten mit Identitätskontrollstellen rechnen, wenn dies zur Verfolgung von Mitgliedern einer terroristischen Vereinigung oder in Fällen schweren Raubes erforderlich ist (§ 111 StPO). Auch eine Inanspruchnahme Unbeteiligter zur Gefahrenabwehr ist nach den Landespolizeigesetzen in Ausnahmefällen zulässig („polizeilicher Notstand“).

Unabhängig von der Frage, inwieweit diese Befugnisse jeweils mit der Verfassung vereinbar sind, ist jedenfalls festzustellen, dass eine allgemeine Vorratsspeicherung von Telekommunikationsdaten selbst im Vergleich zu diesen Befugnissen eine gänzlich neue Qualität hätte[422]. Bisher sind Vorfeldeingriffe nur punktuell und in besonderen Gefährdungslagen zulässig[423]. Bei der generellen Speicherung von Kommunikationsdaten aber geht es um eine umfassende und generelle Überwachung bisher ungekannten Ausmaßes. Weder ist der Nutzer von Telekommunikationsdiensten für eine Gefahren-

416 BVerwGE 26, 169 (171); vgl. dazu Hohmann-Schwan, Freiheitssicherung durch Datenschutz, 276 (298): „Dies gilt selbstverständlich nicht nur für die Aufbewahrung erkennungsdienstlicher Unterlagen, sondern auch für die Speicherung aller anderen personenbezogenen Daten.“

417 Kunz, Kriminologie, § 31, Rn. 40.

418 BVerfG JZ 1996, 1175 (1176).

419 BVerfGE 107, 299 (322).

420 BVerfGE 107, 299 (321).

421 BVerfGE 107, 299 (322).

422 Eckhardt, CR 2002, 770 (774).

423 Hohmann-Schwan, Freiheitssicherung durch Datenschutz, 276 (300).

quelle verantwortlich, noch hält er sich an einem besonders gefährlichen Ort auf, noch wird er ausschließlich hinsichtlich konkreter, in der Vergangenheit vermutlich begangener Straftaten kontrolliert, noch besteht im Einzelfall ein polizeilicher Notstand. Der einzige Anknüpfungspunkt besteht in der Benutzung von Telekommunikationsnetzen.

Als Vergleichsfall kommt weiterhin das Waffenrecht in Betracht. Auf diesem Gebiet hat der Gesetzgeber angenommen, dass der Besitz von Waffen eine abstrakte Gefahr von solcher Art und von solchem Ausmaß begründet, dass ein weitgehendes Verbot und im Übrigen eine strenge Überwachung des Waffenbesitzes gerechtfertigt ist. Im Unterschied zu Telekommunikationsnetzen ist allerdings erstens zu beachten, dass Waffen höchstrangige Rechtsgüter, nämlich Leib und Leben von Personen, gefährden. Außerdem werden diese Rechtsgüter durch den Einsatz von Waffen unmittelbar, also nicht erst in Verbindung mit anderen Faktoren, gefährdet. Ein weiterer Unterschied im Rahmen der grundrechtlich gebotenen Abwägung liegt in dem unterschiedlichen gesellschaftlichen Nutzen der Werkzeuge. Während Waffen nur im Einzelfall, etwa zur Selbstverteidigung oder zur Jagd, nützlich sein können, ihr weitgehendes Fehlen aber auch nicht zu untragbaren Nachteilen führt, baut unsere Gesellschaft immer mehr auf Telekommunikationsnetzen auf. Diese entfalten daher einen großen Nutzen, sowohl materiell-wirtschaftlicher Art wie auch ideell-politischer Art, wenn beispielsweise das Internet zur verstärkten Ausübung von Grundrechten genutzt wird. Die Wertungen des Waffenrechts lassen sich auf das Gebiet der Telekommunikation daher nicht übertragen.

Teilweise wird angeführt, eine Pflicht zur Speicherung von Daten zu staatlichen Zwecken sei dem geltenden Recht nicht fremd, wie das Geldwäschegesetz (GwG) zeige[424]. Das Geldwäschegesetz[425] sieht vor, dass Kreditinstitute, Versicherungen und gewisse andere Stellen fremde Vermögensangelegenheiten erst nach Identifizierung des Kunden anhand eines amtlichen Ausweises wahrnehmen dürfen (§§ 2-4 und 6 GwG), selbst wenn eine Identifizierung für die Durchführung der Geschäfte nicht erforderlich ist. Im Unterschied zu einer Vorratsspeicherung von Telekommunikationsdaten betrifft die Aufbewahrungspflicht nach dem Geldwäschegesetz allerdings nur die Personalien der Kunden, nicht die einzelnen von ihnen vorgenommenen Transaktionen. Daten über die einzelnen Transaktionen mögen zwar nach anderen Vorschriften aufzubewahren sein. Anders als Telekommunikationsunternehmen sind die aufbewahrungspflichtigen Personen im Finanzbereich aber nicht verpflichtet, den Strafverfolgungs- und Gefahrenabwehrbehörden einschließlich der Nachrichtendienste Auskünfte über ihre Aufzeichnungen zu erteilen. Hierin liegt der entscheidende Unterschied zu Telekommunikationsdaten. Auch auf die nach dem Geldwäschegesetz aufzuzeichnenden Personalien dürfen nur sehr eingeschränkt weitergegeben und verwendet werden (§ 10 GwG), insbesondere zur Verfolgung von Geldwäschedelikten. Aus den genannten Gründen ist eine Vorratsspeicherung von Telekommunikationsdaten vielfach eingriffsintensiver als das Geldwäschegesetz.

Eine weitgehende Überwachung auf dem Gebiet der Telekommunikation erlaubt das G10[426], das in seinem § 5 zu einer anlassunabhängigen („strategischen“) Überwachung internationaler Telekommunikationsbeziehungen zur Abwehr schwerster Gefahren ermächtigt. Zwar erlaubt das G10 auch die Kenntnisnahme von Kommunikationsinhalten, während eine Kommunikationsdatenspeicherung auf die Kommunikationsumstände beschränkt ist. Jene Beschränkung verhindert aber lediglich, dass eine generelle Aufhebung des Fernmeldegeheimnisses zu besorgen ist. Ansonsten sind Telekommunikationsdaten nicht generell weniger schutzwürdig als Kommunikationsinhalte[427], so dass darin kein maßgeblicher Unterschied zu § 5 G10 zu sehen ist.

Das Bundesverfassungsgericht hat eine globale und pauschale Überwachung selbst zur Abwehr größter Gefahren ausdrücklich als verfassungswidrig bezeichnet[428] und damit eine „flächendeckende Erfassung [...] des [...] Fernmeldeverkehrs“[429] gemeint. Weil eine Vorratsspeicherung grundsätzlich jeglichen Telekommunikationsverkehr einer Überwachung unterwerfen würde, könnte sie als eine solche „globale und pauschale Überwachung“ des Telekommunikationsverkehrs angesehen werden. In der strategischen Überwachung nach dem G10 hat das Bundesverfassungsgericht nur deswegen keine solche Globalüberwachung gesehen, weil nur der internationale Fernmeldeverkehr betroffen sei, es tatsächlich nur selten zu einer Erfassung komme, der Satelliten-Downlink nicht immer erfasst würde, nur die Überwachung bestimmter Fernmeldeverkehrsbeziehungen angeordnet würde und die Überwa-

424 Beschluss des Bundesrates vom 31.05.2002, BR-Drs. 275/02, 25; Beschluss des Bundesrates vom 19.12.2003, BR-Drs. 755/03, 34.

425 Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten vom 25.10.1993 (BGBl. I 1993, 1770), zuletzt geändert durch Art. 1 des Gesetzes vom 08.08.2002 (BGBl I 2002, 3105).

426 Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses vom 26.06.2001 (BGBl I 2001, 1254, 2298), zuletzt geändert durch Art. 4 des Gesetzes vom 09.01.2002 (BGBl I 2002, 361).

427 Hierzu ausführlich die Seiten 62-65.

428 BVerfGE 313, 100 (376 und 383).

429 BVerfGE 313, 100 (377).

chung wegen begrenzter Kapazitäten faktisch beschränkt sei[430]. All diese Gesichtspunkte treffen auf die gegenwärtigen Vorhaben zur Einführung einer Vorratsspeicherung nicht zu, zumal es auf tatsächliche Begrenzungen – wie bereits gezeigt – ohnehin nicht ankommen kann[431]. Eine beachtliche Begrenzung der Überwachung im Fall der Vorratsspeicherung lässt sich auch nicht durch Verweis auf die Möglichkeiten anonymer Telekommunikation konstruieren, weil die ausschließliche Nutzung anonymer Formen von Telekommunikation auf Dauer nicht möglich oder jedenfalls unzumutbar ist[432].

§ 5 G10 ist insoweit weniger belastend als eine generelle Vorratsspeicherung, als das Bundesverfassungsgericht festgestellt hat, dass ein „verfassungswidriger Missbrauch“ der Befugnis vorliege, wenn sie „zur Einzelüberwachung von Personen oder zur Sammlung von Nachrichten über [...] Gefahren für die innere Sicherheit“ verwendet würde[433]. Auch zur Strafverfolgung darf dieses Instrument nicht eingesetzt werden. Das Mittel der strategischen Überwachung darf vielmehr nur ausnahmsweise zur Aufrechterhaltung der Sicherheit der Bundesrepublik Deutschland gegenüber Gefahren aus dem Ausland, die nicht vornehmlich personenbezogen sind, eingesetzt werden[434]. Nur dieser besondere Zweck rechtfertigt es, dass die Eingriffsvoraussetzungen im G10 anders bestimmt werden als es im Polizei- oder Strafprozessrecht verfassungsrechtlich zulässig ist[435]. Die generelle Aufbewahrung von Kommunikationsdaten ist demgegenüber auf ein nachträgliches Einschreiten in Einzelfällen zugeschnitten. Ansonsten wäre, wie im Bereich des § 5 G10, lediglich eine einmalige Prüfung der Daten erforderlich und nicht auch deren Aufbewahrung. Auch § 110a TKG zielt, wie § 110b Abs. 1 TKG zeigt, ausschließlich auf eine verbesserte Strafverfolgung. Die Richtlinie 2006/24/EG ist nach ihrem Art. 1 Abs. 1 von vornherein auf diesen Bereich beschränkt. In Anbetracht der weiten Verwendungsmöglichkeiten greift eine generelle Vorratsspeicherung von Telekommunikationsdaten daher in erheblich höherem Maße in die Grundrechte ein als § 5 G10.

Darüber hinaus sind selbst die „strategischen“ Kontrollmaßnahmen nach dem G10 nicht ebenso pauschal und allumfassend wie es eine Vorratsspeicherung wäre. Sie sind auf den internationalen Telekommunikationsverkehr beschränkt und werden auch nur im Einzelfall angeordnet, betreffen also nur den Telekommunikationsverkehr mit einzelnen Ländern. Außerdem ist ein Verfahren unter Einschaltung von Kontrollorganen vorgesehen, das die Eignung der Maßnahme fördern kann[436]. Voraussetzung einer Anordnung ist die begründete (vgl. § 9 Abs. 3 G10) Annahme, dass durch die Maßnahme Kenntnisse erlangt werden können, die zur Abwehr schwerster Gefahren für die Sicherheit Deutschlands erforderlich sind. Demnach besteht bei Maßnahmen nach § 5 G10 ein erheblich höherer Eignungsgrad als bei einer generellen Vorratsspeicherung sämtlicher Kommunikationsdaten.

Im Ergebnis ist festzuhalten, dass die einzige Verbindung zwischen den von einer Vorratsspeicherung betroffenen Personen und den Gefahren, die aus der Nutzung von Telekommunikationsnetzen zu rechtswidrigen Zwecken erwachsen, darin besteht, dass das gleiche Medium benutzt wird. Es liegen auch nicht die Voraussetzungen vor, unter denen eine allgemeine Telekommunikationsüberwachung bisher für zulässig erachtet worden ist.

Während Telekommunikationsnetze dort, wo sie als Werkzeug zur Begehung von Straftaten genutzt werden, noch eine eigenständige Rechtsgutsgefahr darstellen könnten, ist dies im Übrigen von vornherein ausgeschlossen. Gleichwohl greifen Eingriffsbehörden oftmals auf die Umstände auch von solchen Telekommunikationsvorgängen zu, die in keinem Zusammenhang mit der Begehung von Straftaten standen, sondern der alltäglichen Kommunikation dienten. Beispielsweise kann die Standortkennung des Mobiltelefons eines Straftäters von Strafverfolgungsbehörden abgefragt werden, um dessen Aufenthaltsort zu ermitteln, selbst wenn der Straftäter sein Mobiltelefon zu keiner Zeit zu rechtswidrigen Zwecken genutzt hat. Die Beziehung zwischen dem durchschnittlichen Telekommunikationsnutzer und den Gefahren, die einzelne Telekommunikationsnutzer allgemein verursachen, ist noch entfernter als in dem Bereich, in dem die Eigenschaften der Telekommunikationsnetze, von denen alle Telekommunikationsbenutzer profitieren, zur Begehung von Straftaten ausgenutzt werden.

Aufschlussreich für die Bemessung der Gefahrennähe ist auch das zahlenmäßige Verhältnis der Gesamtheit aller Telekommunikationsvorgänge zu der Anzahl von Telekommunikationsvorgängen, welche später zu Gefahrenabwehr- oder Strafverfolgungszwecken nachvollzogen werden müssen. Die Wahrscheinlichkeit, dass ein beliebiger Telekommunikationsvorgang zu einem späteren Zeitpunkt einmal zu Gefahrenabwehr- oder Strafverfolgungszwecken nachvollzogen werden muss, ist angesichts

430 BVerfGE 313, 100 (377 f.).
431 Seite 30.
432 Seite 55.
433 BVerfGE 67, 157 (180 f.).
434 BVerfGE 100, 313 (383).
435 BVerfGE 100, 313 (383).
436 BVerfGE 100, 313 (373).

der Vielzahl an Telekommunikationsvorgängen als verschwindend gering anzusehen[437]. Im Jahr 2002 wurden in Deutschland täglich 216 Millionen Telefonverbindungen hergestellt[438], im gesamten Jahr also etwa 79 Milliarden Verbindungen. Die Zahl von Telekommunikationsdatensätzen, die jährlich an Gefahrenabwehr- oder Strafverfolgungsbehörden übermittelt werden, ist zwar nicht bekannt. Es wird sich aber allenfalls um einige tausend Datensätze handeln. Die Wahrscheinlichkeit, dass eine Telefonverbindung zu einem späteren Zeitpunkt einmal nachvollzogen werden muss, läge damit bei einer Größenordnung von 0,00001%. Im Internetbereich wird diese Zahl noch erheblich geringer sein, weil hier ein Vielfaches an Kommunikationsdaten anfällt, Internet-Kommunikationsdaten von Gefahrenabwehr- oder Strafverfolgungsbehörden aber vergleichsweise selten angefordert werden. Berechnungen des Internet-Access-Providers T-Online haben ergeben, dass derzeit nur 0,0004% der insgesamt dort anfallenden Kommunikationsdaten von den Strafverfolgungsbehörden angefordert werden[439].

Angesichts dieser geringen Größenordnung ist fraglich, ob auf dem Gebiet der Telekommunikation die Wahrscheinlichkeit, dass ein beliebiger Kommunikationsvorgang zu einem späteren Zeitpunkt einmal zu Gefahrenabwehr- oder Strafverfolgungszwecken nachvollzogen werden muss, größer ist als im Bereich der traditionellen Kommunikation[440]. Ob dies der Fall ist, ist empirisch noch nicht geprüft worden. Jedenfalls soweit Telekommunikation nicht im unmittelbaren Zusammenhang mit der Begehung von Straftaten erfolgt, ist kein Grund ersichtlich, warum Kommunikationsdaten zu Gefahrenabwehr- oder Strafverfolgungszwecken nützlicher sein sollten als die Kenntnis der Umstände von Kommunikationsvorgängen außerhalb von Telekommunikationsnetzen. Während der Zugriff auf Kommunikationsdaten bei Straftaten, die mittels Telekommunikationsnetzen begangen werden, oft das einzige Mittel zur Aufklärung der Tat sein wird, wird dies bei anderweitig begangenen Straftaten nur ausnahmsweise der Fall sein. In diesem Bereich stellen Kommunikationsdaten eine Informationsquelle wie jede andere dar. Dass sich nur Telekommunikationsdaten generell erfassen und speichern lassen und dass die finanziellen Kosten einer solchen Vorratsspeicherung begrenzt sind, erhöht den durchschnittlichen Nutzen dieser Daten nicht und ist daher unbeachtlich. Es ist sogar denkbar, dass Telekommunikationsdaten von geringerem Erkenntnisinteresse sind als die näheren Umstände sonstiger Kommunikation, weil Straftätern die Überwachbarkeit der Telekommunikationsnetze bekannt ist und sie die Nutzung dieses Mediums für ihre Zwecke aus diesem Grunde möglichst vermeiden werden.

Soweit Telekommunikationsnetze zur Begehung von Netzkriminalität im engeren Sinne genutzt werden, ist zu beachten, dass sich Angriffe auf Computersysteme auch ohne Telekommunikationsnutzung vornehmen lassen. Insbesondere Angriffe von Mitarbeitern eines Unternehmens, die besonders schadensträchtig sind[441], werden vermutlich meist mittels eines Computers des angegriffenen Unternehmens selbst vorgenommen, weil die Angreifer dadurch vermeiden können, dass aufgrund der Zwischenschaltung von Telekommunikationsnetzen Datenspuren entstehen, die sie verraten könnten. Es lässt sich daher ohne nähere Untersuchung nicht sagen, ob im Bereich der Telekommunikation die Wahrscheinlichkeit, dass ein beliebiger Computerbenutzungsvorgang zu einem späteren Zeitpunkt einmal zu Gefahrenabwehr- oder Strafverfolgungszwecken nachvollzogen werden muss, größer ist als im Bereich der unmittelbaren Computernutzung.

Im Bereich der Netzkriminalität im weiteren Sinne wird die Telekommunikation letztlich zum Zweck des Austauschs von Informationen zwischen Menschen eingesetzt. Hier ist also zu fragen, ob der durchschnittliche Kommunikationsvorgang auf dem Gebiet der Telekommunikation öfter der Begehung einer Straftat dient als außerhalb dieses Gebiets, etwa bei der unmittelbar menschlichen Kommunikation oder der Kommunikation per Post. Die verfügbaren Kriminalitätsstatistiken erlauben es leider nicht, Anzahl und Schädlichkeit von Straftaten, die menschliche Kommunikation voraussetzen, inner- und außerhalb von Telekommunikationsnetzen zu vergleichen. Damit ist auch auf diesem Gebiet ein Vergleich der Gefahrennähe nicht möglich.

Lässt man die tatsächlichen Unsicherheiten außer Acht und nimmt man an, dass die Kenntnis der Umstände eines durchschnittlichen Telekommunikationsvorgangs für die Eingriffsbehörden nicht interessanter ist als die Kenntnis der Umstände sonstiger Kommunikationsvorgänge, so fragt es sich, ob schon die allgemeine Möglichkeit, dass Kommunikationsvorgänge zu einem späteren Zeitpunkt einmal von Eingriffsbehörden nachvollzogen werden müssen, deren generelle Aufzeichnung rechtfertigt. Gemessen an der nahezu unbegrenzten Anzahl von Gesprächen, Briefen und anderen Kommuni-

437 Dix, Alexander: Schriftliche Stellungnahme zur öffentlichen Anhörung am 09.02.2004 in Berlin zum Entwurf eines Telekommunikationsgesetzes (TKG), in Ausschussdrucksache 15(9)961, www.bitkom.org/files/documents/-StN_BITKOM_TKG_Wirtschaftsausschuss_03.02.04.pdf, 217 (219).

438 BVerfGE 107, 299 (327).

439 Uhe/Herrmann, Überwachung im Internet (I), 161.

440 Hierzu ausführlich die Seiten 99-108.

441 Seite 42.

kationsvorgängen liegt es auf der Hand, dass die Wahrscheinlichkeit, dass eine beliebiger Kommunikationsvorgang zu einem späteren Zeitpunkt einmal zu Gefahrenabwehr- oder Strafverfolgungszwecken nachvollzogen werden muss, verschwindend gering ist. Wollte man trotz dieser geringen Wahrscheinlichkeit eine hinreichende Nähe jedes Kommunizierenden, also im Grunde jedes Menschen, zur Begehung von Straftaten mittels menschlicher Kommunikation annehmen, dann wäre der Gesetzgeber zur Aufzeichnung der näheren Umstände jedes Informationsaustausches legitimiert, allein schon wegen der Tatsache des Informationsaustausches. Dies würde beispielsweise zum Aufbau eines allgemeinen Spitzelsystems berechtigen, wie es durch die Stasi organisiert wurde.

Fraglich ist, ob Derartiges mit dem Menschenbild des Grundgesetzes zu vereinbaren wäre. Das Bundesverfassungsgericht betont in ständiger Rechtsprechung, dass der Mensch ein gemeinschaftsbezogenes und gemeinschaftsgebundenes Wesen ist[442]. Er „ist eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit“[443]. Seiner besonderen Bedeutung entsprechend wird der Informationsaustausch auch durch das Grundgesetz besonders geschützt. So garantiert das Recht auf informationelle Selbstbestimmung den Schutz personenbezogener Informationen vor staatlichen Zugriffen. Das Gleiche gilt für Art. 10 GG. Art. 5 Abs. 1 und 2 GG gewährleistet die Meinungs-, Informations-, Presse- und Rundfunkfreiheit, deren Ausübung notwendig den Austausch von Informationen voraussetzt. Art. 4 Abs. 1 und 2 GG gewährleistet die ungestörte Religionsausübung, die oftmals in Gemeinschaft mit anderen erfolgt und dementsprechend auf einem Gedankenaustausch basiert. In der Tat lässt sich kaum ein Grundrecht denken, dessen Ausübung nicht einen Informationsaustausch erforderlich machen kann. Die Grundrechtsordnung des Grundgesetzes basiert darauf, dass die Grundrechte grundsätzlich ungestört von staatlichen Eingriffen ausgeübt werden können[444]. Jedenfalls muss der Einzelne keine unzumutbaren Eingriffe in seine Freiheiten dulden[445]. Außerdem gewährleistet Art. 19 Abs. 2 GG einen unantastbaren Bereich der ungestörten Grundrechtsausübung.

Dieser Konzeption des Grundgesetzes würde es widersprechen, wenn man bereits in dem bloßen Austausch von Informationen eine abstrakte Gefahr sehen würde, die den Staat zu Eingriffen berechtigte. Dass ein Informationsaustausch in manchen Fällen konkrete Gefahren begründet oder erhöht, muss vielmehr dem Bereich des allgemeinen Lebensrisikos zugeordnet werden. Der Austausch von Informationen allgemein begründet daher für sich genommen noch keine hinreichende Gefahrennähe der Kommunizierenden, so dass eine Vorratsspeicherung der näheren Umstände beliebiger Kommunikationsvorgänge unzulässig wäre.

Angesichts dessen kann eine generelle Kommunikationsdatenspeicherung nur dann gerechtfertigt sein, wenn die näheren Umstände der Telekommunikation für den Schutz von Rechtsgütern von größerer Relevanz sind als die Umstände sonstiger Kommunikation. Ob dies der Fall ist, ist – wie bereits ausgeführt[446] – unbekannt.

(ff) Aussagekraft der Daten, die erhoben werden können, unter Berücksichtigung ihrer Nutzbarkeit und Verwendungsmöglichkeit; den Betroffenen drohende Nachteile nach Ausmaß und Wahrscheinlichkeit ihres Eintritts

Die vorliegenden Vorschläge zur Einführung einer Vorratsspeicherung sind vage, was die genaue Art der zu speichernden Daten angeht. Der Grund dafür wird darin zu sehen sein, dass Widerstände sowohl von Bürgern wie auch von der Wirtschaft zu erwarten sind, sobald diese klar vor Augen haben, was die Regelungen tatsächlich bedeuten. Es wird daher für politisch klüger erachtet, zunächst die generelle Befugnisnorm zu schaffen. Wenn es dann später um die konkrete Umsetzung geht und den Betroffenen die konkrete Bedeutung der Norm bewusst wird, ist es für sie schon zu spät, über das „Ob“ der Regelung noch zu diskutieren. Diese „Scheibchentaktik“ wurde im Bereich des § 88 TKG a.F. (jetzt § 110 TKG), der erst 2001 durch die TKÜV konkretisiert wurde, erfolgreich angewandt. Auch in EU-Ländern, in denen die Einführung einer generellen Vorratsspeicherung von Kommunikationsdaten geplant ist, ist auf diese Weise verfahren worden.

§ 110a TKG zufolge sollen insbesondere solche Telekommunikationsdaten gespeichert werden, welche die Identifizierung von Ursprung, Ziel, Zeit und Ort eines Informationsaustausches, des eingesetzten Kommunikationsgeräts (bei Mobiltelefonen etwa die IMEI) sowie des Kunden und des Benutzers des elektronischen Kommunikationsdienstes (§ 111 TKG) erlauben.

442 St. Rspr. des BVerfG seit E 4, 7 (15).
443 BVerfGE 65, 1 (44).
444 BVerfGE 65, 1 (44): „Grundrechte [...] als Ausdruck des allgemeinen Freiheitsanspruchs des Bürgers gegenüber dem Staat“.
445 St. Rspr. des BVerfG; für Art. 10 GG vgl. nur BVerfGE 67, 157 (178); BVerfGE 100, 313 (391).
446 Seite 60.

Bei der Bemessung der Eingriffsintensität einer Vorratsspeicherung ist zudem der Vergleich mit bestehenden Eingriffsbefugnissen von Nutzen. Dieser ergibt zunächst, dass die Verarbeitung von Kommunikationsdaten mit erheblich größeren Gefahren verbunden ist als die automatische Verarbeitung personenbezogener Daten generell; die allgemeinen Gefahren einer automatisierten Datenverarbeitung erhalten im Bereich der Telekommunikationsnetze eine neue Dimension[447], denn hier besteht die Möglichkeit, Persönlichkeitsbilder mit einer noch nie da gewesenen Genauigkeit zu gewinnen. Das liegt zum einen daran, dass Daten über jede Telekommunikationsnutzung eines Teilnehmers anfallen, das Telekommunikationsverhalten einer Person also vollständig dokumentiert werden kann. In anderen Bereichen müsste ein solcher Datenberg erst aus unterschiedlichen Quellen zusammen getragen werden, etwa in dem aufwändigen Verfahren der Rasterfahndung. Eine weitere, besondere Gefahr auf dem Gebiet der Telekommunikation ergibt sich daraus, dass die Speicherung von Kommunikationsdaten entweder schon in der Struktur der Systeme angelegt ist oder sich mit begrenztem Aufwand durchführen lässt. Nicht zuletzt sind Kommunikationsdaten auch inhaltlich äußerst aussagekräftig und geben selbst über intime Details Auskunft, etwa im Bereich der Internet-Nutzung. Es lässt sich sagen, dass sich der Mensch nirgendwo im dem Maße, in all seinen Facetten und in so konstanter und aussagekräftiger Weise offenbart wie in den Telekommunikationsnetzen.

Vergleicht man weiterhin beispielsweise den Zugriff auf Mobiltelefon-Positionsdaten mit dem klassischen Mittel der Observation, so ergeben sich gravierende Unterschiede[448]: Standortdaten können auch für die Vergangenheit abgefragt werden, was eine Observation nicht leisten kann. Standortdaten können zeitlich lückenlos aufgezeichnet werden, was bei einer Observation nicht gewährleistet ist. Die Abfrage von Standortdaten bleibt dem Betroffenen – anders als eine Observation – mit Sicherheit verborgen. Schließlich ist der Zugriff auf Kommunikationsdaten für die Behörden mit einem viel geringeren Einsatz von Personal und Kosten möglich als die Vornahme einer Observation, so dass Informationseingriffe tendenziell öfter stattfinden werden. Auch dieses Beispiel zeigt die erheblich höhere Eingriffsintensität einer generellen Vorratsspeicherung von Telekommunikationsdaten gegenüber bestehenden Eingriffsbefugnissen.

(i) Vergleich mit der Aussagekraft von Kommunikationsinhalten

Weit verbreitet ist die Behauptung, der staatliche Zugriff auf die näheren Umstände der Telekommunikation wiege weniger schwer als der Zugriff auf ihren Inhalt[449]. Gegen die Richtigkeit dieser meist ohne Begründung angeführten These, die an die Art des jeweiligen Datums anknüpft, spricht die Feststellung des Bundesverfassungsgerichts, dass bei der Bemessung der Intensität eines Informationseingriffs „nicht allein auf die Art der Angaben abgestellt werden [kann]. Entscheidend sind ihre Nutzbarkeit und Verwendungsmöglichkeit. Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungsmöglichkeiten und Verknüpfungsmöglichkeiten ab. Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses' Datum mehr."[450]

Konkret liegt beispielsweise auf der Hand, dass die Kenntnisnahme des Inhalts eines belanglosen Telefonats mit dem Nachbarn weniger belastend ist als die Kenntnisnahme sämtlicher Positionsdaten eines Mobiltelefons, anhand derer sich ein Bewegungsprofil des Besitzers erstellen lässt. Kommunikationsdaten sind also keineswegs zwangsläufig weniger aussagekräftig als Kommunikationsinhalte. Sie können es im Einzelfall sein, oft verhält es sich aber auch umgekehrt.

Wie bereits erwähnt, sind bei der Beurteilung der Intensität eines Informationseingriffs auch die Möglichkeiten der Verarbeitung oder Verknüpfung erlangter Daten zu berücksichtigen[451]. Kommunikationsinhalte – mit Ausnahme unverschlüsselter Textübertragungen wie E-Mail oder SMS – liegen regelmäßig nicht in maschinenlesbarer Form vor (z.B. akustische Gespräche, Telefaxe). In absehbarer Zukunft werden keine Computer zur Verfügung stehen, die ausreichend leistungsfähig sind, den Inhalt solcher Kommunikationsvorgänge automatisch zu analysieren oder eine Vielzahl von Kommunikationsvorgängen nach bestimmten Inhalten zu durchsuchen. Eine Auswertung wird vielmehr stets durch Menschen erfolgen müssen, so dass Inhalte bereits aus diesem Grund nur punktuell erfasst werden können. Auch ist im Bereich der E-Mail-Kommunikation eine effektive, kostengünstige und einfache

447 Zum Folgenden Gridl, Datenschutz in globalen Telekommunikationssystemen, 74 ff.

448 Schenke, AöR 125 (2000), 1 (28).

449 BVerfGE 107, 299 (322); BVerfGE 109, 279 (345); Bundesregierung in BT-Drs. 14/7008, 6 für Verbindungsdaten: „regelmäßig"; Bundesrat in BT-Drs. 14/7258, 1 für Verbindungsdaten: „bei weitem"; Thüringen in BR-Drs. 513/02, 3 für Mobilfunkstandortdaten; BGH-Ermittlungsrichter, MMR 1999, 99 (101) für Verbindungsdaten; Weichert, Bekämpfung von Internet-Kriminalität (I), Punkt 3: „regelmäßig"; Germann, 620: „deutlich".

450 BVerfGE 65, 1 (45).

451 BVerfGE 65, 1 (45).

Verschlüsselung der Kommunikationsinhalte möglich[452], so dass eine staatliche Vorratsspeicherung insoweit nutzlos wäre. Selbst unverschlüsselte, maschinenlesbare Kommunikationsinhalte könnten wegen der unüberschaubaren Datenmengen kaum auf Vorrat gespeichert werden. Die Entlastung, welche die Ausnahme von Kommunikationsinhalten von einer Vorratsspeicherung bewirkt, darf daher nicht überschätzt werden[453].

Im Vergleich zu Inhaltsdaten sind die Verarbeitungsmöglichkeiten von Kommunikationsdaten weit höher. Da Kommunikationsdaten von vornherein als computerlesbare Datensätze gespeichert werden, eignen sie sich in hohem Maße zur Speicherung, Übermittlung und Verknüpfung mit anderen Datenbeständen. Sie können automatisch analysiert und auf bestimmte Suchmuster hin durchkämmt[454], nach bestimmten Kriterien geordnet und ausgewertet[455] werden. All diese Möglichkeiten bestehen bei Inhaltsdaten nicht, was für eine höhere Sensibilität von Kommunikationsdaten spricht.

In vielen Fällen ist der Staat auch von vornherein oder jedenfalls zunächst nur an den Umständen eines Telekommunikationsvorgangs interessiert. Geht es etwa darum, heraus zu finden, von welchem Telefonanschluss aus zu einer bestimmten Zeit ein bestimmter anderer Anschluss angerufen wurde (beispielsweise in einem Erpressungsfall), dann müssen alle bei einem Telekommunikationsunternehmen gespeicherten Verbindungsdaten daraufhin durchgesehen werden, ob sie mit diesen Suchmerkmalen übereinstimmen. Was in den einzelnen Gesprächen gesagt wurde, ist den Behörden gleichgültig. Bei dieser Maßnahme geht es nicht um den Inhalt der Gespräche, so dass es falsch wäre, dem Eingriff geringes Gewicht zuzumessen, weil „nur“ Kommunikationsdaten betroffen sind. Der Eingriff hat vielmehr umgekehrt ein besonders großes Gewicht, da er die Daten einer Vielzahl unbeteiligter Personen betrifft.

Während die Eingriffsbehörden häufig nur oder jedenfalls zunächst nur an Kommunikationsdaten interessiert sind, kommt der umgekehrte Fall praktisch nicht vor. Selbst im Fall der strategischen Telekommunikationsüberwachung durch den BND ist ein Zugriff auf Kommunikationsdaten erforderlich, um festzustellen, mit welchem Land kommuniziert wird. Die strategische Überwachung nach dem G10 kann nämlich nur für bestimmte Länder angeordnet werden. Aus diesem Grund ist ein Abhören von Kommunikationsinhalten praktisch bedeutungslos, wenn nicht zugleich festgestellt werden kann, wer an dem Kommunikationsvorgang beteiligt ist. Die Aussage, Kommunikationsdaten seien für die Arbeit der Sicherheitsbehörden ebenso wichtig wie Kommunikationsinhalte[456], ist daher eine Untertreibung. An der fehlenden praktischen Nutzbarkeit von Kommunikationsinhalten ohne die zugehörigen Kommunikationsdaten zeigt sich die essenzielle Bedeutung von Telekommunikationsdaten.

Hinzu kommt, dass die Unterscheidung von Inhalts- und Kommunikationsdaten besonders im Internetbereich unklar ist[457]. Im Bereich öffentlich zugänglicher Internet-Inhalte erlaubt es die Kenntnis der Kommunikationsdaten (URLs) etwa regelmäßig, den Inhalt der Kommunikation selbst nachzuvollziehen[458]. Dazu genügt es, die URL in einen Internet-Browser einzugeben. Dementsprechend ist eine niedrigere Eingriffsschwelle als für den unmittelbaren Zugriff auf Kommunikationsinhalte nicht gerechtfertigt[459]. Teilweise werden WWW-Nutzungsdaten – die als Kommunikationsumstände an sich zu den Kommunikationsdaten zu zählen sind[460] – schon dem Kommunikationsinhalt zugerechnet[461].

---

452 BMI/BMJ, Sicherheitsbericht 2001, 200, wonach PGP-chiffrierte Daten derzeit mit unter Kostengesichtspunkten vertretbaren Mitteln nicht entschlüsselbar seien.

453 Weinem (Diplom-Informatiker beim Bundeskriminalamt), TK-Überwachung, 451 (453).

454 DSB-Konferenz, Freie Telekommunikation (I); Omega Foundation, Report (I) mit der Forderung, den Einsatz solcher Techniken denselben Tatbestandsvoraussetzungen zu unterwerfen wie das Abfangen von Telekommunikationsinhalten.

455 Gridl, Datenschutz in globalen Telekommunikationssystemen, 61.

456 Weinem (Diplom-Informatiker beim Bundeskriminalamt), TK-Überwachung, 451 (453).

457 Kommission, Discussion Paper for Expert’s Meeting on Retention of Traffic Data (I); Artikel-29-Gruppe der EU, Privatsphäre im Internet (I), 55.

458 Schaar, Cybercrime und Bürgerrechte (I), 11; Queen Mary (University of London), Studie über Netzkriminalität (I); Kommission, Discussion Paper for Expert’s Meeting on Retention of Traffic Data (I); Weßlau, ZStW 113 (2001), 681 (703); Weichert, Thilo: BigBrotherAward 2002 in der Kategorie „Kommunikation“, 25.10.2002, www.big-brother-award.de/2002/.comm. Laut EPIC/PI, Privacy and Human Rights 2002 (I), Teil I, 58 und Queen Mary (University of London), Studie über Netzkriminalität (I) sind in Großbritannien für den Zugriff auf URLs stärkere Schutzvorkehrungen vorgesehen als für den Zugriff auf sonstige Verkehrsdaten, soweit nicht nur auf den Namen des Servers zugegriffen wird.

459 Artikel-29-Gruppe der EU, Privatsphäre im Internet (I), 55.

460 Schaar, Retention (I), 1.

461 Schaar, Datenschutz im Internet, Rn. 143; EPIC/PI, Privacy and Human Rights 2002 (I), Teil I, 57: dem Kommunikationsinhalt ähnlicher als Verbindungsdaten; laut Dänemark in MDG, EU-Questionnaire (I), 13 f. unterliegt dort der Zugriff auf Verkehrsdaten denselben Voraussetzungen wie der Zugriff auf Inhaltsdaten; Gridl, Datenschutz in globalen Telekommunikationssystemen, 74: „Aufgrund der verschwimmenden Grenzen zwischen diesen beiden Daten im Internet und in Online-Netzen kann die klassische Unterscheidung zwischen dem Inhalt einer Kommunikation und der Information darüber, dass eine solche Kommunikation stattgefunden hat, nicht mehr aufrecht erhalten werden.“

Das Verschwimmen der Grenzen von Verkehrs- und Inhaltsdaten ist nicht auf das Internet begrenzt. Auch wo die Telefontastatur zur Eingabe von Kontonummern und anderen Inhaltsdaten genutzt wird, ist eine technische Abgrenzung zur Eingabe von Telefonnummern nicht möglich[462]. Dabei erlaubt es die Kenntnis der „Kommunikationsdaten", die bei der Kommunikation mit dem Telefoncomputer einer Bank anfallen („Telefonbanking"), den gesamten Kommunikationsvorgang nachzuvollziehen: Werden die aufgezeichneten Ziffern im Rahmen eines Anrufs des Telefoncomputers durch die Polizei erneut gewählt, dann kann ihre Bedeutung anhand der Ansagen des Telefoncomputers ohne Weiteres nachvollzogen werden. Auch insoweit fehlt jeder Unterschied zu einer direkten Aufzeichnung des Inhalts des Gesprächs, so dass unterschiedliche Eingriffsschwellen nicht gerechtfertigt sind.

Besonders im Bereich der neuen Technologien können Kommunikationsdaten aussagekräftiger sein als die Kenntnis von Inhalten. Während Kommunikationsdaten traditionell allenfalls im Bereich der Individualkommunikation zur Verfügung standen und dort nur besagen, ob, wann und wie oft zwischen welchen Personen oder Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat oder versucht worden ist[463], hat die Feststellung der jeweiligen Position eines Mobiltelefons oder der von einer Person abgerufenen Internet-Inhalte eine völlig neue Qualität[464]. Schon quantitativ entstehen durch ein eingeschaltetes Mobiltelefon oder während einer Internetsitzung laufend neue Kommunikationsdaten, während im Bereich der Sprachtelefonie nur ein Datensatz pro Kommunikationsvorgang anfällt. Gerade im Bereich der neuen Netze fällt eine so große Menge an Kommunikationsdaten an, dass die Bildung umfassender Persönlichkeits- und Verhaltensprofile möglich ist[465].

In geringerem Maße ist dies auch im Bereich der Individualkommunikation der Fall. Zwar bilden Verbindungsdaten in diesem Bereich insgesamt gesehen nicht einen ebenso großen Bereich des täglichen Lebens ab. Im Einzelfall kann die Kenntnis der Tatsache, ob, wann und wie oft zwischen bestimmten Personen oder Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat oder versucht worden ist, für den Betroffenen aber belastender sein als die Kenntnis von Internet-Kommunikationsdaten oder Gesprächsinhalten. Dies gilt nicht nur für das Verbindungsdatum der Position eines Mobiltelefons, dessen Aufzeichnung weitgehende Schlüsse über das Verhalten des Benutzers erlaubt. Auch die Kenntnis des Gesprächspartners (z.B. Anwalt für internationales Steuerrecht, Drogenhilfe, auf Geschlechtskrankheiten spezialisierter Arzt), der sich anhand des Verkehrsdatums der Anschlussnummer ermitteln lässt, ermöglicht Rückschlüsse auf das Privatleben einer Person[466]. Bereits aus solchen Verbindungsdaten können – auch falsche – Folgerungen über Gesundheitszustand, kriminelle Verstrickungen oder sonstige Eigenschaften einer Person gezogen werden[467]. Das Bundesverfassungsgericht stellt daher fest, dass „Verbindungsdaten ein detailliertes Bild über Kommunikationsvorgänge und Aufenthaltsorte" ermöglichen[468] und Rückschlüsse etwa auf das soziale Umfeld einer Person erlauben[469]. Die Eingriffsintensität, so das Gericht, würde durch die Datenmenge weiter verstärkt, da Auskunftsanordnungen über Verbindungsdaten meist eine Vielzahl von Verbindungen und Personen erfassten[470].

Weil Telekommunikation in immer mehr Bereichen des täglichen Lebens zum Einsatz kommt, hat sich auch die Menge der anfallenden Kommunikationsdaten erhöht. Im Jahr 2002 wurden täglich 216 Millionen Telefonverbindungen hergestellt[471]. 1997 fielen allein im Festnetz der Deutschen Telekom AG 54 Milliarden Verbindungsdatensätze an[472]. Nimmt man den Mobilfunkbereich und den Internetbereich hinzu, dann wird deutlich, dass gespeicherte Telekommunikationsdaten eine Datensammlung unermesslichen Ausmaßes darstellen[473]. Teilweise wird angenommen, dass es sich schon bei den bisher von Telekommunikationsunternehmen gespeicherten Kommunikationsdaten um die größte Sammlung personenbezogener Daten in Deutschland handele[474].

Bei genauer Betrachtung ist auch der Inhalt eines Kommunikationsvorgangs nichts anderes als ein näherer Umstand der Kommunikation[475], weil er den Kommunikationsvorgang näher beschreibt. Die

462 Queen Mary (University of London), Studie über Netzkriminalität (I).
463 Vgl. BVerfGE 100, 313 (358).
464 Schaar, Retention (I), 2 für Positionsdaten; Gridl, Datenschutz in globalen Telekommunikationssystemen, 74: „neue Dimension"; Meade, Retention of Communications Traffic Data (I): „far more personal and revealing".
465 Gridl, Datenschutz in globalen Telekommunikationssystemen, 61.
466 Gridl, Datenschutz in globalen Telekommunikationssystemen, 73 f.
467 Gridl, Datenschutz in globalen Telekommunikationssystemen, 74.
468 BVerfGE 107, 299 (322).
469 BVerfGE 107, 299 (320).
470 BVerfGE 107, 299 (320 f.).
471 BVerfGE 107, 299 (327).
472 Welp, TKÜV, 3 (9).
473 Welp, TKÜV, 3 (9).
474 Welp, TKÜV, 3 (9).
475 Vgl. Breyer, Vorratsspeicherung, 76 f.

Unterscheidung von Verkehrs- und Inhaltsdaten ist daher rein technischer und begrifflicher Art, ohne dass daraus auf eine unterschiedliche Aussagekraft der jeweiligen Daten geschlossen werden könnte. Kommunikationsdaten bilden vielmehr einen mindestens ebenso großen Ausschnitt des täglichen Lebens ab wie Kommunikationsinhalte[476].

Die anfängliche Plausibilität der These, der Zugriff auf Kommunikationsdaten wiege weniger schwer als der Zugriff auf Inhalte, beruht allein auf der Tatsache, dass die Kenntnisnahme der äußeren Umstände eines Kommunikationsvorgangs weniger belastend ist als wenn zusätzlich noch der Kommunikationsinhalt abgehört wird. Hierbei handelt es sich aber um keine Besonderheit im Verhältnis von Verkehrs- zu Inhaltsdaten. Der Zugriff auf eine quantitativ größere Datenmenge ist für den Betroffenen vielmehr immer belastender als der Zugriff auf nur einige dieser Daten. Wollte man bei der rechtlichen Ausgestaltung der Eingriffsschwellen auf diesen Unterschied abstellen, so müsste man die Eingriffsvoraussetzungen von der Menge wahrgenommener Daten abhängig machen. Es kann demgegenüber nicht angehen, dass das Kommunikationsverhalten einer Vielzahl von Personen anhand derer Telekommunikationsdaten unter geringeren Voraussetzungen nachvollzogen werden darf als der Inhalt eines Telefongesprächs zwischen Nachbarn.

Dem Bundesverfassungsgericht zufolge ist für die Beurteilung der Schwere eines Informationseingriffs die Nutzbarkeit und Verwendungsmöglichkeit des jeweiligen Datums entscheidend. Nach dem Gezeigten kann, abhängig von den jeweiligen Umständen des Einzelfalls, die Aussagekraft von Telekommunikationsdaten die Aussagekraft von Inhalten erreichen oder übersteigen[477]. Ein Grundsatz, wonach Kommunikationsdaten typischerweise weniger schutzbedürftig seien als Inhaltsdaten, lässt sich nicht aufstellen[478]. Da sich die Schwere der Belastung eines Grundrechtsträgers durch die Kenntnisnahme von Aspekten seiner Telekommunikation jeweils nur im Einzelfall bestimmen lässt, die Voraussetzungen eines zulässigen Eingriffs in das Fernmeldegeheimnis aber durch abstrakt-generelle Rechtsnormen zu regeln sind[479], ist ein unterschiedliches Schutzniveau für Inhaltsdaten einerseits und Kommunikationsdaten andererseits nicht gerechtfertigt[480], wie es in den Rechtsordnungen einer Reihe von Ländern bereits anerkannt ist[481].

(ii) Besonders sensible Kommunikationsdaten

Auch wenn die Bedeutung einer Unterscheidung von Daten ihrer Art nach im Allgemeinen gering ist, ist sie doch in den Fällen relevant, in denen ein Datum seiner Natur nach in besonders belastender Weise verwendet werden kann[482]. Dies gilt insbesondere für sensible Daten etwa über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben (vgl. § 3 Abs. 9 BDSG). Solche Daten können im Bereich von Telekommunikationsdaten etwa insoweit anfallen, wie die Identität eines Kommunikationspartners – insbesondere bei dauerhaften Kommunikationsbeziehungen – Rückschlüsse auf derartige Tatsachen erlaubt. Das Internet etwa wird im Bereich von Diskussionsforen (Newsgroups) und Beratungsangeboten spezifisch zur Preisgabe und Diskussion von Details des Sexual- und Intimlebens und von Tatsachen genutzt, deren Kenntnis und Zuordnung durch Dritte die Gefahr sozialer Abstempelung (etwa als Drogensüchtiger, Vorbestrafter, Geisteskranker, Asozialer)[483] mit sich bringt. Das Gleiche gilt für Telekommunikation außerhalb des Internet[484]. Insbesondere die Rufnummern der Gesprächspartner und der jeweilige Aufenthaltsort, der sich aus Telekommunikationsdaten ermitteln lässt, kann derartige Rückschlüsse erlauben.

476 Walden, Ian in APIG, All Party Parliamentary Internet Group (UK): Dr. Ian Walden, APIG Communications Data Inquiry Oral Evidence, 11.12.2002, www.apig.org.uk/walden_oral_evidence.htm.

477 DSB-Konferenz, Datenschutzbeauftragte des Bundes und der Länder: Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in der Telekommunikation, Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08.10.1999, BT-Drs. 14/5555, 217; so auch bereits 1984 der Richter am EGMR Pettiti in seiner zustimmenden Meinung zu EGMR, Malone-GB (1984), Publications A82: „It is known that, as far as data banks are concerned, the processing of 'neutral' data may be as revealing as the processing of sensitive data."

478 Allitsch, CRi 2002, 161 (164).

479 Breyer, Vorratsspeicherung, 101.

480 Internationale Konferenz der Datenschutzbeauftragten, Fernmeldegeheimnis (I); Schaar, Retention (I), 2 für Standortdaten; Queen Mary (University of London), Studie über Netzkriminalität (I); Welp, Die strafprozessuale Überwachung des Post- und Fernmeldeverkehrs, 129; ders., Überwachung und Kontrolle, 91; Omega Foundation, Working document (I), Punkt 4.vii. für die automatische Auswertung von Telefongesprächen; Data Protection Commissioner (UK), RIP (I), Punkt 8; Allitsch, CRi 2002, 161 (164 und 166): „outdated and artificial distinction"; IWGDPT, Standortdaten für Standortdaten.

481 G8 Workshop, Workshop A (I); für Österreich Lücking, Die strafprozessuale Überwachung des Fernmeldeverkehrs.

482 Vgl. Bizer, Forschungsfreiheit, 148 f.

483 BVerfGE 65, 1 (48); BVerfGE 78, 78 (87).

484 Seite 64.

Während sich bei der bisherigen Erfassung von Daten im Einzelfall meistens feststellen lässt, wie sensibel ein Datum ist (vgl. § 100h Abs. 2 StPO), würde eine Vorratsspeicherung unterschiedslos die gesamte Nutzung von Telekommunikationsnetzen abbilden. Es ist technisch unmöglich, sensible Daten von der Aufzeichnung auszunehmen[485]. Dies erhöht die Eingriffsintensität einer Vorratsspeicherung von Telekommunikationsdaten weiter.

Das Leben des modernen Menschen verlagert sich zunehmend in den Bereich der Telekommunikationsnetze[486], wie bereits die Schlagworte Telearbeit, Telemedizin, Telebanking, Telelernen, Teleshopping und Telematik deutlich machen. Betroffen von diesem Trend ist nicht nur das öffentliche, sondern auch das Privatleben. Eine Vorratsspeicherung von Telekommunikations- und Internet-Nutzungsdaten würde weite – und weiterhin steigende – Teile des Privatlebens erfassen. Dementsprechend groß sind auch die Nachteile, die mit einer Vorratsspeicherung einher gehen könnten.

(iii) Staatliche Fehlurteile

Ein Nachteil, den eine generelle Vorratsspeicherung von Telekommunikationsdaten mit sich bringen könnte, ist eine erhöhte Anzahl von Fehlentscheidungen in Ermittlungs- und Gerichtsverfahren. Wie verbreitet Irrtümer in Ermittlungsverfahren allgemein sind, zeigt sich daran, dass 1998 in den alten Bundesländern 2.728 strafmündige Personen von der Polizei ermittelt wurden, welche die Polizei für überführt hielt, ein vorsätzliches Tötungsdelikt begangen zu haben. Wegen eines vorsätzlichen Tötungsdelikts rechtskräftig verurteilt wurden im selben Jahr aber nur 875 Personen[487], also etwa ein Drittel der vorgenannten Zahl. Für die Annahme einer erheblichen Zahl von Fehlurteilen der Staatsanwaltschaft spricht, dass 1998 in den alten Bundesländern 947.187 Personen strafrechtlich angeklagt wurden, davon aber 176.000 Personen freigesprochen wurden oder das Verfahren gegen sie durch das Gericht eingestellt wurde[488].

Dass auch gerichtliche Fehlentscheidungen nicht selten sind, zeigen beispielsweise wissenschaftliche Untersuchungen in den USA, wo immer wieder Fälle von zu Unrecht ausgesprochenen Todesurteilen an das Licht der Öffentlichkeit gelangen. In der Tat liegt bei genauer Betrachtung jedem erfolgreichen Rechtsmittel eine gerichtliche Fehlentscheidung in der Vorinstanz zugrunde. Rechtsmittel sind in unzähligen Fällen erfolgreich, und auch wenn sie nicht eingelegt werden oder werden können, garantiert das nicht die Richtigkeit einer Entscheidung. Vielmehr ist anzunehmen, dass eine substanzielle Anzahl rechtskräftiger Gerichtsentscheidungen falsch ist. Es ist daher von großer Bedeutung, eine angemessen hohe Einschreitschwelle für strafprozessuale Ermittlungen vorzusehen, um Fehlurteilen vorzubeugen.

Insgesamt muss davon ausgegangen werden, dass viele Personen unschuldig in Ermittlungs- und Strafverfahren verwickelt werden und dass es in einer erheblichen Anzahl von Fällen zu ungerechtfertigten Verurteilungen kommt. Zahlenmäßig ist von Hunderttausenden auszugehen, die jedes Jahr unschuldig von Eingriffen betroffen sind[489]. Nicht nur staatskritische Personen wie Globalisierungskritiker müssen staatliche Vor- und Fehlurteile fürchten, wenn sie in einen falschen Verdacht geraten. Selbst der unauffälligste Kleinstadtbürger, der an sich „nichts zu verbergen“[490] hat, kann unschuldig belangt werden, wenn er zur falschen Zeit am falschen Ort war.

Zugriffsmöglichkeiten der Behörden auf Telekommunikationsdaten erhöhen die allgemeine Gefahr, unschuldig verdächtigt zu werden[491]. Erstens beziehen sich Kommunikationsdaten stets nur auf den Inhaber eines Anschlusses. Wird der Anschluss ohne Wissen des Inhabers missbraucht, dann kann dieser leicht in einen falschen Verdacht geraten. Zweitens ermöglicht es der Zugriff auf Kommunikationsdaten den Behörden, nach dem Eliminierungsprinzip zu arbeiten. Dabei wird nicht, wie traditionell üblich, eine „heiße Spur“ verfolgt, sondern es werden – etwa mit Hilfe von Kommunikationsdaten – eine (oft große) Gruppe von Personen ermittelt, die aufgrund bestimmter Merkmale als Täter in Betracht kommen (beispielsweise alle Personen, die innerhalb eines bestimmten Zeitraums das Opfer einer Straftat angerufen haben). Es kommt dadurch quasi zu einer Inflation an Verdächtigungen, aus der sich die so Erfassten nur noch im Wege einer Art Beweislastumkehr befreien können[492]. Weil ein Kommunikationsdatensatz ein Indiz gegen den Angeklagten bilden kann, muss dieser unter Umständen den Richter von seiner Unschuld überzeugen (vgl. § 261 StPO), um nicht zu Unrecht verurteilt zu

485 Weichert, Bekämpfung von Internet-Kriminalität (I), Punkt 6.
486 DSB-Konferenz, Freie Telekommunikation (I).
487 BMI/BMJ, Sicherheitsbericht 2001, 4 f.
488 BMI/BMJ, Sicherheitsbericht 2001, 360.
489 Albrecht, Die vergessene Freiheit, 139.
490 Vgl. Wagner, Marita: Intimsphäre - lückenlos überwacht? Telepolis, Heise-Verlag, 28.06.2002, www.heise.de/tp/-deutsch/inhalt/te/12813/1.html.
491 BVerfGE 107, 299 (321).
492 Hamm, TKÜV, 81 (86).

werden[493]. Mangels eines Alibis wird Unschuldigen der Beweis des Gegenteils keineswegs immer gelingen.

Aber auch, wenn sich die Unschuld einer Person noch im Ermittlungsverfahren herausstellt, kann ein falscher Verdacht ausreichen, um zu Hausdurchsuchungen, Untersuchungshaft, Bewegungseinschränkungen oder Aus- und Einreiseverboten zu führen, was mit erheblichen Belastungen für die Betroffenen verbunden ist. Dies verdeutlicht ein Blick auf die Rasterfahndung zum Auffinden von Terroristen, die allein in Nordrhein-Westfalen Informationen über 250.000 Personen erbracht hat[494]. „Verdächtige" Personen wurden von der Polizei überprüft, wobei die Überprüfung die Befragung von Nachbarn, Hausmeister und Arbeitgeber ebenso einschließen konnte wie das Durchsuchen des Mülleimers[495].

Folgende Fälle von Fehlurteilen aufgrund einer Analyse von Telekommunikationsdaten sind in Europa bereits bekannt geworden: In Österreich wurde ein Nigerianer mehrere Monate lang in Untersuchungshaft genommen, weil er wegen seiner zahlreichen Telefonkontakte als Anführer einer Rauschgiftbande in Verdacht geraten war[496]. Später stellte sich der Verdacht als unbegründet und der Nigerianer lediglich als gefragter Ratgeber in der schwarzen Gemeinschaft in Wien heraus[497]. In Schweden gab es Fälle, in denen unschuldige Personen im Zusammenhang mit Ermittlungen wegen Netzkriminalität festgenommen wurden. Später stellte sich heraus, dass die wirklichen Straftäter den Internet-Zugangscode der festgenommenen Personen ohne deren Kenntnis missbraucht hatten[498].

Aufgrund des begrenzten Aussagegehalts von Telekommunikationsdaten und der Tatsache, dass der Zugriff auf Kommunikationsdaten oft eine Vielzahl von Personen betrifft, birgt der Zugriff auf Kommunikationsdaten ein besonderes Risiko falscher Verdächtigungen. Weil eine generelle Vorratsspeicherung eine erheblich umfangreichere Speicherung von Kommunikationsdaten als bisher zur Folge hätte, ist zu erwarten, dass auch die Anzahl der Zugriffe auf Kommunikationsdaten erheblich steigen würde. Damit würde sich auch das Risiko von Fehlentscheidungen in Ermittlungs- und Gerichtsverfahren erhöhen.

(iv) Staatlicher Gebrauch und Missbrauch von Kommunikationsdaten

Aufgrund der hohen Aussagekraft von Telekommunikationsdaten birgt eine Sammlung dieser Daten zudem die Gefahr staatlichen Missbrauchs. Die Artikel-29-Datenschutzgruppe stellt fest: „Allein dadurch, dass es sie gibt, ermöglichen es Kommunikationsdaten, persönliches Verhalten in einem bisher ungekannten Maße zu überwachen und zu kontrollieren."[499] Telekommunikation wird heute längst nicht mehr nur zur persönlichen Kommunikation genutzt, sondern zur Bewältigung fast beliebiger Alltagsaktivitäten, seien sie intimer, privater oder beruflicher Art. Dies lässt die Telekommunikationsüberwachung zu einem Mittel der Totalkontrolle werden[500]. Die Datenschutzbeauftragten des Bundes und der Länder wiesen schon 1996 auf diese Gefahr hin[501]: „Bei digitalen Kommunikationsformen läßt sich anhand der Bestands- und Verbindungsdaten nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und damit wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Eine staatliche Überwachung dieser Vorgänge greift tief in das Persönlichkeitsrecht der Betroffenen ein und berührt auf empfindliche Weise die Informationsfreiheit und den Schutz besonderer Vertrauensverhältnisse (z.B. Arztgeheimnis, anwaltliches Vertrauensverhältnis)." Die mit einer Vorratsspeicherung von Telekommunikationsdaten verbundene „Gefahr der Sammlung, Verwertung und Weitergabe der Informationen zu anderen Zwecken"[502] nimmt mit der zunehmenden Verlagerung des Lebens in die Welt der neuen Medien[503] weiter zu. In

493 L/D3-Lisken, C 26.

494 Albrecht, Die vergessene Freiheit, 137 f.

495 Albrecht, Die vergessene Freiheit, 137 f.

496 Krempl, Stefan: Die totale Informationsüberwachung, die Demokratie und die Hacker, Telepolis, Heise-Verlag, 28.12.2002, www.heise.de/tp/deutsch/inhalt/te/13870/1.html.

497 Krempl, Stefan: Die totale Informationsüberwachung, die Demokratie und die Hacker, Telepolis, Heise-Verlag, 28.12.2002, www.heise.de/tp/deutsch/inhalt/te/13870/1.html.

498 Kronqvist, Stefan (Leiter der IT-Kriminalitätsgruppe der nationalen schwedischen Strafverfolgungsbehörde): Submission to the European Commission for the Public Hearing on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, europa.eu.int/ISPO/eif/InternetPoliciesSite/-Crime/PublicHearingPresentations/Kronqvist.html.

499 Artikel-29-Gruppe der EU, Anonymität, 5.

500 Weichert, Bekämpfung von Internet-Kriminalität (I), Punkt 5; ders., BigBrotherAward 2002; vgl. auch LINX, User Privacy (I), Punkt 1 für das Internet.

501 DSB-Konferenz, Datenschutzbeauftragte des Bundes und der Länder: Eingriffsbefugnisse zur Strafverfolgung im Informations- und Telekommunikationsbereich, Entschließung der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22./23.10.1996, BT-Drs. 13/7500, 200.

502 BVerfGE 85, 386 (399).

503 Ruhmann/Schulzki-Haddouti, Abhör-Dschungel (I); Artikel-29-Gruppe der EU, Anonymität, 5.

Zukunft wird möglicherweise in jedes Kleidungsstück ein mittels Telekommunikation vernetzter Computer eingebaut sein („Ubiquitous Computing").

Das Ausmaß der Gefahr eines staatlichen Missbrauchs von Kommunikationsdaten hängt von der Ausgestaltung der Vorratsspeicherung ab. Besonders wenn sämtliche Kommunikationsdaten in einer zentralen, staatlichen Datenbank gespeichert würden, wäre der staatliche Zugriff auf sie kaum kontrollierbar, so dass dem Missbrauch Tür und Tor geöffnet wäre. Aber auch wenn den Eingriffsbehörden die Möglichkeit eines automatischen Online-Zugriffs auf Kommunikationsdaten-Datenbanken von privaten Telekommunikationsunternehmen eingeräumt würde, bestünde eine erhebliche Missbrauchsgefahr.

Die britischen Eingriffsbehörden forderten bereits im Jahr 2000 die Einrichtung eines zentralen „Datawarehouse", in dem sämtliche britischen Kommunikationsdaten gespeichert werden sollten, um den Behörden das zeitgleiche Durchsuchen und Analysieren des gesamten Datenbestands zu ermöglichen[504]. Bei Einrichtung eines derartigen Datawarehouse in Deutschland würde selbst die geringe Missbrauchskontrolle entfallen, die durch die derzeit noch notwendige Einschaltung der Telekommunikationsunternehmen gewährleistet ist. Bisher müssen Telekommunikationsunternehmen schriftlich um Auskunft ersucht werden, so dass sie immerhin regelmäßig einige formelle Voraussetzungen überprüfen werden, etwa ob ein Ersuchen von einer zuständigen Stelle gestellt wurde. Ein automatisiertes Abrufverfahren würde dagegen die mit schriftlichen Auskunftsersuchen verbundenen Verfahrensschritte und den damit einher gehenden Arbeitsaufwand überflüssig machen, der bisher als faktische Begrenzung der Inanspruchnahme dieser Befugnisse wirkt.

Die moderne Technik erleichtert die Gewinnung vielfältiger Informationen anhand von Telekommunikationsdaten ungemein. Systeme der Firma Harlequin etwa ermöglichen es, automatisch Kommunikationsprofile auf der Basis von Telefon-Verbindungsdaten erstellen zu lassen, um Freundschaftsnetzwerke darzustellen[505]. Solche Software wird etwa in Großbritannien routinemäßig von allen Sicherheitsbehörden verwendet[506]. Mit etwas Mühe lässt sich das soziale Umfeld einer Person auch ohne diese Software identifizieren. Erforderlich ist nur eine Zugriffsmöglichkeit auf Verkehrs- und Bestandsdaten, wie sie schon heute in Deutschland gegeben ist. Mit Hilfe von Computern ist es auch ein Leichtes, anhand von Telekommunikationsdaten allgemein nach „abnormalem" Kommunikationsverhalten Ausschau zu halten. Mit Hilfe einer Analyse von Kommunikationsdaten sind sogar automatisierte Vorhersagen von Verhaltensweisen durchführbar[507].

Die abstrakten Bezeichnungen für die verschiedenen Arten von Kommunikationsdaten wie „Ursprung und Ziel einer Kommunikation" sind insoweit irreführend, als sie die Daten als harmlos erscheinen lassen. Die tatsächlichen Verwendungsmöglichkeiten von Kommunikationsdaten sind heutzutage jedoch enorm, gerade angesichts der moderner „Informationstechnologie eigenen Verarbeitungsmöglichkeiten und Verknüpfungsmöglichkeiten"[508]. Im Vergleich zu 1983 ist es heute ungleich leichter, verschiedene Informationen zu einem „weitgehend vollständigen Persönlichkeitsbild"[509] zusammen zu fügen. Gerade Telekommunikationsdaten ermöglichen die Gewinnung mannigfaltiger Informationen über Menschen bis hin zur Bildung von Persönlichkeitsprofilen[510]. Im Vergleich zu Telekommunikationsdaten gibt es wohl keine andere Methode, die auf ähnlich billige und bequeme Weise die Erforschung der privaten, geschäftlichen und öffentlichen Beziehungen einer Person ermöglicht[511].

Anhand von Kommunikationsdaten lassen sich etwa Fragen der folgenden Art beantworten: Hat eine Person bestimmte Beratungsgespräche per Telefon geführt? Hat sie bei muslimischen Vereinigungen angerufen oder deren Internetseiten betrachtet? Welche Personen surfen überdurchschnittlich oft auf afghanischen Webseiten? Wer benutzt oft die „Online-Banking"-Funktion von schweizer oder liechtensteiner Banken? Hat eine Person an Internet-Foren von Globalisierungskritikern teilgenommen? Wer erhält regelmäßig E-Mails von palästinensischen Menschenrechtsorganisationen? Die Beispiele machen deutlich, welchen Sprengstoff für eine Demokratie der staatliche Zugriff auf Kommunikationsdaten darstellt.

504 NCIS Submission (I), Punkt 6.6.5.
505 Omega Foundation, Working document (I), 10.
506 NCIS Submission (I), Punkt 2.1.5.
507 DSB-Konferenz, Datenschutzbeauftragte des Bundes und der Länder: Data Warehouse, Data Mining und Datenschutz, Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15.03.2000, BT-Drs. 14/5555, 232.
508 BVerfGE 65, 1 (45).
509 BVerfGE 65, 1 (42).
510 Bundesregierung, BT-Drs. 14/9801, 14 (15); Schaar, Datenschutz im Internet, 3.
511 Welp, TKÜV, 3 (9).

Was Staaten mit Informationen der genannten Art anfangen können, zeigt ein Bericht über die Möglichkeiten des Einsatzes von „Technologien zur politischen Kontrolle“, den das Europäische Parlament erstellen ließ[512]. Der Bericht führt aus, dass ein Großteil moderner Überwachungstechnologie in Teilen der Welt eingesetzt wird, um die Aktivitäten von Dissidenten, Menschenrechtsaktivisten, Journalisten, Studentenführern, Minderheiten, Gewerkschaftsführern und politischen Gegenspielern zu überwachen[513]. Selbst der britische Geheimdienst GCHQ soll Organisationen wie Amnesty International und Christian Aid überwachen[514].

Die Möglichkeit von Missbräuchen staatlicher Befugnisse darf man in Anbetracht weitgehend fehlender Kontrollmöglichkeiten auch in Deutschland nicht unterschätzen. Dies lehrt bereits die geschichtliche Erfahrung. Bezeichnenderweise erwogen bereits die Verfasser des Grundgesetzes, in dem späteren Art. 10 GG eine Telekommunikationsüberwachung „zu Zwecken der politischen Überwachung“ ausdrücklich auszuschließen[515]. Die Erfahrung lehrt auch, dass einmal etablierte Überwachungsstrukturen im Laufe der Zeit in immer größerem Maße genutzt zu werden pflegen, auch infolge von rechtlichen Erweiterungen. Dies relativiert mögliche rechtliche Begrenzungen, die in Verbindung mit einer Vorratsspeicherung von Telekommunikationsdaten vorgesehen werden könnten.

Hinzu kommen die offiziellen Zugriffsmöglichkeiten ausländischer Staaten nach der Cybercrime-Konvention. Dieser Vereinbarung zufolge darf Deutschland anderen Vertragsstaaten den Zugriff auf hierzulande gespeicherte Kommunikationsdaten nicht verwehren, selbst wenn in diesen Staaten keine auch nur annähernd vergleichbaren Sicherungsmechanismen existieren. Davon ist angesichts der Vielzahl von Vertragsstaaten (darunter Albanien, Azerbaijan und Russland) auszugehen. Sobald ausländische Staaten Zugriff auf deutsche Kommunikationsdaten erhalten, kann von deutscher Seite nicht mehr verhindert werden, dass die Daten im Ausland in einer Weise eingesetzt werden, die in Deutschland als exzessiv und rechtswidrig anzusehen wäre. Als Beispiel für ein solches Vorgehen lässt sich anführen, dass in den USA 800 Menschen nur deshalb monatelang inhaftiert worden sein sollen, weil sie im Vorfeld des 11. September 2001 besonders viel kommuniziert haben[516]. Aussicht auf ordnungsgemäße Gerichtsverfahren hatten diese Menschen nicht[517]. Man hüte sich auch vor der leichtfertigen Aussage, in Europa sei ein solcher Vorgang nicht denkbar. Eine solche Prognose würde die Veränderlichkeit von Werten außer Betracht lassen.

In diesem Zusammenhang ist zu beachten, dass auch Interessen der Wirtschaft geeignet sind, Tendenzen zur Überwachung der Nutzung von Telekommunikationsnetzen zu bestärken. Unternehmen, die im Bereich der Telekommunikationsnetze aktiv sind, sind regelmäßig an der Gewährleistung eines geschützten Bereiches für ihre Kunden und sie selbst interessiert, in dem ungestört konsumiert werden kann. Kritische Aktivitäten im Netz können dabei etwa insoweit stören, wie Eltern ihren Kindern bestimmte Inhalte im Internet vorenthalten wollen und die Kinder deswegen insgesamt von der Nutzung des Internet ausschließen könnten, wodurch diese auch kommerzielle Angebote nicht mehr nutzen könnten. Von Seiten der Wirtschaft bestehen daher Tendenzen, Aktivitäten außerhalb des Gewöhnlichen oder sogar am Rand des Illegalen aus den Telekommunikationsnetzen zu verdrängen und nur wirtschaftlich und politisch erwünschtes Verhalten zuzulassen[518]. Dieser Gefahr muss vorgebeugt werden, und es muss stets im Auge behalten werden, dass Freiheitsbeschränkungen durch andere Interessen motiviert sein können als es öffentlich vorgetragen wird.

Staatlichen Überwachungsbefugnissen wohnt stets die Gefahr inne, gezielt gegen Personen eingesetzt zu werden, die dem Staat missliebig sind. Dass auch hierzulande gegen staatskritische Personen bislang gezielt vorgegangen wird, zeigt etwa der Fall einer bayerischen Lehrerin, die wegen ihrer „Tätigkeit in organisierten Friedensbewegungen“ Repressalien seitens ihres Dienstherrn hinzunehmen hatte[519]. Weil sie das Hauptquartier des Palästinenserpräsidenten Jassir Arafat in Ramallah besucht hatte, an einer Demonstration für „Solidarität mit Palästina“ teilgenommen hatte und Mitglied bei der globalisierungskritischen Nichtregierungsorganisation Attac war, äußerte die Regierung von Oberbay-

512 Omega Foundation, Report (I).
513 Omega Foundation, Report (I), Punkt 7.
514 Omega Foundation, Report (I).
515 AK-GG-Bizer, Art. 10, Rn. 10, Fn. 57.
516 Krempl, Stefan: Die totale Informationsüberwachung, die Demokratie und die Hacker, Telepolis, Heise-Verlag, 28.12.2002, www.heise.de/tp/deutsch/inhalt/te/13870/1.html.
517 Krempl, Stefan: Die totale Informationsüberwachung, die Demokratie und die Hacker, Telepolis, Heise-Verlag, 28.12.2002, www.heise.de/tp/deutsch/inhalt/te/13870/1.html.
518 Zur Parallele bei der Videoüberwachung Achelpöhler/Niehaus, DuD 2002, 731 (734 f.).
519 Eckert, Dirk: Ist eine Tätigkeit in der Friedensbewegung verfassungskonform?, 20.05.2002, Telepolis, Heise-Verlag, www.heise.de/tp/deutsch/inhalt/co/12578/1.html.

ern Zweifel an ihrer Verfassungstreue[520]. Derartige Zweifel hätten sich auch aus der Analyse von Telekommunikationsdaten ergeben können, etwa aufgrund bestimmter Kontakte oder eines Interesses an bestimmten Internetangeboten. Als weiteres Beispiel politischer Kontrolle ist ein Fall zu nennen, in dem – noch in den 80er Jahren – das Land Niedersachsen eine Lehrerin namens Vogt vom Dienst suspendierte, nachdem sich diese als Kandidatin für die Kommunistische Partei hatte aufstellen lassen. Erst der Europäische Gerichtshof für Menschenrechte stellte fest, dass in diesem Vorgehen ein Verstoß gegen die Meinungsfreiheit der Lehrerin (Art. 10 EMRK) lag[521]. Dass der deutsche Staat bisweilen versucht ist, in demokratisch bedenklicher Weise seine Muskeln spielen zu lassen, zeigten auch die internationalen Spitzengipfel in Salzburg und Genua im Jahre 2001. In deren Vorfeld hat man auf deutscher Seite die Befugnisse, die ursprünglich als Maßnahmen gegen Hooligans präsentiert und in das Passgesetz eingefügt worden waren, gegen Globalisierungskritiker eingesetzt[522].

Weiterhin haben die Praktiken einiger Staaten, Kommunikationsüberwachung zum Zwecke von Wirtschaftsspionage einzusetzen, traurige Berühmtheit erlangt[523]. In Großbritannien und den USA z.B. ist Wirtschaftsspionage im Ausland legal[524]. Auch im Zusammenhang mit der Ausforschung wissenschaftlicher Forschungserkenntnisse könnten Zugriffe auf Kommunikationsdaten erfolgen, die auf Vorrat gespeichert wurden.

Es existiert mithin eine Vielzahl von Fällen, in denen staatliche Eingriffsbefugnisse – gemessen an dem Standard des Grundgesetzes und der Menschenrechtskonvention – missbraucht wurden, gerade im Bereich der Telekommunikationsüberwachung und des Zugriffs auf Kommunikationsdaten. Deshalb und wegen der enormen Verwendungsmöglichkeiten von Telekommunikationsdaten sind missbräuchliche Zugriffe gerade auch auf vorratsgespeicherte Kommunikationsdaten zu erwarten.

Was die rechtlich zulässigen Verwendungsmöglichkeiten von mittels einer generellen Vorratsspeicherung erlangten Telekommunikationsdaten angeht, knüpft § 110b TKG an die bestehenden Zugriffsrechte von Strafverfolgungsbehörden an.

Zugriffsnormen wie die §§ 100g, 100h StPO dürften es ausschließen, dass Behörden „ins Blaue hinein“ auf die gespeicherten Daten zugreifen, also losgelöst vom Einzelfall den gesamten Datenbestand durchsuchen und auswerten, um überhaupt erst Anhaltspunkte für begangene oder geplante Straftaten zu gewinnen. Aufgrund der unvorstellbar großen Datenmengen könnte dabei zwangsläufig nur nach dem Muster der Rasterfahndung vorgegangen werden, indem nach bestimmten, auffälligen Merkmalen gesucht wird. Gerade diese Vorgehensweise würde der freien Kommunikation in unserer Gesellschaft großen Schaden zufügen. Jeder, dessen Kommunikationsverhalten von dem des europäischen Durchschnittsbürgers abweicht, hätte dann nämlich zu befürchten, allein wegen dieses abweichenden Verhaltens von den Behörden unter die Lupe genommen zu werden und weiteren Ermittlungen, die zwangsläufig das Risiko von Vor- und Fehlurteilen mit sich bringen, ausgesetzt zu werden.

(v) Risiko des Missbrauchs durch Private

Neben dem Risiko einer missbräuchlichen oder exzessiven Verwendung von Kommunikationsdaten durch den Staat besteht die Gefahr, dass der Staat, wo er wegen eigener Überwachungsinteressen einen effektiven Schutz personenbezogener Daten verhindert, auch Dritten den missbräuchlichen Zugriff auf diese Daten erleichtert. Beispielsweise sind die gegenwärtig nach § 110 TKG einzurichtenden Überwachungsschnittstellen Schwachstellen im Sicherheitssystem der Telekommunikationsunternehmen, weil sie den Einbruch unbefugter Personen und das unbefugte Abhören durch Mitarbeiter des Anlagenbetreibers ermöglichen[525]. Teilweise wird davon ausgegangen, dass es nur eine Frage von Monaten sei, bis diese Schnittstellen von ausländischen Geheimdiensten und der organisierten Kriminalität

520 Eckert, Dirk: Ist eine Tätigkeit in der Friedensbewegung verfassungskonform?, 20.05.2002, Telepolis, Heise-Verlag, www.heise.de/tp/deutsch/inhalt/co/12578/1.html.

521 EGMR, Vogt-D (1995), Publications A323.

522 Kaleck, Wolfgang u.a.: Stellungnahme von Bürgerrechtsorganisationen zur Anhörung des Innenausschusses des Deutschen Bundestages am 30.11.2001 zum Entwurf eines Gesetzes zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz), www.cilip.de/terror/atg-stell-281101.pdf, 6.

523 Dazu nur EP, Echelon-Bericht (I), 102 ff.; Omega Foundation, Report (I); Garstka/Dix/Walz/Sokol/Bäumler, Hintergrundpapier (I), Punkt II.

524 Schulzki-Haddouti, Christiane: Widerstände gegen Cybercrime-Abkommen aus eigenen Reihen, 09.11.2000, Telepolis, Heise-Verlag, www.heise.de/tp/deutsch/inhalt/te/4228/1.html.

525 VATM: 15 Punkte zur TKG-Novelle, 17.12.2002, www.vatm.de/images/dokumente/15_punkte_tkg.pdf: „[...] beabsichtigtes und unbeabsichtigtes Eindringen Unbefugter [wird] erleichtert mit dem Risiko schwerster Schäden an innerbetrieblicher bzw. vertraulicher Information“; AK-GG-Bizer Art. 10, Rn. 17 und 114; Garstka/Dix/Walz/Sokol/Bäumler, Hintergrundpapier (I), Punkt II; Germann, 323: wie wenn die Polizei nach einer gewaltsamen Wohnungsöffnung die Tür offen lassen würde; Weichert, Bekämpfung von Internet-Kriminalität (I); Pernice, Ina (Deutscher Industrie- und Handelskammertag) in Bundestag, Öffentliche Anhörung zum Thema Cyber-Crime/TKÜV (I), 14.

genutzt würden[526]. Im Fall der Einführung einer Vorratsspeicherung von Telekommunikations-Verbindungsdaten würde sich diese Problematik erheblich verschärfen[527]. Wegen der Sicherheitsprobleme und der Kosten für die Wirtschaft hat man in den USA auf die für die Behörden bequeme und preiswerte Schnittstellenlösung verzichtet, ohne dass dies zu erkennbaren Erfolgseinbußen geführt hätte[528].

Große Bestände von personenbezogenen Daten, wie sie eine Vorratsspeicherung von Telekommunikationsdaten zur Folge hätte, bilden stets einen Anreiz für technisch versierte Hacker[529]. Sogar deutsche Kreditinstitute, deren Anlagen in hohem Maße gesichert sein sollten, erlagen in der Vergangenheit wiederholt Angriffen von Hackern. Organisationen wie der Chaos Computer Club demonstrierten immer wieder Sicherheitslücken von Online-Banking, Telefonkarten, Geldkarten-PINs usw. Wenn selbst der Großkonzern Microsoft laufend Sicherheitsverbesserungen seiner Internet-Produkte veröffentlichen muss, weil ständig neue Sicherheitslücken bekannt werden, dann ist kaum zu erwarten, dass es hunderte von Telekommunikationsunternehmen in Deutschland verstehen werden, ihre Daten ausreichend zu sichern. Das Risiko eines unbefugten Datenzugriffs steigt allgemein mit der Anzahl von Daten speichernden Stellen. Im Fall einer Vorratsspeicherung wäre eine Vielzahl von Telekommunikationsunternehmen mit der Datenvorhaltung betraut, so dass das Missbrauchsrisiko entsprechend groß wäre. Verbände von Internet-Service-Providern warnen ausdrücklich, dass ihnen die Gewährleistung der Datensicherheit aller Wahrscheinlichkeit nach unmöglich sein würde, sollten sie zu einer generellen Vorratsspeicherung von Telekommunikationsdaten verpflichtet werden[530]. Durch Absicht oder unbeabsichtigterweise könnten gespeicherte Daten vielmehr jederzeit in falsche Hände gelangen[531].

Tatsächlich ist es in der Praxis immer wieder vorgekommen, dass wegen technischer Fehler plötzlich ganze Kundendateien einschließlich Kreditkartennummern für jedermann über das Internet abrufbar waren[532]. Sogar die Firma Microsoft, die für die Sicherheit der meisten Heimcomputer verantwortlich ist, hat in der Vergangenheit versehentlich interne Geschäftsgeheimnisse und persönliche Daten von Millionen von Kunden öffentlich zugänglich ins Internet gestellt[533]. Das Internet hat bekanntlich die Eigenschaft, dass sich alle Daten, die dort einmal verfügbar waren, beliebig oft vervielfältigen lassen, so dass Inhalte, einmal veröffentlicht, meistens nicht mehr entfernt werden können. Zu welchen Schäden die unfreiwillige Veröffentlichung von Telekommunikationsdaten führen könnte, lässt sich kaum abschätzen.

Außer durch Hacking könnten Telekommunikationsdaten auch auf dem Übertragungsweg zwischen Telekommunikationsunternehmen und Sicherheitsbehörden abgefangen werden. Schon die nach der bestehenden TKÜV in Verbindung mit der zugehörigen technischen Richtlinie geforderten Sicherheitsmechanismen entsprechen aus Sicht von Sachverständigen bei weitem nicht dem, was technisch möglich und zumutbar ist[534]. Die vorgesehenen Sicherheitsfunktionen schützten allenfalls vor Angriffsversuchen durch Unbedarfte[535]. Wie allgemein bei den hier diskutierten Missbrauchsrisiken liegt

526 Pfitzmann, Andreas in Bundestag, Öffentliche Anhörung zum Thema Cyber-Crime/TKÜV (I), 24.

527 ULD-SH, Kampagne, Hintergrund (I).

528 Schulzki-Haddouti, Internationale Abhörpolitik, 125 (130).

529 Etwa Heise Verlag: Kreditkarten-Nummern bei Online-Händler erbeutet, Meldung vom 19.05.2001, www.heise.de/-newsticker/data/em-19.05.01-000/.

530 EuroISPA, Internet Service Providers' Association (Europe) / US ISPA, Internet Service Providers' Association (U.S.A.): Position on the Impact of Data Retention Laws on the Fight against Cybercrime, 30.09.2002, www.euroispa.org/docs/020930eurousispa_dretent.pdf, 2; Bernhard Rohleder (Bitkom-Geschäftsführer) in Heise Verlag: IT-Branchenverband gegen Vorratsspeicherung von Verbindungsdaten, Meldung vom 19.08.2002, www.heise.de/-newsticker/data/hod-19.08.02-001/; Deutsche Telekom AG: Schriftliche Stellungnahme zur öffentlichen Anhörung am 09.02.2004 in Berlin zum Entwurf eines Telekommunikationsgesetzes (TKG), in Ausschussdrucksache 15(9)961, www.bitkom.org/files/documents/StN_BITKOM_TKG_Wirtschaftsausschuss_03.02.04.pdf, 150 (163): „potentiell wesentlich erhöhte Gefahr des Missbrauchs personenbezogener Daten".

531 EuroISPA, Internet Service Providers' Association (Europe) / US ISPA, Internet Service Providers' Association (U.S.A.): Position on the Impact of Data Retention Laws on the Fight against Cybercrime, 30.09.2002, www.euroispa.org/docs/020930eurousispa_dretent.pdf, 2.

532 Vgl. etwa Darstellung bei EPIC/PI, Privacy and Human Rights 2002 (I), Teil I, 79; für Deutschland etwa Heise Verlag: Versicherungsgruppe HUK-Coburg legte Kundendaten offen ins Netz, Meldung vom 06.11.2002, www.heise.de/-newsticker/data/jk-06.11.02-001/; Heise Verlag: Schwerwiegende Sicherheitsmängel bei T-Com, Meldung vom 26.07.2004, www.heise.de/newsticker/meldung/49424; für die USA Heise Verlag: Daten von mehr als acht Millionen US-Kreditkarten geklaut, Meldung vom 19.02.2003, www.heise.de/newsticker/data/jk-19.02.03-000/.

533 Heise Verlag: Microsoft mit offenem ftp-Server, Meldung vom 19.11.2002, www.heise.de/newsticker/data/ps-19.11.02-000/; Heise Verlag: Microsoft veröffentlicht unfreiwillig Kundendaten, c't 25/2002, S. 25.

534 Federrath, Schwachstelle Schnittstelle, 115 (122).

535 Federrath, Schwachstelle Schnittstelle, 115 (122).

die besondere Gefahr dieser Einbruchstelle darin, dass ein Abhören regelmäßig unbemerkt bleiben wird.

Ein Grund dafür, dass Private großen Aufwand treiben könnten, um illegal an Kommunikationsdaten zu gelangen, liegt in dem hohen kommerziellen Wert von Persönlichkeitsprofilen, die durch die Auswertung von Telekommunikationsdaten erstellt werden können[536]. Nach den Erfahrungen der Datenschutz-Aufsichtsbehörden genügen zur Erstellung eines Persönlichkeitsprofils schon die Kommunikationsdaten, die bei dem Besuch weniger Internetseiten durch eine Person anfallen[537]. Ein Online-Nutzerprofil erspart jedem Unternehmen Marketingausgaben in Höhe von ca. 100 Euro pro Kunde[538], insbesondere wegen der darin enthaltenen detaillierten Hinweise auf die Interessen, Vorlieben und Gewohnheiten einer Person, die ihre gezielte Ansprache ermöglichen. Die Kenntnis von Kommunikationsdaten ermöglicht es damit, Menschen unbemerkt in ihrem Konsumverhalten zu steuern[539].

Wegen des hohen Wertes von Kommunikationsdaten wäre die Versuchung von Telekommunikationsunternehmen groß, die äußerst aussagekräftigen und umfangreichen Kommunikationsdaten, die sie zu staatlichen Zwecken auf Vorrat speichern müssten, anderweitig zu nutzen. Ein solcher Missbrauch wäre von außen kaum feststellbar. Zurecht wird darauf hingewiesen, dass eine Vorratsspeicherung insoweit Straftaten nicht bekämpfen, sondern umgekehrt ihre Begehung begünstigt würde (vgl. §§ 206 StGB, 44, 43 BDSG)[540]. Wenn für die Daten von 10.000 Kunden nach der oben genannten Wertschätzung bis zu eine Million Euro locken, sind derartige Befürchtungen nicht aus der Luft gegriffen. Gerade bei kleineren Anbietern, die keinen Ruf zu verlieren haben oder sich wirtschaftlich am Rande der Insolvenz bewegen, wäre das Risiko eines solchen Missbrauches hoch. Schon heute gibt es immer wieder Gerüchte, wonach Internetfirmen persönliche Daten ihrer Kunden gewinnbringend weitergegeben haben sollen[541]. In den USA steht ein Mitarbeiter des Internet-Zugangsanbieters AOL im Verdacht, 92 Millionen Kundendatensätze des Unternehmens für 152.000 US$ verkauft zu haben[542].

Selbst wenn ein Unternehmen guten Willens wäre, könnte es nicht immer verhindern, dass einzelne Mitarbeiter unbefugt Daten heraus geben, wie es etwa im Rahmen der Bonusmeilen-Affäre mit den Daten von Abgeordneten des Deutschen Bundestags geschehen ist. Dieses Beispiel zeigt, dass im Fall einer Vorratsspeicherung von Telekommunikationsdaten nicht nur die Herausgabe gesamter Datenbestände etwa an Direktmarketingunternehmen zu befürchten wäre, sondern auch die – im Einzelfall ebenfalls lukrative – Erteilung einzelner Auskünfte an Presse, Wirtschaftsauskunfteien, Detektivbüros, Banken, Arbeitgeber oder sonstige interessierte Stellen[543]. Auch Mitarbeiter staatlicher Stellen missbrauchen ihre Zugriffsbefugnisse mitunter[544].

Dass Wissen eine Machtposition verleiht, weiß schon der Volksmund. Das Wissen um eine Person, etwa um ihre persönlichen Schwächen, kann zu ihrer Manipulation verwendet werden[545]. Teilweise wird sogar angenommen, dass man nahezu jeden Menschen inkriminieren kann, wenn man ihn nur lange genug unbemerkt in seinem Tun beobachten kann[546]. Das Wissen um Telekommunikationsdaten einer Person eignet sich wegen der hohen Aussagekraft der Daten in besonderem Maße zur Manipulation von Menschen.

Zu welchen Konsequenzen es führen kann, wenn Daten in die falschen Hände gelangen, zeigt in neuester Zeit der bereits erwähnte „Bonusmeilen-Skandal“. Deutsche Politiker, die mit dienstlich erworbenen Bonusmeilen Privatflüge bezahlt haben, sahen sich infolge der Veröffentlichung dieser Tatsache zum Rücktritt gezwungen. Auch infolge der „Hunzinger-Affäre“ standen plötzlich alle im Rampenlicht der Öffentlichkeit, die Beziehungen zu diesem PR-Berater hatten.

---

536 Feather, Clive, zitiert bei Loney, Matt: ISPs spell out true cost of data retention, 12.12.2002, news.zdnet.co.uk/story/-0,,t295-s2127408,00.html.

537 Bäumler, Helmut / Leutheusser-Schnarrenberger, Sabine / Tinnefeld, Marie-Theres: Grenzenlose Überwachung des Internets? Steht die freie Internetkommunikation vor dem Aus? Stellungnahme zum Gesetzesentwurf des Bundesrates vom 31. Mai 2002, www.rainer-gerling.de/aktuell/vorrat_stellungnahme.html, Punkt 1.

538 Schaar, DuD 2001, 383 (384).

539 Gridl, Datenschutz in globalen Telekommunikationssystemen, 61.

540 Bäumler, Helmut / Leutheusser-Schnarrenberger, Sabine / Tinnefeld, Marie-Theres: Grenzenlose Überwachung des Internets? Steht die freie Internetkommunikation vor dem Aus? Stellungnahme zum Gesetzesentwurf des Bundesrates vom 31. Mai 2002, www.rainer-gerling.de/aktuell/vorrat_stellungnahme.html, Punkt 1.

541 Bager/Bleich/Heidrich, c't 22/2002, 150 (150 f.).

542 Heise Verlag: AOL-Mitarbeiter wegen Verkaufs von Kundendaten verhaftet, 24.06.2004, www.heise.de/newsticker/-meldung/48542.

543 Gridl, Datenschutz in globalen Telekommunikationssystemen, 39 und 61.

544 Vgl. nur Landesbeauftragter für den Datenschutz in Baden-Württemberg, 7. Tätigkeitsbericht, LT-Drs. 9/4015, 45-49 mit Fällen von absichtlichem und fahrlässigem Datenmissbrauch bei der Polizei.

545 Buxel, DuD 2001, 579 (581).

546 Fairbrother, Peter: Defeating traffic analysis, www.apig.org.uk/fairbrother.pdf, 3.

Das Informationspotenzial der Spuren aller deutschen Telekommunikationsnutzer ist nur schwer einzuschätzen. Wer mit Herrn Hunzinger per Telefon, Fax oder E-Mail in Kontakt stand, ließe sich mit ihrer Hilfe unschwer ermitteln. Unzählige Tatsachen über das Privatleben von Prominenten könnten enthüllt werden[547]. Politiker könnten zum Rücktritt gezwungen, Amtsträger könnten erpresst werden. Informationen über das Sexualleben ließen sich mit Hilfe von Telekommunikationsdaten ebenso ausbeuten wie Hinweise auf Kontakte mit bestimmten Personen oder Ländern.

Nicht nur im öffentlichen und privaten, sondern auch im geschäftlichen Bereich bringt eine generelle Vorratsspeicherung von Telekommunikationsdaten erhebliche Gefahren mit sich[548]. Unter dem Gesichtspunkt der Wirtschaftsspionage kann es beispielsweise von großem Interesse sein, wo sich ein Vorstandsmitglied aufhält und mit welchen Firmen es Kontakte pflegt. Anfällig für Wirtschaftsspionage sind auch Verhandlungen über die Vergabe großer Aufträge. Für geschäftliche Verhandlungen ist Anonymität nach außen oft vital. Die Speicherung von Kommunikationsdaten stellt diese Anonymität in Frage. Angesichts der hohen Summen, um die es im Bereich der internationalen Wirtschaft geht, wird selbst großer Aufwand nicht gescheut werden, um an auf Vorrat gespeicherte Datenbestände zu gelangen. In dementsprechend hohem Maße wären solche Datenbestände gefährdet.

Einen effektiven Schutz vor Missbräuchen ermöglichen letztlich nur Verfahren, die es zur Speicherung von Daten von vornherein nicht kommen lassen (Datensparsamkeitsprinzip, vgl. § 3a BDSG). Eine Vorratsspeicherung von Telekommunikationsdaten würde dem Datensparsamkeitsprinzip diametral zuwider laufen. Insofern spiegelt sich bei den Plänen zur Vorratsspeicherung von Kommunikationsdaten ein allgemeiner Konflikt im Bereich der Telekommunikationsüberwachung wider. Die Konfliktlinie verläuft nicht streng zwischen den Sicherheitsbehörden einerseits und Datenschützern andererseits. Vielmehr hat sich auch im staatlichen Bereich bei nicht wenigen Personen die Ansicht durchgesetzt, dass der Aufbau einer sicheren Infrastruktur und der damit einher gehende präventive Schutz von persönlichen Daten und Geschäftsgeheimnissen Vorrang haben muss vor kurzfristigen Ermittlungsvorteilen für die Sicherheitsbehörden, die eine Schwächung der informationstechnischen Sicherheit mit sich bringen[549]. In Anbetracht dieser Tatsache hat die Politik in der Vergangenheit davon abgesehen, die Nutzung von Verschlüsselungstechnologien einzuschränken. Im Bereich der anonymen Telekommunikationsnutzung ist die Interessenlage vergleichbar[550]. Eine generelle Vorratsspeicherung von Kommunikationsdaten würde demgegenüber ein unkontrollierbares Missbrauchspotenzial begründen.

(vi) Verursachung von Hemmungen seitens der Grundrechtsträger

Wie gezeigt, müsste der Bürger im Falle einer Vorratsspeicherung seiner Telekommunikationsdaten ständig mit dem Risiko staatlicher Fehlentscheidungen oder eines staatlichen oder privaten Missbrauchs seiner Daten rechnen. Aus diesem Grund ist eine Vorratsspeicherung von Telekommunikationsdaten geeignet, die Unbefangenheit der zwischenmenschlichen Kommunikation in unserer Gesellschaft zu gefährden. Wer ständig damit rechnen muss, sein Kommunikationsverhalten könnte in Zukunft einmal gegen ihn verwendet werden, wird im Zweifel versuchen, sich möglichst unauffällig zu verhalten oder Kommunikationsvorgänge gänzlich zu unterlassen. Dies jedoch wäre unserem demokratischen Staatssystem (Art. 20 Abs. 1 GG) abträglich, das auf die aktive und unbefangene Mitwirkung der Bürger angewiesen ist[551]. Jede Demokratie lebt von der Meinungsfreude und dem Engagement der Bürger und setzt daher Furchtlosigkeit voraus[552]. Dort, wo „ein Klima der Überwachung und Bespitzelung herrscht, [kann] ein freier und offener demokratischer Prozess nicht stattfinden“[553]. Gerade eine Vorratsspeicherung von Telekommunikationsdaten wäre ein großer Schritt hin zu mehr Überwachung, weil die Überwachung über Einzelfälle hinaus auf die gesamte Telekommunikation der Gesellschaft ausgedehnt würde. Dies wäre auch für diejenigen Bürger, die sich mit den Feinheiten der

547 Königshofen, Thomas, zitiert bei Krempl, Stefan: Datenschutz ade? Telepolis, Heise-Verlag, 29.12.2001, www.heise.de/tp/deutsch/inhalt/te/11456/1.html.

548 ULD-SH, Sichere Informationsgesellschaft (I), Punkt 7a.

549 Etwa Tauss/Kelber, DuD 2001, 694 (694); vgl. auch Pfitzmann, Andreas in Bundestag, Öffentliche Anhörung zum Thema Cyber-Crime/TKÜV (I), 24.

550 Fox/Bizer, DuD 1998, 616 (616).

551 Vgl. BVerfGE 65, 1 (43); BVerfGE 100, 313 (381).

552 Limbach, Jutta: Ist die kollektive Sicherheit Feind der individuellen Freiheit? 10.05.2002, www.zeit.de/reden/-Deutsche%20Innenpolitik/200221_limbach_sicherheit. html.

553 Kutscha, Martin, zitiert bei Limbach, Jutta: Ist die kollektive Sicherheit Feind der individuellen Freiheit? 10.05.2002, www.zeit.de/reden/Deutsche%20Innenpolitik/200221_limbach_sicherheit.html; DG Research, Economic risks arising from the potenzial vulnerability of electronic commercial media to interception (I); vgl. zu Maßnahmen der Terrorismusbekämpfung auch Weichert, Terror und Informationsgesellschaft (I); Schwimmer, Anti-terrorist measures and Human Rights (I).

gesetzlichen Regelungen nicht auskennen, deutlich erkennbar, so dass ein deutlicher Einfluss auf das Kommunikationsverhalten der gesamten Gesellschaft zu befürchten ist.

In besonderem Maße gilt dies dort, wo staatlicher Missbrauch besonders nahe liegt, nämlich bei staatskritischen Organisationen, deren Aktivitäten in einer Demokratie besonders wichtig sind. Beispielsweise waren die anlässlich des letzten Deutschlandbesuches des US-Präsidenten Bush angekündigten Demonstrationen der Bundesregierung aus Gründen des „außenpolitischen Ansehens" ein Dorn im Auge. In solchen Situationen könnten Organisatoren von Demonstrationen durchaus Anlass sehen, ihre Telekommunikation einzuschränken, um einer missbräuchlichen Überwachung zu entgehen. Von jeher ein besonders legitimes Interesse an Anonymität haben Journalisten, Menschenrechtsaktivisten, Minderheitenvertreter und Oppositionelle. Dies gilt heute besonders in totalitären Staaten[554]. Aber auch westliche Staaten wie Deutschland sind, wie gezeigt[555], gegen Missbräuche bezüglich dieser Personen nicht von vornherein immun.

Um Anhaltspunkte für die Frage zu gewinnen, wie sich eine generelle Vorratsspeicherung von Kommunikationsdaten auf das Kommunikationsverhalten in Deutschland auswirken könnte, hat *Breyer* im April 2003 einen kurzen Fragenkatalog an Personen und Organisationen versandt, die aufgrund ihrer politisch teilweise brisanten Arbeit besonders sensibel auf staatliche Überwachung reagieren könnten[556].

Die Antwort der Journalistin und Autorin Christiane Schulzki-Haddouti weist darauf hin, dass die Einführung einer Vorratsspeicherung von Telekommunikationsdaten Beeinträchtigungen der Telekommunikationsnutzung mit sich bringen könnte. Frau Schulzki-Haddouti beschäftigt sich kritisch mit politischen Themen wie etwa der staatlichen Telekommunikationsüberwachung. In der Vergangenheit hat sie unter anderem Informationen über das geheime weltweite Überwachungssystem Echelon recherchiert und veröffentlicht. In Anbetracht solcher Aktivitäten lässt sich sicherlich sagen, dass Frau Schulzki-Haddouti Nachteile infolge einer Vorratsspeicherung der näheren Umstände ihrer Telekommunikation nicht ohne Grund befürchtet[557]. In ihrer Antwort auf die Fragen des Verfassers gab Frau Schulzki-Haddouti an, bereits gegenwärtig in bestimmten Angelegenheiten auf die Nutzung von Telekommunikationsnetzen zu verzichten und stattdessen auf persönliche Gespräche zurückzugreifen. Für den Fall einer generellen Vorratsspeicherung von Telekommunikationsdaten kündigte sie an, im Bereich des Internet nur noch anonym zu kommunizieren und im Übrigen nur noch unbedenkliche Aktivitäten über die Telekommunikationsnetze abzuwickeln. Teilweise würde sie auch auf die Kommunikation per Briefpost ausweichen.

Auch die Hilfsorganisation Misereor gab an, bei ihrer Telekommunikation zu berücksichtigen, welche Staaten den Telekommunikationsverkehr generell aufzeichnen, besonders, wenn es sich um sensible Themenbereiche wie die Menschenrechtsarbeit handele. Gegebenenfalls würden sensible Informationen in persönlichen direkten Gesprächen oder per Briefpost übermittelt, anstatt Telekommunikationsnetze einzusetzen.

Diese Angaben machen deutlich, dass eine Vorratsspeicherung von Telekommunikationsdaten teilweise einen Verzicht auf die Nutzung des Mediums der Telekommunikation zur Folge hätte. Dieser Verzicht könnte weder durch einen Einsatz anonymer Telekommunikation noch durch eine Nutzung alternativer Kommunikationsformen wie Briefkommunikation oder persönliche Gespräche voll ausgeglichen werden, weil diese Möglichkeiten nur in bestimmten Bereichen praktikabel sind. Letztlich würde eine Vorratsspeicherung daher die gesamtgesellschaftliche Kommunikation beeinträchtigen, was wiederum zur Einschränkung politischer Aktivitäten und damit zu gravierenden Nachteilen für unser demokratisches System führen kann.

Wenn 60% der Deutschen darauf vertrauen, dass die Polizei gespeicherte Daten absolut richtig und zuverlässig verwendet[558], handelt es sich dabei möglicherweise nur um die „schweigende Mehrheit". Zu den übrigen 40% gehören möglicherweise gerade solche Personen, die sich politisch engagieren und daher für eine funktionierende Demokratie von besonderer Bedeutung sind. Bereits wenn 40% der Bevölkerung Bedenken im Hinblick auf die korrekte Verwendung ihrer Daten durch die Polizei hätten, begründete dies eine reale Gefahr für unser freiheitliches demokratisches Gemeinwesen[559]. Im Jahr

554 Artikel-29-Gruppe der EU, Anonymität, 5.
555 Seiten 69-70.
556 Näher Breyer, Vorratsspeicherung, 235 ff.
557 Vgl. Seiten 29-30.
558 Opaschowski, DuD 2001, 678 (679).
559 Vgl. BVerfGE 65, 1 (43).

2003 waren 20% der im Rahmen einer Umfrage befragten Deutschen der Ansicht, es sei besser, vorsichtig zu sein, wenn man in Deutschland seine politische Meinung äußern wolle[560].

Auch außerhalb des öffentlichen Lebens, wo die Funktionsfähigkeit der Demokratie nicht unmittelbar bedroht ist, muss der Einzelne grundsätzlich sicher sein können, seine Grundrechte unbeschwert und frei von Überwachung oder auch nur der Möglichkeit der Überwachung wahrnehmen zu können. Der Mensch ist ein gemeinschaftsbezogenes Wesen, und der Schutz seiner Würde (Art. 1 Abs. 1 GG) verlangt ein gewisses Maß an unbeobachteter Kommunikation mit anderen Personen, beispielsweise in besonderen Notlagen. Der Schutz der Privatsphäre bildet die Grundlage der Handlungsfreiheit[561]. Nur wer sich vor Beobachtung sicher sein kann, kann ohne Druck zur Konformität und zur Anpassung an vorgegebene soziale, gesellschaftliche und moralische Standards handeln[562]. Dementsprechend stellt das Bundesverfassungsgericht in einer neueren Entscheidung – interessanterweise ohne auf die Funktionsfähigkeit der Demokratie abzustellen – allgemein fest: „Es gefährdet die Unbefangenheit der Nutzung der Telekommunikation und in der Folge die Qualität der Kommunikation einer Gesellschaft, wenn die Streubreite von Ermittlungsmaßnahmen dazu beiträgt, dass Risiken des Missbrauchs und ein Gefühl des Überwachtwerdens entstehen.“[563]

Gerade das Medium der Telekommunikation dient in besonderem Maße der Grundrechtsverwirklichung, so dass sich Überwachungsmaßnahmen in diesem Bereich besonders nachteilig auf die Kommunikation in einer Gesellschaft auswirken. Wie die folgende Aufzählung[564] zeigt, sind gerade die vielfältigen Tätigkeiten auf den „Datenautobahnen“ mindestens ebenso reichhaltig wie das „wirkliche“ Leben außerhalb von Telekommunikationsnetzen: Surfen im Web (Recht auf informationelle Selbstbestimmung, Art. 1 und 2 GG; Informationsfreiheit, Art. 5 Abs. 1 GG; Fernmeldegeheimnis, Art. 10 Abs. 1 Var. 3 GG), E-Mail-Versand und Internet-Telefonie (Fernmeldegeheimnis, Art. 10 Abs. 1 Var. 3 GG), Elektronische Presse, Chatrooms und Newsgroups (Presse- und Meinungsfreiheit, Art. 5 Abs. 1 GG), Elektronischer Handel, E-Commerce (Berufsfreiheit, Art. 12 GG), virtuelle Kunstausstellungen (Kunstfreiheit, Art. 5 Abs. 3 GG), Recherchen für wissenschaftliche Veröffentlichungen (Forschungsfreiheit, Art 5 Abs. 3 GG), elektronische Beichten (Glaubensfreiheit, Art. 4 GG), Beschwerden bei Behörden mittels E-Mail (Petitionsrecht, Art. 17 GG), virtuelle Demonstrationen (Versammlungsfreiheit, Art. 8 GG), virtuelle „Ortsvereine“ (Vereinigungs- und Koalitionsfreiheit, Art. 9 GG; Parteienprivileg, Art. 21 GG), behindertengerechte Internetangebote staatlicher Behörden (Diskriminierungsverbot, Art. 3 Abs. 3 GG).

In den Kommunikationsnetzen werden auch viele private und vertrauliche Gespräche und Tätigkeiten abgewickelt. Gerade was Kommunikationsvorgänge privaten Inhalts anbelangt, so geht die Globalisierung an engen persönlichen Beziehungen zu Familienmitgliedern oder Freunden nicht spurlos vorbei und führt zunehmend zu örtlicher Trennung. Das Bedürfnis nach der Möglichkeit, im Familien- und Freundeskreis vertrauliche Gespräche führen zu können, nimmt dabei nicht ab, sondern eher noch zu, so dass privater Telekommunikation in Zukunft zunehmende Bedeutung zukommen wird.

Was besondere Vertrauensverhältnisse zu Vertretern bestimmter Berufsgruppen angeht, so bieten die neuen Medien ideale Voraussetzungen dafür, sich schnell und anonym jemandem anvertrauen zu können, ohne Konsequenzen befürchten zu müssen. Die Bedeutung dieser Möglichkeit für Menschen in Not ist in der heutigen, von Beziehungsdesintegration geprägten Zeit noch gewachsen. Die lange Liste besonderer Vertrauensverhältnisse, in deren Rahmen sich die Beteiligten zunehmend telekommunikativer Mittel bedienen, umfasst Abgeordnete, Geistliche, Rechtsanwälte, Wirtschaftsprüfer, Steuerberater, Ärzte, Psychotherapeuten, Volksvertreter, Journalisten, aber auch Einrichtungen der Schwangerschaftsberatung und der Drogenhilfe (vgl. § 53 StPO). Damit wird das Fernmeldegeheimnis zunehmend zur Vorbedingung einer Vielzahl von Vertrauensverhältnissen und seine zunehmende Durchlöcherung zu einer Gefahr für weite Bereiche der Gesellschaft[565].

Auch über die Privatsphäre im engeren Sinne hinaus kann schließlich ein legitimes Interesse an Geheimhaltung bestehen, etwa was das eigene Vermögen angeht oder den Schutz von Geschäftsgeheimnissen[566]. Würde für die Kommunikation in all diesen Situationen nicht das Medium der Telekommunikation genutzt, so würde regelmäßig in einer Wohnung oder einem Geschäftsraum kommuniziert werden, so dass Art. 13 GG einschlägig wäre. Auch tatsächlich werden die Telekommunikationsnetze

560 Institut für Demoskopie Allensbach: Der Wert der Freiheit, Ergebnisse einer Grundlagenstudie zum Freiheitsverständnis der Deutschen, Oktober/November 2003, www.ifd-allensbach.de/pdf/akt_0406.pdf, 48.
561 Buxel, DuD 2001, 579 (581).
562 Buxel, DuD 2001, 579 (581).
563 BVerfGE 107, 299 (328).
564 Nach Schaar, Sicherheit und Freiheitsrechte (I), 2 ff.
565 Ruhmann/Schulzki-Haddouti, Abhör-Dschungel (I).
566 Ruhmann/Schulzki-Haddouti, Abhör-Dschungel (I).

regelmäßig von abgeschlossenen Räumen aus genutzt, was weiter verdeutlicht, dass die Telekommunikation einer Person oftmals dem Bereich ihrer Privatsphäre zuzuordnen ist. Schon 1983 hat die internationale Konferenz der Datenschutzbeauftragten erklärt, dass die Erfassung von Telekommunikationsdaten das Recht der Unverletzlichkeit der Wohnung berühre[567]. Auch wenn man so weit nicht gehen möchte, so ist die Schutzwürdigkeit von Telekommunikation derjenigen von Gesprächen in einer Wohnung jedenfalls vergleichbar.

Eine Vorratsspeicherung von Telekommunikationsdaten würde unterschiedslos alle Kommunikationsdaten erfassen, also auch die Umstände von Kommunikationsvorgängen mit privatem und vertraulichem Inhalt. Damit müssten sich die an solchen Kommunikationsvorgängen Beteiligten stets mit dem Gedanken tragen, dass ihre Kommunikation jederzeit nachvollzogen werden könnte und dass es zur missbräuchlichen Kenntnisnahme dieser Informationen durch Dritte kommen könnte. Es ist daher nicht unwahrscheinlich, dass eine Vorratsspeicherung von Telekommunikationsdaten zu Kommunikationsanpassungen führen würde, dass also auf die Nutzung des Mediums Telekommunikation für private oder vertrauliche Kommunikationsvorgänge teilweise verzichtet würde, ohne dass den Beteiligten immer Alternativen zur Verfügung stünden. Unerwünschte Beeinträchtigungen der gesamtgesellschaftlichen Kommunikation wären die Folge.

Angesichts der besonderen Bedeutung von Vertrauensverhältnissen hat der sächsische Verfassungsgerichtshof entschieden, dass es unzulässig sei, zum Zwecke der Gefahrenabwehr Daten über unbeteiligte Personen aus Vertrauensverhältnissen zu erheben[568]. Unbeteiligt sind Personen, bei denen nicht aufgrund tatsächlicher Anhaltspunkte anzunehmen ist, dass von ihnen eine Gefahr ausgeht oder dass sie Nachrichtenmittler eines Störers sind. Erst recht muss all dies im Bereich der Strafverfolgung gelten, die einen verfassungsrechtlich geringeren Stellenwert hat als die unmittelbare Abwehr von Gefahren[569].

Für eine Drogenberatungsstelle hat das Bundesverfassungsgericht ausdrücklich entschieden, dass der Schutz von Vertrauensverhältnissen schwerer wiege als das allgemeine Interesse an der Aufklärung von Straftaten[570]. In der Umgehung des Zeugnisverweigerungsrechts durch eine Beschlagnahmeanordnung sah es einen unverhältnismäßigen Eingriff in das Recht auf informationelle Selbstbestimmung[571]. Nur wenn im Einzelfall spezifische Anhaltspunkte dafür bestünden, dass Unterlagen zur Verfolgung besonders schwerer Straftaten benötigt werden, sei eine Beschlagnahme zulässig[572]. Diese Erwägungen des Bundesverfassungsgerichts müssen für Eingriffe in den Fernmeldeverkehr erst recht gelten, weil solche Eingriffe – im Unterschied zu einer Beschlagnahme – geheim erfolgen und daher tendenziell schwerer wiegen. Ob damit eine pauschale Erhebung von Kommunikationsdaten aus Vertrauensverhältnissen, wie sie mit einer Vorratsspeicherung verbunden wäre, zu vereinbaren ist, erscheint fragwürdig.

Wegen der Vielzahl von privilegierten Kommunikationsvorgängen, die über wechselnde Anschlüsse von Telefon, Fax, E-Mail, WWW usw. abgewickelt werden, ist es nicht möglich, solche Kommunikationsvorgänge zuverlässig von einer Vorratsspeicherung auszunehmen. Zeugnisverweigerungsberechtigte Stellen pauschal von einer Speicherung auszunehmen, könnte einerseits dazu führen, dass nicht privilegierte Kommunikationsvorgänge, etwa Privatgespräche von Rechtsanwälten (§ 53 Abs. 1 Nr. 3 StPO), die über den beruflichen Telefonanschluss geführt würden, von einer Überwachung ausgenommen wären. Andererseits wäre etwa ein Gespräch des Bruders eines Beschuldigten, das von einer öffentlichen Telefonzelle aus geführt wird, nicht geschützt.

Daraus ergibt sich, dass man bei sämtlichen Kommunikationsdaten von der Möglichkeit ausgehen muss, dass es sich um Daten über besondere Vertrauensverhältnisse handelt. Die einzige Möglichkeit eines wirksamem Schutzes von Vertrauensverhältnissen im Bereich der Telekommunikationsnetze ist daher ein generell hohes Schutzniveau. Eine generelle Vorratsspeicherung von Telekommunikationsdaten ist mit einem wirksamen Schutz von Vertrauensverhältnissen demnach nicht in Einklang zu bringen.

Die Pläne zur Einführung einer generellen Vorratsspeicherung von Telekommunikationsdaten sind auch im Zusammenhang mit anderen Bestrebungen zur Verbesserung der Sicherheit zu sehen. In der jüngeren Vergangenheit Deutschlands wurden etwa die Instrumente der Rasterfahndung, der akustischen Wohnraumüberwachung und der Ortung von Mobiltelefonen eingeführt. Einen Blick in die mögliche Zukunft erlauben die schon heute existierenden technischen Möglichkeiten: So gibt es Soft-

567 Internationale Konferenz der Datenschutzbeauftragten, Neue Medien (I).
568 SächsVerfGH, DuD 1996, 429 (439).
569 Seite 46.
570 BVerfGE 44, 353 (380).
571 BVerfGE 44, 353 (380).
572 BVerfGE 44, 353 (379).

ware, die von Überwachungskameras aufgenommene Bilder zeitgleich auswertet und bei „abnormalen Bewegungen“ Alarm schlägt[573]. Auch Bewegungen bestimmter Personen lassen sich so analysieren, dass für jede Person ein unverwechselbares Bewegungsprofil entsteht und dass Personen folglich für entsprechend eingerichtete Überwachungssysteme überall und schon von weitem an ihrem Laufstil erkennbar sind[574]. Aufnahmen, die Überwachungskameras von Gesichtern anfertigen, lassen sich unter Anwendung eines modernen biometrischen Verfahrens automatisch analysieren und mit einem Datenbestand – etwa aus Fahndungsfotos gewonnen – vergleichen. Das derartige Auffinden und Überwachen von Personen findet in Städten Großbritanniens und der USA bereits statt[575].

Stets lassen sich die aus den unterschiedlichen Quellen gewonnenen Daten mit Hilfe von Computern ohne Weiteres verknüpfen, so dass sich der Bürger insgesamt einem immer dichter werdenden Netz von Überwachungs-, Kontroll- und Überprüfungsmöglichkeiten ausgesetzt sieht[576], das ihn veranlassen kann, jedes Verhalten zu meiden, mit dem er sich verdächtig machen könnte. Auch wenn jeder einzelne Eingriff für sich genommen eine gewisse Berechtigung haben mag, so dürfen die gesellschaftlichen Auswirkungen einer insgesamt zunehmenden Überwachung der Bevölkerung nicht unbeachtet bleiben. Leider ist kaum messbar, wie sehr das unbefangene Gebrauchmachen von Grundrechten in einer Demokratie unter staatlichen Überwachungsmöglichkeiten leidet. Es spricht allerdings einiges für die Annahme, dass der Schaden für unsere demokratische Gesellschaft infolge einer zunehmenden Überwachung des Bürgers durch den graduellen Effizienzgewinn, den viele Befugniserweiterungen bestenfalls bewirken können, nicht aufgewogen werden kann. Jedenfalls muss bei der Abwägung von Sicherheit und Freiheit heutzutage besonders vorsichtig vorgegangen und jede einzelne, für sich genommen vielleicht unbedeutende Regelung in ihrer Gesamtwirkung bedacht werden[577].

(vii) Kontraproduktive Effekte

Auch die kontraproduktiven Effekte auf das Kriminalitätsniveau, die mit der insgesamt zunehmenden Ausweitung von Eingriffsbefugnissen einher gehen können, sind zu beachten[578]: Vieles spricht für die Annahme, dass die absolute Achtung der Menschenwürde einer Gemeinschaft nach innen und nach außen zu einer moralischen Anziehungs- und Überzeugungskraft verhilft[579], welche auf lange Sicht einzelne Vorteile, die durch exzessive Eingriffe erzielt werden könnten, überwiegt. Wissenschaftler haben als wichtiges Motiv von Terroristen die Erfahrung von Demütigung ausgemacht[580]. Schädliche Auswirkungen kann auch eine ausländerfeindliche Einstellung oder ein Klima des Misstrauens haben[581]. Gerade dies sucht ein Rechtsstaat zu vermeiden. Die Aufgabe rechtsstaatlicher Prinzipien ist demgegenüber geeignet, Fundamentalisten und Extremisten im In- und Ausland Auftrieb zu geben[582]. Nur der entschiedene Eintritt für Menschenrechte auch in Krisenzeiten sichert die Unterstützung der öffentlichen Meinung im In- und Ausland[583]. Die Einigkeit über die Achtung der Rechte anderer stärkt soziale Normen in der Gesellschaft und reduziert so zugleich das Maß an Kriminalität[584]. Maßnahmen staatlicher Überwachung, die diesen sozialen Zusammenhalt gefährden können, sollten daher gerade im Interesse der Sicherheit sehr genau überlegt sein.

Des Weiteren geht mit der Erweiterung staatlicher Ermittlungsbefugnisse auf dem Gebiet der Telekommunikation stets auch die verstärkte Entwicklung von Gegenmaßnahmen, insbesondere von Verschlüsselungs- und Anonymisierungstechniken einher[585]. Es ist zu erwarten, dass die Einführung einer Vorratsspeicherung von Telekommunikationsdaten über die schon bisher vorsichtigen Kreise organisierter Kriminalität hinaus auch bei Normalnutzern ein Problembewusstsein entstehen lassen würde und dass dadurch auch in diesen Kreisen verstärkt Möglichkeiten zur anonymen und verschlüs-

573 Spiegel Online: Software warnt vor Verbrechen, 01.05.2002, www.spiegel.de/wissenschaft/mensch/-0,1518,194325,00.html.

574 Spiegel Online: Übeltäter verraten sich durch ihren Gang, 05.11.2001, www.spiegel.de/wissenschaft/mensch/-0,1518,166107,00.html.

575 Achelpöhler/Niehaus, DuD 2002, 731 (734) für die Stadt Tampa in Florida.

576 DSB-Konferenz, Zehn Jahre nach dem Volkszählungsurteil (I).

577 Ähnlich schon BVerfGE 34, 238 (249); vgl. auch Weßlau, ZStW 113 (2001), 681, 691.

578 Schieder, Anti-Terrorist Measures and Human Rights (I).

579 Hassemer, Freiheitliches Strafrecht, 173.

580 Rötzer, Florian: Armut ist keine Ursache für den Terrorismus, Telepolis, Heise-Verlag, 01.08.2002, www.heise.de/tp/-deutsch/inhalt/co/13015/1.html; Limbach, Jutta: Ist die kollektive Sicherheit Feind der individuellen Freiheit? 10.05.2002, www.zeit.de/reden/Deutsche%20Innenpolitik/200221_limbach_sicherheit.html.

581 Weichert, Terror und Informationsgesellschaft (I): „So wird die Terroristenbekämpfung selbst zum Sicherheitsrisiko“.

582 Schieder, Anti-Terrorist Measures and Human Rights (I); Schwimmer, Anti-terrorist measures and Human Rights (I).

583 Schwimmer, Anti-terrorist measures and Human Rights (I).

584 Hassemer, Strafen im Rechtsstaat, 262.

585 Hamm, NJW 2001, 3100 (3101).

selten Netznutzung eingesetzt würden[586]. Beispielsweise könnten sich Firmen zu Maßnahmen des technischen Selbstschutzes genötigt sehen, wenn sie den Schutz ihrer Geschäftsgeheimnisse und Kontakte auf andere Weise nicht mehr gewährleisten können. Auf dem Gebiet der Verschlüsselung beobachten die Strafverfolgungsbehörden bereits jetzt, dass von diesen Möglichkeiten zunehmend Gebrauch gemacht wird und dass die Nutzung von Verschlüsselungstechniken mit steigendem Benutzerkomfort der verfügbaren Werkzeuge zunimmt[587]. Dasselbe wird auf dem Gebiet von Anonymisierungstechniken, deren Entwicklung sich momentan teilweise noch in den Kinderschuhen befindet, zu beobachten sein.

Wenn der Staat mit einer erweiterten Telekommunikationsüberwachung indirekt die anonyme Telekommunikation fördert, dann schneidet er sich mittelfristig selbst in Fällen größter Gefahr die Möglichkeit eines Abhörens ab. Selbst die schon bisher zulässige Telekommunikationsüberwachung in Einzelfällen würde damit unmöglich. Ähnlich wie im Falle des Volkszählungsgesetzes[588] sind zu weite Eingriffsbefugnisse daher kontraproduktiv, weil sie die Überwachung der Telekommunikation letztlich insgesamt in Frage stellen[589]. Vor dem Hintergrund, dass die Eingriffsbehörden nicht müde werden, die Bedeutung der Telekommunikationsüberwachung für die Wahrnehmung ihrer Aufgaben zu betonen[590], stimmt dies bedenklich. Im Rahmen der Verhältnismäßigkeitsprüfung ist dieser kontraproduktive Effekt negativ zu bewerten.

Eine Minderung der Effektivität bestehender Befugnisse ist auch im Hinblick auf die Kosten einer Vorratsspeicherung für die Wirtschaft abzusehen[591]: Internationale Telekommunikationskonzerne zentralisieren ihre Informationsverarbeitung schon heute zunehmend und verlagern sie beispielsweise in die USA. Dieser Trend würde durch eine Verpflichtung zu einer kostenträchtigen Vorratsspeicherung erheblich beschleunigt. Die Speicherung von Kommunikationsdaten im Ausland würde nicht nur dazu führen, dass eine nationale Pflicht zur Vorratsspeicherung leer laufen würde. Sie würde außerdem die bestehenden Zugriffsbefugnisse im Einzelfall gefährden, weil auf Kommunikationsdaten im Ausland in der Praxis nicht oder nur nach langer Zeit zugegriffen werden könnte. Dadurch kann die Einführung einer Vorratsspeicherung letztlich dazu führen, dass weniger Kommunikationsdaten verfügbar wären als zuvor.

(viii) Zwischenergebnis

Zusammenfassend ist festzuhalten, dass die Aussagekraft von Kommunikationsdaten, gemessen an ihrer Nutzbarkeit und Verwendungsmöglichkeit, äußerst hoch ist und mindestens der Aussagekraft von Kommunikationsinhalten entspricht. Zwar kann mangels einschlägiger Forschung nicht in seriöser Weise angegeben werden, mit welcher Wahrscheinlichkeit eine Vorratsspeicherung wie viele Fehlentscheidungen, Missbräuche und Mitwirkungshemmungen seitens der Bürger hervorrufen würde. Dies hindert aber nicht die Berücksichtigung dieser Faktoren, denn auch ein möglicher Nutzen einer Vorratsspeicherung ist nicht durch konkrete Daten belegt. Anhand von Erfahrungswerten, die nur den öffentlich bekannten Ausschnitt aller Fälle betreffen können, lässt sich jedenfalls sagen, dass die Gefahr von Fehlentscheidungen, Missbräuchen und Mitwirkungshemmungen infolge einer Vorratsspeicherung real und nicht nur unerheblich ist.

Fraglich ist, ob sich argumentieren lässt, dass wesentliche Nachteile für die Betroffenen nicht schon mit der Speicherung von Kommunikationsdaten, sondern erst infolge eines anschließenden staatlichen Zugriffs darauf drohten und dass diesen Nachteilen daher durch eine Beschränkung der staatlichen Zugriffsrechte hinreichend begegnet werden könne[592]. Dieser Argumentation ist entgegenzuhalten, dass Zugriffsbeschränkungen nur Nachteile infolge eines legalen Zugriffs auf Kommunikationsdaten abwenden können, etwa Nachteile infolge staatlicher Fehlurteile. Demgegenüber besteht selbst dann, wenn der Zugriff auf gespeicherte Daten verboten ist, die Gefahr von Missbräuchen der Daten von staatlicher oder privater Seite sowie das Risiko von Kommunikationsanpassungen auf Seiten der Betroffenen. Diesen für die Betroffenen und die Gesellschaft insgesamt wesentlichen Nachteilen lässt sich allein dadurch effektiv vorbeugen, dass bereits die Vorratsspeicherung von Telekommunikations-

586 Lenz, Karl-Friedrich: Stellungnahme zur Anhörung der Kommission über die Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität, europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/Comments/kf_lenz.html.

587 Zwingel (Leiter des BKA-Referates IT-Nutzung und Telekommunikationsüberwachung), Technische Überwachungsmaßnahmen aus Sicht der Polizei, 37 (42).

588 BVerfGE 65, 1 (64 und 50).

589 Bonitz, Sylvia (MdB) in Bundestag, Öffentliche Anhörung zum Thema Cyber-Crime/TKÜV (I), 47.

590 Breyer, Vorratsspeicherung, 12 f.

591 Zum Folgenden APIG, Communications Data, 26 f.

592 Ähnlich BVerfGE 100, 313 (384) für die vorbereitende Erfassung von Telekommunikation durch den BND.

daten unterbleibt. Es wäre daher unzutreffend, zu behaupten, dass den Betroffenen aufgrund einer bloßen Datenvorhaltung keine Nachteile drohten.

(gg) Zusammenfassung: Eingriffstiefe und negative Auswirkungen einer Vorratsspeicherung von Telekommunikationsdaten

Unabhängig von der Ausgestaltung einer Vorratsspeicherung von Telekommunikationsdaten im Einzelnen wäre die Beeinträchtigung der betroffenen Grundrechtsträger außerordentlich schwerwiegend. Dies ergibt sich aus folgenden Umständen:

- Nicht nur einzelne Personen, sondern grundsätzlich jeder Bürger wäre von der Aufzeichnung seines Telekommunikationsverhaltens betroffen.
- In vielen Fällen können Personen die Nutzung von Telekommunikationsnetzen nicht oder nur unter unzumutbaren Nachteilen meiden. Dementsprechend könnte im Fall einer Vorratsspeicherung von Telekommunikationsdaten einer Überwachung des eigenen Kommunikationsverhaltens oft nicht entgangen werden[593].
- Nicht nur vermutete Straftäter oder Störer oder deren vermutete Kontaktpersonen wären betroffen, sondern jeder Telekommunikationsnutzer, ohne dass er einen Grund für die Überwachung geliefert hat[594] oder in einer besonderen Nähebeziehung zu kriminellem Verhalten steht, dessentwegen die Vorratsspeicherung vorgenommen wird. Die Aufzeichnung wäre weder sachlich auf gefahrenträchtige Situationen noch zeitlich auf Sondersituationen noch auf Fälle begrenzt, in denen Anhaltspunkte für das Vorliegen oder Bevorstehen einer konkreten Straftat oder Gefahr gegeben sind.
- Jede Inanspruchnahme der Medien Festnetztelefon, Mobiltelefon, Fax, SMS, E-Mail, WWW usw. würde nach Beteiligten, Zeit, Ort usw. festgehalten, ohne dass es eine Eingriffsschwelle gäbe. Eine Einzelfallprüfung mit Verhältnismäßigkeitskontrolle fände nicht statt. Betroffen wären auch sämtliche Vertrauensverhältnisse und Geschäftsbeziehungen. Entsprechend der fehlenden Eingriffsschwelle würde nur ein verschwindend geringer Teil der gespeicherten Daten später tatsächlich benötigt[595]. Es würde damit im Wesentlichen keine unbeobachtete Telekommunikation mehr geben[596].
- Erfasst würden nicht etwa nur öffentlich zugängliche Daten oder Adressdaten, sondern unmittelbar die Privatsphäre betreffende Daten über das Verhalten des Einzelnen[597]. Die Aussagekraft der Daten ist extrem hoch. Eine missbräuchliche Auswertung könnte daher großen Schaden anrichten und beispielsweise zur öffentlichen Diskreditierung oder zum Verlust der beruflichen Stellung von Personen führen.
- Kommunikationsdaten würden nicht nur aus öffentlichen oder geschäftlichen Räumen erhoben. Vielmehr werden Telekommunikationsnetze von Privatpersonen regelmäßig im Schutz der eigenen Wohnung, also innerhalb ihrer räumlichen Privatsphäre, genutzt. Das Verhalten der Bürger in diesem Bereich unterliegt ansonsten nur ausnahmsweise staatlichem Zugriff (vgl. Art. 13 GG).
- Die Kommunikationsdaten würden nicht etwa als Akten, sondern in maschineller Form gespeichert. Sie können daher potenziell unbegrenzt gespeichert, abgerufen, übermittelt, vervielfältigt oder mit anderen Daten verknüpft werden.

---

593 Vgl. dazu MVVerfG, LKV 2000, 149 (156).

594 Zur rechtlichen Bewertung solcher Maßnahmen vgl. BVerfGE 100, 313 (383) zum G10: „Entgegen der Auffassung des Beschwerdeführers zu 1) folgt die Unverhältnismäßigkeit der Überwachungs- und Aufzeichnungsbefugnisse und der gesetzlich vorgesehenen Maßnahmen nicht schon aus dem Fehlen von Einschreitschwellen [...] Die unterschiedlichen Zwecke rechtfertigen es [...], daß die Eingriffsvoraussetzungen im G 10 anders bestimmt werden als im Polizei- oder Strafprozeßrecht. Als Zweck der Überwachung durch den Bundesnachrichtendienst kommt wegen der Gesetzgebungskompetenz des Bundes aus Art. 73 Nr. 1 GG nur die Auslandsaufklärung im Hinblick auf bestimmte außen- und sicherheitspolitisch relevante Gefahrenlagen in Betracht“; SächsVerfGH, DuD 1996, 429 (432): Generell gegen unbeteiligte Dritte mit informationellen Eingriffsmaßnahmen vorzugehen, wäre mit dem freiheitlichen Menschenbild der Verfassung unvereinbar; L/D3-Lisken, C 40: Heimliche Vorfeldbefugnisse sind nur den Ämtern für Verfassungsschutz gestattet; ders., C 31: Inanspruchgenommene Nichtbeteiligte müssen ansonsten in irgendeiner besonderen Nähe zu der polizeilichen Situation stehen; L/D3-Rachor, F 182: Vorfeldbefugnisse heben das Verhältnismäßigkeitsprinzip aus den Angeln; L/D3-Bäumler, J 546: Die Verarbeitung von Daten über Nichtverdächtige oder Nichtbeteiligte ist unzulässig; ders., J 607 und 671: Zu repressiven Zwecken dürfen Daten nur über Verdächtige gespeichert werden; Albers, ZRP 1990, 147 (149): Nichtstörer dürfen jedenfalls nicht in gleichem Maße in Anspruch genommen werden wie Störer.

595 Vgl. dazu BVerfGE 109, 279 (354); MVVerfG, LKV 2000, 149 (153).

596 Vgl. Bäumler, zitiert bei Wagner, Marita: Intimsphäre - lückenlos überwacht? Telepolis, Heise-Verlag, 28.06.2002, www.heise.de/tp/deutsch/inhalt/te/12813/1.html: Der Datenschutz für Internet und Telekommunikation würde fast vollkommen ausgehebelt.

597 Vgl. dazu L/D3-Bäumler, J 742: In aller Regel ist die Speicherung von das Privatleben oder die Persönlichkeit betreffenden Daten über Personen, die weder Verdächtige noch Störer sind oder waren, unverhältnismäßig.

- Kommunikationsdaten würden bei einer Vielzahl verschiedener Unternehmen dezentral gespeichert werden und zwar in vielen Fällen auf Datenverarbeitungsanlagen, die mit Telekommunikationsnetzen verbunden wären. Beides erhöht die Gefahr, dass missbräuchlich auf gespeicherte Kommunikationsdaten zugegriffen wird.
- Kommunikationsdaten würden nicht anonym oder nur zur statistischen Nutzung gespeichert, sondern sie wären dazu bestimmt, für den Verwaltungsvollzug eingesetzt zu werden. Ihre Speicherung und staatliche Verwendung könnte daher einschneidende Folgen für die Betroffenen haben, bis hin zum lebenslänglichen Freiheitsentzug, unter Umständen auch zuunrecht aufgrund eines falschen Verdachts.
- Die Daten würden nicht offen erhoben, sondern im Geheimen. Dadurch könnten die Betroffenen keine rechtzeitige Überprüfung der Richtigkeit der Daten oder der Rechtmäßigkeit des Zugriffs veranlassen[598]. Eine Überprüfung der Richtigkeit der Daten ist den Betroffenen angesichts der enormen Datenmassen realistischerweise ohnehin nicht möglich.
- Die Daten würden nicht etwa durch die Betroffenen persönlich angegeben, sondern unabhängig von deren Willen und deren Kenntnis automatisch aufgezeichnet und gegebenenfalls an Behörden weiter übermittelt.
- Im Gegensatz zu bisher bekannten Maßnahmen würden nicht nur ursprünglich zu einem anderen Zweck erfasste Daten auf Vorrat gespeichert, bei denen wegen eines früheren Verfahrens eine erhöhte Wahrscheinlichkeit besteht, dass sie in Zukunft erneut benötigt werden. Vielmehr erfolgt bei einer Vorratsspeicherung von Kommunikationsdaten bereits die Erhebung ohne konkreten Anlass[599]. Der Bürger würde also rein vorsorglich überwacht[600].
- Den zuständigen Behörden entstünden durch Zugriffe auf die gespeicherten Daten kaum Kosten, und es wäre kaum Personal nötig. Damit entfallen faktische Begrenzungen der Eingriffshäufigkeit, die bei traditionellen Befugnissen stets bestanden[601].
- Mit der Einführung einer Vorratsspeicherung von Telekommunikationsdaten sind gravierende Änderungen und Einschränkungen des Kommunikationsverhaltens zu befürchten, besonders auf Seiten regierungskritischer Personen, deren Aktivitäten in einer Demokratie besonders wichtig sind.
- Es würde zu Gegenmaßnahmen auf Seiten der Telekommunikationsnutzer und der Telekommunikationsunternehmen kommen. Dadurch könnten Maßnahmen der Telekommunikationsüberwachung selbst bei Vorliegen eines konkreten Verdachts unmöglich werden.
- Soweit den Behörden im Hinblick auf Bestandsdaten ein Online-Zugriff auf die Datenbestände eingeräumt wurde, fällt auch die faktische Begrenzung der Anzahl von Eingriffen durch den bürokratischen, mit Anfragen verbundenen Aufwand weg. Zugriffe bleiben selbst vor den Telekommunikationsunternehmen geheim, was eine Rechtmäßigkeitskontrolle durch diese ausschließt. Außerdem bieten diese Schnittstellen eine große Angriffsfläche für Hacker.
- Die Zugriffsnormen schließen eine Durchsuchung ganzer Datenbestände nach bestimmten Merkmalen, um Verdachtsmomente überhaupt erst zu gewinnen (ähnlich dem Verfahren der Rasterfahndung), nicht aus. Unter Umständen ist damit die Erstellung von Bewegungsbildern, Interessenprofilen, die Abbildung sozialer Beziehungen und die Erstellung weitgehend vollständiger Persönlichkeitsabbilder zulässig.
- Weil nicht nur Individualkommunikation, sondern auch der Abruf öffentlich zugänglicher Informationen über Telekommunikationsnetze – insbesondere das Internet – aufgezeichnet wird, lassen sich auch das Informationsverhalten und die Interessen einzelner Personen und der Bevölkerung insgesamt in weitem Umfang überwachen und auswerten. Hierzu benötigt der Staat zwar neben den vorratsgespeicherten Protokollen der Internet-Zugangsanbieter auch die Zugriffsprotokolle der Internet-Inhalteanbieter. Letztere werden aber verbreitet auf freiwilliger Basis erstellt und können von Behörden im Wege der Beschlagnahme oder im Wege der nachrichtendienstlichen Zugriffsbefugnisse erlangt werden.
- Da Rechtshilfeabkommen und die Cybercrime-Konvention auch ausländischen Staaten Zugriff auf die Datenbestände eröffnen, ist nicht gewährleistet, dass der Zugriff auf die Daten und die Nut-

598 Vgl. dazu SächsVerfGH, JZ 1996, 957 (963).
599 Vgl. zu dieser Unterscheidung L/D3-Bäumler, J 537 f.
600 DSB-Konferenz, Vorratsspeicherung (I).
601 Vgl. dazu Albrecht/Arnold/Demko/Braun, Rechtswirklichkeit und Effizienz der Telekommunikationsüberwachung, 192, wonach das das Ausmaß an Telefonüberwachung fiskalisch weit mehr begrenzt wird als durch das Gesetz.

zung der Daten durch den ausländischen Staat unter denselben grundrechtssichernden Bedingungen erfolgen wie sie in Deutschland bestehen.

(hh) Ergebnis

Wie gezeigt, lassen sich sowohl die positiven wie auch die negativen Auswirkungen, die eine Vorratsspeicherung von Telekommunikationsdaten hätte, auf der Basis der gegenwärtigen Erkenntnisse nicht sicher beurteilen. Auch ohne die experimentelle Einführung einer solchen Regelung ließen sich die maßgeblichen Tatsachen aber durch Auswertungen und Untersuchungen in vielerlei Hinsicht klären[602]. Weil eine Vorratsspeicherung von Telekommunikationsdaten zu schweren und irreparablen Einbußen auf Seiten der Betroffenen führen könnte, ist der Gesetzgeber grundsätzlich verpflichtet, die ihm zugänglichen Erkenntnisquellen vor Einführung einer Vorratsspeicherung auszuschöpfen[603].

Dies hat der Gesetzgeber in keiner Weise getan. Die dem Bundestag im Jahre 2005 vorgelegte Untersuchung des Bundeskriminalamts ist weder wissenschaftlich noch unabhängig erfolgt. Sie beschränkte sich vornherein darauf, Einzelfälle aufzuzeigen, in denen das Fehlen von Kommunikationsdaten Ermittlungsansätze vereitelt hat. Demgegenüber untersucht sie in keiner Weise den tatsächlichen Nutzen einer Vorratsdatenspeicherung im Vergleich zur bisherigen Rechtslage und erst recht nicht ihre negativen Folgen.

Mangels Klärung der für die Beurteilung der Angemessenheit maßgeblichen Tatsachen wäre die Einführung einer Vorratsspeicherung von Telekommunikationsdaten nur zulässig, wenn sie ausnahmsweise zum Schutz vor hinreichend wahrscheinlichen Gefahren für wichtige Rechtsgüter erforderlich wäre und die beeinträchtigten Rechtsgüter dahinter zurücktreten müssen[604]. Wie dargelegt, wäre ein erweiterter Zugriff auf Telekommunikationsdaten vorwiegend im Rahmen der Strafverfolgung von Nutzen. Im Gegensatz zur Netzkriminalität betreffen die allgemeinen Kriminalitätsrisiken auch höchstwertige Rechtsgüter. Die allgemeine Eignung einer Grundrechtsbeschränkung zur Erleichterung der Strafverfolgung kann jedoch noch nicht genügen, um eine besondere Dringlichkeit zu begründen, die ein sofortiges Handeln erforderlich macht. Gegen eine besondere Dringlichkeit einer Vorratsspeicherung von Telekommunikationsdaten spricht auch, dass der Gesetzgeber die Einführung einer Vorratsspeicherung über lange Zeit abgelehnt hat. Zudem lässt eine generelle Kommunikationsdatenspeicherung den Schutz von Rechtsgütern nur in wenigen und regelmäßig wenig bedeutenden Einzelfällen erwarten. Sie kann sogar in erheblichem Maße kontraproduktiv wirken.

Die Einführung einer Vorratsspeicherung von Telekommunikationsdaten ohne vorheriges Ausschöpfen der verfügbaren Erkenntnisquellen kann daher nicht als ausnahmsweise zum Schutz wichtiger Rechtsgüter erforderlich angesehen werden. Erst recht nicht müssen die beeinträchtigten Rechtspositionen hinter das Vollzugsinteresse zurücktreten, da eine Vorratsspeicherung unabsehbar große Schäden für die betroffenen Grundrechtsträger und für die gesellschaftliche Kommunikation insgesamt befürchten lässt. Angesichts dessen ist den Betroffenen die experimentelle Einführung einer Vorratsspeicherung unzumutbar. Der Gesetzgeber ist stattdessen verpflichtet, zunächst die ihm bereits jetzt zugänglichen Erkenntnisquellen auszuschöpfen.

Wägt man die verfassungsrechtlichen Interessen auf der Grundlage bisheriger Erkenntnisse gegeneinander ab, so ergibt sich, dass der zu erwartende Nutzen einer Vorratsspeicherung von Telekommunikationsdaten in einem deutlichen Missverhältnis zu den damit verbundenen Nachteilen für die Betroffenen und die Gesellschaft insgesamt steht[605]. Während der drohende Schaden für unser demokrati-

602 Seite 33.

603 Vgl. Seite 32.

604 Vgl. Seite 32.

605 Artikel-29-Gruppe der EU, Stellungnahme 5/2002 (I); Bäumler/v. Mutius-Bäumler, Anonymität im Internet, 8; BfD, 19. Tätigkeitsbericht, BT-Drs. 15/888, 78; BITKOM: Stellungnahme zur Gesetzesinitiative des Bundesrates vom 31.05.2002 (BR-Drs. 275/02), 12.08.2002, www.bitkom.org/files/documents/-Position_BITKOM_Vorratsdatenspeicherung_u.a._12.08.2002.pdf, 10; Covington & Burling, Memorandum (I), 3; Bundesregierung in BT-Drs. 13/4438, 39; Dix, Alexander, zitiert bei LDA Bbg.: Datenschutzbeauftragte kritisieren Entwurf für neues Telekommunikationsgesetz, 21.11.2003, www.lda.brandenburg.de/sixcms/detail.php?id=112968&-template=lda_presse; DSB-Konferenz, Vorratsspeicherung (I); DSB-Konferenz, Datenschutzbeauftragte des Bundes und der Länder: Entschließung zur systematischen verdachtslosen Datenspeicherung in der Telekommunikation und im Internet der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./25.10.2002, BT-Drs. 15/888, 199; eco, Electronic Commerce Forum e.V., Verband der deutschen Internetwirtschaft: Vorratsdatenspeicherung ist verfassungswidrig! Pressemitteilung vom 17.12.2003, www.eco.de/servlet/PB/menu/1236462_pcontent_l1/content.html; 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, Dokument Nr. T5-0452/2001; EDSB-Konferenz, Europäische Datenschutzbeauftragte: Statement at the International Conference in Cardiff (09.-11.09.2002) on mandatory systematic retention of telecommunication traffic data, BT-Drs. 15/888, 176; EDSB-Konferenz, Europäische Datenschutzbeauftragte: Statement at the International Conference in Athens (10.-11.05.2001) on the retention of traffic data by Internet Service Providers

sches Gemeinwesen unabsehbar groß wäre, ist der zu erwartende Zusatznutzen einer Vorratsspeicherung von Telekommunikationsdaten insgesamt gering. Eine Vorratsspeicherung von Telekommunikationsdaten lässt den Schutz von Rechtsgütern nur in wenigen und regelmäßig wenig bedeutenden Einzelfällen erwarten, ohne dass mit einem dauerhaften, negativen Einfluss auf das Kriminalitätsniveau zu rechnen wäre. Etwas anderes lässt sich auf der Grundlage der gegenwärtigen Erkenntnisse nicht vertretbar annehmen, so dass der Gesetzgeber seinen Beurteilungsspielraum in verfassungswidriger Weise überschreiten würde, wenn er eine Vorratsspeicherung von Telekommunikationsdaten gleichwohl anordnete. Dass nähere Untersuchungen der maßgeblichen Tatsachen an diesem Ergebnis etwas ändern könnten, ist nicht zu erwarten.

(e) Angemessenheit eines Vorratsspeicherungsrechts für Telekommunikationsunternehmen

Soweit § 150 Abs. 11a TKG Internet-Telekommunikationsunternehmen vorläufig lediglich zur Vorratsspeicherung von Kommunikationsdaten berechtigt, ist festzuhalten, dass eine solche Regelung für die betroffenen Bürger im Vergleich zu einer Vorratsspeicherungspflicht zwar weniger belastend ist, wenn insgesamt weniger Kommunikationsdaten gespeichert werden. Dem stehen aber erhebliche Nachteile entgegen, insbesondere Effektivitätseinbußen bei der Arbeit der Sicherheitsbehörden. Die Abwägungsentscheidung kann daher im Ergebnis nicht anders ausfallen als hinsichtlich einer obligatorischen Vorratsspeicherung. Demnach ist § 110a TKG auch im Bereich von Internetdiensten mit Art. 10 Abs. 1 Var. 3 GG oder, soweit das Fernmeldegeheimnis nicht einschlägig ist, Art. 2 Abs. 1, 1 Abs. 1 GG unvereinbar.

Vor allem liegt es auf der Hand, dass ein System teilweiser Datenvorratshaltung dem Gebot gleichmäßiger Strafverfolgung gravierend zuwider läuft. Während einige Kleinkriminelle, die auf die Verdeckung ihrer Spuren keinen Wert legen, auf diese Weise überführt werden könnten, wächst die Wahrscheinlichkeit, dass anonyme Dienste eingesetzt werden, mit dem Ausmaß an Gefahr, das von einer Person ausgeht. Damit aber ist eine freiwillige Datenspeicherung zum Schutz von Rechtsgütern noch weniger geeignet als eine obligatorischen Vorratsspeicherung. Ist diese Eignung bereits bei einer obligatorischen Vorratsspeicherung so gering, dass sie Eingriffe nicht rechtfertigen kann[606], dann gilt dies erst recht in Bezug auf eine teilweise Vorratsspeicherung.

(ISP's), BT-Drs. 15/888, 178; EDSB-Konferenz, Europäische Datenschutzbeauftragte: Statement at the International Conference in Stockholm (06.-07.04.2000) on the retention of traffic data by Internet Service Providers (ISP's), BT-Drs. 14/5555, 211; GDD, Gesellschaft für Datenschutz und Datensicherung e.V.: Bundesratsinitiative zur Vorratsdatenspeicherung verstößt gegen elementare Grundsätze des Datenschutzes, Pressemitteilung vom 05.06.2002, www.rainer-gerling.de/aktuell/vorrat.html; Krader, DuD 2001, 344 (347); Kugelmann, DuD 2001, 215 (220); Queen Mary (University of London), Studie über Netzkriminalität (I): „arguable"; Schaar, Forderungen an Politik und Gesetzgebung (I); Schaar, zitiert bei Hänel, Oberster Datenschützer kritisiert TKG-Novelle (I); Schaar, Retention (I), 4; Uhe/Herrmann, Überwachung im Internet (I), 164 m.w.N.; Unabhängiges Landeszentrum für den Datenschutz Schleswig-Holstein, Tätigkeitsbericht 2002, LT-Drs. 15/1700, 112; ULD-SH, Sichere Informationsgesellschaft (I), Punkt 6; Vertreterin des Bundesministeriums für Wirtschaft und Arbeit für die Bundesregierung, zitiert in der Niederschrift über die Sitzung des Rechtsausschusses des Bundesrates vom 12.11.2003, 16, www.spindoktor.de/vorratsspeicherung1103.pdf; Weichert, Bekämpfung von Internet-Kriminalität (I); Weßlau, ZStW 113 (2001), 681 (703); für Bestandsdaten schon Rieß, DuD 1996, 328 (333); vgl. auch BAG, 1 ABR 21/03 vom 29.06.2004, Absatz-Nrn. 38 ff., www.bundesarbeitsgericht.de zur Unverhältnismäßigkeit einer allgemeinen Videoüberwachung und -aufzeichnung am Arbeitsplatz.

606 Seite 81.

2. Die Berufsfreiheit (Artikel 12 Abs. 1 GG)

Die §§ 110a, 110b TKG verstoßen weiterhin gegen die Berufsfreiheit aus Art. 12 Abs. 1 GG.

a) Schutzbereich

Art. 12 Abs. 1 GG gewährleistet jedem Deutschen das Recht, seinen Beruf grundsätzlich frei wählen und ausüben zu dürfen[607]. Beruf im Sinne des Art. 12 Abs. 1 GG ist jede Tätigkeit, die der Schaffung und Erhaltung einer Lebensgrundlage dient[608] oder jedenfalls auf Erwerb gerichtet ist, ohne sich in einem einmaligen Erwerbsakt zu erschöpfen[609]. Es genügt, dass eine Gewinnerzielung durch Ausübung der Tätigkeit angestrebt wird und möglich ist, ohne dass es darauf ankommt, ob im einzelnen Fall tatsächlich ein Gewinn erzielt wird[610]. Auch gesetzlich verbotene Tätigkeiten können einen Beruf darstellen[611], da ansonsten der einfache Gesetzgeber entgegen Art. 1 Abs. 3 GG die Reichweite des Schutzbereichs eines verfassungsrechtlich garantierten Grundrechts bestimmen könnte. Ob eine Tätigkeit zurecht verboten ist, etwa weil sie sozialschädlich ist, ist eine Frage der Abwägung und damit der Rechtfertigung eines Eingriffs in die Berufsfreiheit, nicht eine Frage des Schutzbereichs.

Das Erbringen von Telekommunikationsdiensten ist, wie die Vielzahl der auf diesem Gebiet tätigen Unternehmen zeigt, zur dauerhaften Erzielung von Gewinnen geeignet und kann daher als berufliche Tätigkeit ausgeübt werden[612].

b) Eingriffstatbestand

Die Berufsfreiheit schützt jedenfalls vor finalen oder unmittelbar auf eine Berufstätigkeit bezogenen Einschränkungen der freien Berufswahl und -ausübung[613]. Sie schützt aber auch vor sonstigen belastenden Maßnahmen, wenn diese einen spezifischen Bezug zu dem Beruf aufweisen (sogenannte „objektiv berufsregelnde Tendenz“) und sich auf die Berufswahl oder -ausübung auswirken[614]. Angesichts der Vielzahl staatlicher Maßnahmen mit Auswirkungen auf die Berufswahl und -ausübung kommt dem Merkmal der „berufsregelnden Tendenz“ die Funktion zu, das Grundrecht der Berufsfreiheit vor einer Ausuferung zu bewahren[615]. Rechtsnormen, die Tätigkeiten unabhängig davon regeln, ob sie berufsmäßig durchgeführt werden oder nicht, kommt jedenfalls dann eine berufsregelnde Tendenz zu, wenn die geregelten Tätigkeiten typischerweise beruflich ausgeübt werden[616]. In derartigen Fällen liegt ein deutlicher Berufsbezug vor, der eine Anwendung des Art. 12 GG erforderlich macht.

Die §§ 110a, 110b TKG greifen in die Berufsfreiheit ein. Die Speicherpflichten zielen nicht final auf eine Einschränkung der Berufsfreiheit. Sie knüpfen aber spezifisch an das Angebot von Telekommunikationsdiensten an und regeln diese Tätigkeit, indem geschäftsmäßigen Anbietern von Telekommunikationsdiensten die Speicherung von Kommunikationsdaten im Rahmen ihrer Tätigkeit aufgegeben wird. Die angestrebten Speicherpflichten sind zwar nicht unmittelbar auf die Berufstätigkeit gewerblicher Anbieter von Telekommunikationsdiensten bezogen, weil alle geschäftsmäßigen und damit auch die nicht berufsmäßigen Anbieter in Anspruch genommen werden sollen. Allerdings zeigt die praktische Erfahrung, dass geschäftsmäßige Anbieter von Telekommunikationsdiensten typischerweise zum Zweck der Gewinnerzielung handeln. Gewerbliche Angebote werden auch am häufigsten in Anspruch genommen, so dass sich eine Vorratsspeicherungspflicht schwerpunktmäßig auf kommerzielle Diensteanbieter auswirken würde. Damit weisen die §§ 110a, 110b TKG einen spezifischen Bezug zu der Tätigkeit des gewerblichen Angebots von Telekommunikationsdiensten, also eine „berufsregelnde Tendenz“, auf. Sie greifen daher jedenfalls in die Freiheit der Berufsausübung ein[617].

Fraglich ist, was außerhalb des Felds der gewerblichen Anbieter von Telekommunikationsdiensten gilt. Gemäß § 3 Nr. 10 TKG ist „geschäftsmäßiges Erbringen von Telekommunikationsdiensten“ ein nachhaltiges Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht. Diese Definition geht daher über gewerbliche Anbieter hinaus.

Soweit Telekommunikationsdienste zwar nachhaltig, aber ohne Gewinnerzielungsabsicht angeboten werden, ist zu differenzieren: Zum einen kann die Tätigkeit der Ausübung eines anderen Berufes zuzurechnen sein. Beispielsweise lassen die Inhaber mancher Gaststätten von Telefongesellschaften öffent-

607 J/P6-Jarass, Art. 12, Rn. 8 m.w.N.
608 BVerfG seit E 7, 377 (397); in neuerer Zeit etwa BVerfGE 97, 228 (252 f.).
609 BVerfGE 97, 228 (253).
610 v. Münch/Kunig-Gubelt, Art. 12, Rn. 10.
611 A.A. BVerfGE 7, 377 (397); das Merkmal der Legalität nicht mehr erwähnend BVerfGE 97, 228 (252 f.).
612 Friedrich, Verpflichtung, 165.
613 BVerfGE 22, 380 (384); BVerfGE 46, 120 (137); BVerfGE 97, 228 (254).
614 BVerfGE 22, 380 (384); BVerfGE 46, 120 (137).
615 BVerfGE 97, 228 (253 f.).
616 BVerfGE 97, 228 (254); zum mittelbaren Eingriffsbegriff vgl. schon Seite 24.
617 Ebenso BeckTKG-Ehmer, § 88, Rn. 45 zu Speicherpflichten allgemein, allerdings ohne Begründung.

liche Telefone aufstellen. In manchen Fällen sind die Gaststätteninhaber an dem Gewinn nicht beteiligt – ansonsten sind sie selbst gewerbsmäßige Anbieter von Telekommunikation –, sondern wollen das Telefon ihren Kunden lediglich als Service zur Verfügung stellen. In diesem Fall kann das Angebot eines Telefons dem Beruf des Gastwirtes zugerechnet werden, so dass Art. 12 Abs. 1 GG unter diesem Aspekt einschlägig ist. Andererseits gibt es Fälle, in denen keinerlei Gewinnerzielungsabsicht im Spiel ist, etwa wenn gemeinnützige Privatuniversitäten ihren Studenten Internet-Zugänge zur Verfügung stellen. Da das Angebot von Telekommunikationsdiensten in solchen Fällen nicht als berufliche Tätigkeit ausgeübt wird, kann ein Eingriff die Berufsfreiheit nicht geltend gemacht werden. Insoweit ist lediglich Art. 2 Abs. 1 GG einschlägig[618].

Ein Eingriff in Art. 12 Abs. 1 GG liegt somit vor, soweit gewerbsmäßige Anbieter von Telekommunikationsdiensten zu einer Vorratsspeicherung von Telekommunikationsdaten ihrer Benutzer verpflichtet werden sollen.

c) Verfassungsmäßige Rechtfertigung

Die Berufsfreiheit kann nach der Rechtsprechung des Bundesverfassungsgerichts durch Gesetz oder auf Grund eines Gesetzes eingeschränkt werden[619].

aa) Berufswahl- oder Berufsausübungsregelung

Die wichtigste Schranke dieses Gesetzesvorbehalts stellt das Verhältnismäßigkeitsprinzip dar[620]. Es ist als Berufsausübungsregelung anzusehen, wenn der Gesetzgeber Telekommunikationsdiensteanbieter zur Vorratsspeicherung von Kommunikationsdaten verpflichtet[621]. Das für Berufsausübungsregelungen aufgestellte Erfordernis, dass vernünftige Erwägungen des Gemeinwohls die Beschränkung zweckmäßig erscheinen lassen müssen[622], geht der Sache nach über das allgemeine Verhältnismäßigkeitsgebot nicht hinaus.

bb) Verhältnismäßigkeitsprüfung

Das Verhlätnismäßigkeitsgebot ist verletzt. Die Einschränkung der Berufsfreiheit durch die §§ 110a, 110b TKG ist nicht verhältnismäßig im engeren Sinne.

Das Bundesverfassungsgericht hat in einer Entscheidung ausgesprochen, dass eine unangemessene Einschränkung der Berufsausübung durch ein Gesetz nur vorliege, wenn die wirtschaftliche Existenz der Gesamtheit der betroffenen Berufsgruppe gefährdet sei[623]. Während das Abstellen auf die Gesamtheit der Berufsgruppe akzeptiert werden kann, weil Besonderheiten innerhalb einer Berufsgruppe an Art. 12 Abs. 1 GG in Verbindung mit Art. 3 Abs. 1 GG gemessen werden können, ist fraglich, ob eine unangemessene Einschränkung der freien Berufsausübung in jedem Fall eine Existenzgefährdung voraussetzt. Die allgemeine Dogmatik zum Verhältnismäßigkeitsprinzip lässt es genügen, wenn der Verlust an grundrechtlich geschützter Freiheit in einem unangemessenen Verhältnis zu den Gemeinwohlzwecken steht, denen die Grundrechtsbeschränkung dient. Wendet man diese Formel im Bereich der Berufsfreiheit an, so liegt eine unangemessene Grundrechtsbeschränkung bereits dann vor, wenn ihr keine überwiegenden Interessen des Allgemeinwohls gegenüber stehen, und nicht erst, wenn ein Berufszweig in seiner Existenz gefährdet wird. Eine abweichende Handhabung im Bereich der Berufsfreiheit könnte sich mit einem niedrigeren Stellenwert der Berufsfreiheit im Vergleich zu anderen Grundrechten rechtfertigen lassen, jedenfalls soweit nur die Freiheit der Berufsausübung betroffen ist. Zwar kann die Tatsache, dass ein Eingriff in die Freiheit der wirtschaftlichen Betätigung weniger schwer wiegen mag als ein Eingriff in andere, enger mit der menschlichen Persönlichkeit verbundene Freiheiten, im Rahmen der Abwägung Berücksichtigung finden. Allein dieser Umstand kann aber nicht genügen, um beispielsweise schwerwiegende Beeinträchtigungen der wirtschaftlichen Rentabilität eines Berufs, denen nur geringe Vorteile für das Gemeinwohl gegenüber stehen, zu rechtfertigen.

Beschränkungen der Berufsfreiheit können daher auch ohne Gefährdung der Existenz einer Berufsgruppe unverhältnismäßig sein. Maßgeblich ist – auch bei Einschränkungen der Berufsausübungsfreiheit –, ob die Grundrechtsbeschränkung durch überwiegende Allgemeininteressen gerechtfertigt ist oder nicht. Die abweichende Entscheidung des Bundesverfassungsgerichts auf dem Gebiet der Berufsfreiheit beruhte möglicherweise darauf, dass das Gericht über eine – seiner Meinung nach – in hohem Maße geeignete Maßnahme zum Schutz wichtiger Rechtsgüter zu entscheiden hatte und die angeführte Aussage daher nur in diesem Zusammenhang Geltung beansprucht.

618 Vgl. BVerfGE 97, 228 (263); Friedrich, Verpflichtung, 165.
619 J/P6-Jarass, Art. 12, Rn. 19 f. m.w.N.
620 Dazu Seite 28.
621 Ebenso für die allgemeine Pflicht zur Vorhaltung von Überwachungsvorrichtungen VG Köln, CR 2000, 747 (749).
622 Vgl. BVerfGE 7, 377 (405).
623 BVerfGE 30, 292 (325).

Bei der Prüfung der Verhältnismäßigkeit im engeren Sinne kann auf die Ausführungen zu Art. 10 Abs. 1 Var. 3 GG verwiesen werden, was den möglichen Nutzen einer Vorratsspeicherung von Telekommunikationsdaten angeht[624]. Mitunter wird behauptet, dass eine EU-weite Kommunikationsdatenspeicherung für die betroffenen Unternehmen insoweit nützlich sei, als sie vor Wettbewerbsverzerrungen durch von Mitgliedstaat zu Mitgliedstaat unterschiedliche Belastungen geschützt würden. Diese Argumentation ist abzulehnen. Im Rahmen des Art. 12 Abs. 1 GG kommt es zuallererst auf die Situation deutscher Unternehmen an. Deutsche Unternehmen sind aber im Wettbewerb bereits nicht benachteiligt, weil hierzulande bisher keine Pflicht zur Vorratsspeicherung von Telekommunikationsdaten besteht. Das Fehlen einer Kommunikationsdatenspeicherungspflicht bedeutet umgekehrt einen Vorteil deutscher Unternehmen im Wettbewerb, der durch die Richtlinie 2006/24/EG beseitigt wird. Aber auch für solche ausländische Unternehmen, die einer Vorratsspeicherungspflicht bereits unterworfen sind, wäre ein Entlastungseffekt kaum spürbar. Zunächst einmal steht die Richtlinie 2006/24/EG umfassenderen Regelungen in den Mitgliedstaaten nicht entgegen und sieht nur einen Mindeststandard vor. Ihre Umsetzung kann daher nicht verhindern, dass es auch weiterhin erhebliche Wettbewerbsverzerrungen innerhalb der EU gäbe. Die verbleibende Entlastung bereits betroffener Unternehmen wird dadurch relativiert, dass der Kostenvorteil außereuropäischer Unternehmen, die einer Pflicht zur Vorratsspeicherung nicht unterliegen, in jedem Fall bestehen bleibt und die Europäische Union einen „verzerrten Wettbewerb“ von Seiten dieser Unternehmen im Zeitalter einer globalen Informationswirtschaft nicht verhindern kann. Die Entlastung einiger Unternehmen von einem „verzerrten Wettbewerb“ innerhalb der EU kann die Wettbewerbsnachteile für die durch die Richtlinie 2006/24/EG erstmals von einer Vorratsspeicherung betroffenen Unternehmen somit nicht aufwiegen, so dass von einem Nutzen für die betroffenen Unternehmen insgesamt keine Rede sein kann.

Mit welchen Belastungen der betroffenen Unternehmen eine Verpflichtung zur Vorratsspeicherung verbunden ist, lässt sich abstrakt nicht bestimmen[625]. Es kommt auf die Ausgestaltung der Regelung im Einzelnen an[626], insbesondere hinsichtlich der genauen Art der zu speichernden Daten[627]. Außerdem hängt es vom jeweiligen Geschäftsmodell eines Unternehmens ab, inwieweit die erforderlichen Einrichtungen bereits vorhanden sind oder zusätzliche Investitionen erforderlich sind[628]. Zukünftige Geschäftsmodelle können schließlich dazu führen, dass bisher verfügbare Daten nicht mehr zur Verfügung stehen werden[629]. Eine Quantifizierung der Belastungen infolge einer Kommunikationsdatenspeicherungspflicht ist daher schwierig.

(1) Speicherungskosten

Während Anbieter von Inhalten im Internet, das heißt Betreiber von Internet-Servern, regelmäßig schon über die zur Aufzeichnung von Kommunikationsdaten erforderlichen Einrichtungen verfügen, sind bei Anbietern von E-Mail und sonstiger Individualkommunikation im Internet, bei Anbietern von Internetzugängen und bei Betreibern von Internet-Verbindungsnetzen hohe Anlaufkosten zu erwarten. Da die meisten Geschäftsmodelle dieser Unternehmen keine Aufzeichnung von Internet-Kommunikationsdaten erfordern, verfügen diese Anbieter nicht über die dazu erforderlichen Geräte. Zudem ist diese Gruppe von Unternehmen in Deutschland bisher gemäß § 3 Abs. 2 TKÜV teilweise von der Pflicht zur Vorhaltung von Überwachungseinrichtungen befreit[630], so dass insoweit auch Geräte zur Inhaltsüberwachung nicht zur Verfügung stehen. Eine Pflicht zur Vorratsspeicherung aller Kommunikationsdaten würde den ständigen Einsatz spezieller Geräte durch die Anbieter erfordern, was hohe anfängliche Investitionskosten zur Folge hätte[631]. Weitere Kosten fielen für die technische Nachrüstung an, die für die Trennung von Kommunikationsdaten und Nachrichteninhalten notwendig wäre[632]. Insgesamt gesehen müssten bei vielen Unternehmen die Mehrzahl der bisher eingesetzten Geräte ausgewechselt werden[633]. Darüber hinaus kann der Kauf von Hardware-Verschlüsselungsmodulen erforderlich sein, um die unbefugte Kenntnisnahme durch Dritte zu verhindern[634]. AOL Großbritannien schätzt die anfänglichen Investitionskosten für das eigene Unternehmen

624 Seite 34 ff.
625 G8 Workshop, Workshop 1 (I).
626 Home Office (UK), Retention (I), 2.
627 G8 Workshop, Potential Consequences for Data Retention.
628 Kommission, Discussion Paper for Expert’s Meeting on Retention of Traffic Data (I); G8 Workshop, Potential Consequences for Data Retention; G8 Workshop, Workshop 1 (I); Home Office (UK), Retention (I), 5.
629 G8 Workshop, Workshop 1 (I).
630 Berliner Datenschutzbeauftragter, Bericht zum 31. Dezember 2001, LT-Drs. 15/591, 156 f..
631 APIG, Communications Data, 26.
632 Schulzki-Haddouti, Lauscher unter Beschuss, c’t 09/2001, 24 ff.
633 APIG, Communications Data, 26.
634 Schulzki-Haddouti, Lauscher unter Beschuss, c’t 09/2001, 24 ff.

auf 39 Millionen Euro[635], was – hochgerechnet auf alle britischen Internet-Access-Provider – Anlaufkosten in Höhe von etwa 160 Millionen Euro bedeuten würde. Während in den USA ein Erstattungsanspruch vorgesehen ist[636] und auch in Großbritannien der Staat einen „fairen Anteil" der Kosten zu tragen hat[637], kennen weder das geltende deutsche Recht noch die Vorschläge zur Einführung einer Vorratsspeicherung einen Erstattungsanspruch betroffener Unternehmen für anfängliche Investitionskosten. Das JVEG greift nur für Aufwendungen aufgrund einzelner Auskunftsersuchen.

Was die erforderliche Speicherkapazität angeht, so wird auf Seiten der Internetwirtschaft zwar teilweise von angeblich erforderlichen „Lagerhallen" und einem drohenden „Ersticken im Datenmüll" gesprochen[638] oder auch behauptet, dass die Speicherung solcher Datenmengen überhaupt „unmöglich" sei[639]. Davon kann aber bei Vorhandensein der erforderlichen finanziellen Mittel nicht ausgegangen werden. Allerdings wäre eine Vorratsspeicherung von Telekommunikationsdaten mit hohen Kosten verbunden. Die deutschen Provider rechnen mit Kosten von mehreren hunderttausend bis Millionen Euro pro Anbieter, wenn sie zu einer generellen Vorratsspeicherung von Kommunikationsdaten verpflichtet würden[640]. Bei größeren Unternehmen könnten sogar Kosten im mehrstelligen Millionenbereich anfallen[641]. In Großbritannien hat die Regierung die mit einer Vorratsspeicherung verbundenen Kosten auf insgesamt ca. 30 Millionen Euro geschätzt[642]. Berechnungen einzelner Unternehmen zeigen aber, dass diese Zahl allenfalls die Kosten für die bloße Datenspeicherung abdecken kann[643]. AOL Großbritannien geht allein für sein Unternehmen bereits von Speicherkosten in Höhe von 14 Millionen Euro pro Jahr aus[644].

Bei den Berechnungen der zu speichernden Datenmengen wird davon ausgegangen, dass die deutschen Internet-Provider gegenwärtig eine Datenmenge von ca. sechs Gigabit pro Sekunde transportieren und dass mindestens ein Tausendstel davon als Kommunikationsdaten gespeichert werden müsste[645]. Das entspräche 65 Gigabyte pro Tag. Auf der Basis dieser Zahlen müssten 5,8 Terabyte Kommunikationsdaten ständig gespeichert sein, wenn eine Speicherfrist von drei Monaten vorgesehen wäre, 11,6 Terabyte bei einer Frist von sechs Monaten und 24 Terabyte bei einem Jahr. In Spanien hat die „Nationale Vereinigung von Internet-Firmen" (ANEI) errechnet, dass pro Terabyte gespeicherter Daten etwa 750.000 Euro Kosten im Jahr anfallen[646]. Die anfänglich erforderlichen Anlaufinvestitionen sind darin nicht berücksichtigt. Übertragen auf die deutschen Zahlen würden dies Kosten von 4,3 Millionen Euro pro Jahr, wenn eine Speicherfrist von drei Monaten vorgesehen wäre, 8,6 Millionen

635 De Stempel, Camille (AOL), zitiert bei BBC News Online: Rethink urged over net snooping laws, BBC News Online, 19.12.2002, news.bbc.co.uk/1/hi/technology/2588213.stm.

636 Ruhmann/Schulzki-Haddouti, Abhör-Dschungel (I); ECTA, European Competitive Telecommunications Association: ECTA position on data retention in the EU, August 2002, https://www.ectaportal.com/uploads/-1412ECTAdataretentionstatement.DOC.

637 § 14 des Regulation of Investigatory Powers Act 2000, www.legislation.hmso.gov.uk/acts/acts2000/00023--b.htm#14; vgl. auch APIG, Communications Data, 24.

638 Summa, Harald (Geschäftsführer des Verbands der deutschen Internetwirtschaft eco), zitiert bei Heise Verlag: Empörung über die Datensammelwut der Bundesländer, Meldung vom 02.06.2002, www.heise.de/newsticker/data/jk-02.06.02-004/.

639 Summa, Harald (Geschäftsführer des Verbands der deutschen Internetwirtschaft eco), zitiert bei Krempl, Stefan: Widerstand gegen die neuen Enfopol-Überwachungspläne, Telepolis, Heise-Verlag, 23.05.2001, www.heise.de/tp/deutsch/-special/enfo/7709/1.html.

640 Summa, Harald (Geschäftsführer des Verbands der deutschen Internetwirtschaft eco), zitiert bei Hürter, Tobias: Der große Bruder wird größer, www.sueddeutsche.de/computer/artikel/367/367/print.htmlwww.sueddeutsche.de/computer/artikel/367/-367/print.html.

641 Summa, Harald (Geschäftsführer des Verbands der deutschen Internetwirtschaft eco), zitiert bei Heise Verlag: Empörung über die Datensammelwut der Bundesländer, Meldung vom 02.06.2002, www.heise.de/newsticker/data/jk-02.06.02-004/; Bäumler, Helmut / Leutheusser-Schnarrenberger, Sabine / Tinnefeld, Marie-Theres: Grenzenlose Überwachung des Internets? Steht die freie Internetkommunikation vor dem Aus? Stellungnahme zum Gesetzesentwurf des Bundesrates vom 31. Mai 2002, www.rainer-gerling.de/aktuell/vorrat_stellungnahme.html, Punkt 1; Wolf Osthaus (Branchenverband Bitkom), zitiert in Frankfurter Rundschau vom 04.06.2002.

642 BBC News Online: Anti-terror laws raise net privacy fears, BBC News Online, 11.11.2001, news.bbc.co.uk/2/hi/-science/nature/1647309.stm.

643 APIG, Communications Data, 24.

644 De Stempel, Camille (AOL), zitiert bei BBC News Online: Rethink urged over net snooping laws, BBC News Online, 19.12.2002, news.bbc.co.uk/1/hi/technology/2588213.stm.

645 Summa, Harald (Geschäftsführer des Verbands der deutschen Internetwirtschaft eco), zitiert bei Heise Verlag: Empörung über die Datensammelwut der Bundesländer, Meldung vom 02.06.2002, www.heise.de/newsticker/data/jk-02.06.02-004/; ders., zitiert bei Krempl, Stefan: Gläsern im Netz?, www.heise.de/ct/04/05/041/, geht inzwischen von einem Datenvolumen von 15 Gigabit pro Sekunde und einem Verkehrsdatenanteil von 5-10% aus, was einer Datenmenge von 8,1-16,2 Terabyte am Tag entspräche; Uhe/Herrmann, Überwachung im Internet (I), 123 rechnen mit 8,7 Gigabit pro Sekunde und einem Verkehrsdatenanteil von 5%, was insgesamt eine Datenmenge von 4,7 Terabyte am Tag ergäbe.

646 Streck, Ralf: Keine 12 Monate Speicherung von Verbindungsdaten, Telepolis, Heise-Verlag, 14.06.2002, www.heise.de/tp/deutsch/inhalt/te/12726/1.html.

Euro pro Jahr bei einer Frist von sechs Monaten und 17,2 Millionen Euro pro Jahr bei einer Speicherfrist von einem Jahr bedeuten.

Eigene Berechnungen zeigen, dass das tatsächliche Datenvolumen und damit die Kosten um ein Vielfaches höher sein könnten. Die durchschnittliche Größe eines mittels des HTTP-Protokolls übertragenen Objekts beträgt 15 Kilobyte[647], und pro Kommunikationsvorgang fallen Kommunikationsdaten von durchschnittlich mindestens 90 Byte an (Datum, Zeit, IP-Adresse, Operation, Pfadname), die sich auf ca. 30 Byte komprimieren lassen. Dies ergibt ein Verhältnis von etwa zwei Tausendsteln, so dass zwei Tausendstel des gesamten Datenstroms als Kommunikationsdaten gespeichert werden müssten. Die oben genannte Annahme von einem Tausendstel ist daher eher noch bescheiden. Verschiedentlich finden sich sogar Angaben, wonach Kommunikationsdaten 5% des gesamten Internetverkehrs ausmachten[648].

Auf höhere Zahlen lässt auch die folgende Rechnung schließen: Im März 2002 hat jeder Internetnutzer durchschnittlich 826 WWW-Seiten im Monat betrachtet[649]. Jede Internetseite enthält durchschnittlich weitere 14 Grafiken[650]. Deutschland hatte im Jahre 2000 etwa 24 Millionen Internetnutzer[651]. Nimmt man ein Kommunikationsdatenvolumen von 30 Byte pro Abruf an, dann würden allein durch die WWW-Nutzung in Deutschland pro Jahr 107 Terabyte an Kommunikationsdaten anfallen. Hinzu käme die Nutzung anderer Internetdienste wie File Transfer Protocol, Internet Relay Chat, Usenet und E-Mail.

Auf dem Gebiet von E-Mails lassen sich ähnliche Rechnungen anstellen. Bei jeder E-Mail fallen etwa 1,6 Kilobyte an Kommunikationsdaten an (sog. „Header“), die sich auf etwa ein Drittel ihrer Größe komprimieren lassen. In den USA werden schätzungsweise 300 Millionen E-Mails pro Tag versandt[652]. Anhand der jeweiligen Zahl von Internetnutzern[653] auf Deutschland übertragen ergäben dies etwa 50 Millionen deutscher E-Mails pro Tag. Es fielen dann etwa 25 Gigabyte pro Tag[654] und über 9 Terabyte pro Jahr allein an E-Mail-Kommunikationsdaten an. Auch insoweit handelt es sich um enorme Datenmengen.

AOL Großbritannien rechnet allein für sein Unternehmen mit einem Kommunikationsdatenvolumen von 800 Gigabyte pro Tag, was einem Speichervolumen von 292 Terabyte oder 360.000 CD-Roms pro Jahr entspricht[655]. Ob bei diesen Berechnungen eine mögliche Kompression der Daten berücksichtigt wurde, ist unklar. Über AOL werden jeden Tag 329 Millionen Internetverbindungen hergestellt und 597 Millionen E-Mails versandt[656].

In der Literatur werden die bei einer Kommunikationsdatenspeicherung vorzuhaltenden Datenmengen teilweise weit höher geschätzt. Eine Berechnung geht von 4,7 Terabyte Kommunikationsdaten pro Tag seitens der deutschen Internet-Access-Provider, 9,75 Terabyte am Tag seitens der deutschen Internet-Content-Provider und 150 Gigabyte pro Tag seitens der deutschen E-Mail-Provider aus[657]. Bei einer Speicherungsfrist von sechs Monaten müssten insgesamt 2.700 Terabyte an Daten ständig vorgehalten werden, was Kosten von 2 Milliarden Euro pro Jahr verursachen könne[658]. Dies mache 3,5% des Umsatzes der deutschen Internetwirtschaft aus[659].

Im Internetbereich ist über die gegenwärtigen Zahlen hinaus zu beachten, dass die Zahl der Internetnutzer in Deutschland durchschnittlich um ein Drittel pro Jahr steigt[660]. In Bezug auf die Zahl von

---

647 Berkeley Universität: Raw Data, How much Information Project, www.sims.berkeley.edu/research/projects/how-much-info/internet/rawdata.html.

648 Uhe/Herrmann, Überwachung im Internet (I), 123 m.w.N.; Wirtschaftsausschuss des Bundesrates in BR-Drs. 755/2/03, 37: „der Anteil der Verkehrsdaten beträgt 5 bis 10 %.“

649 Nielsen Netratings, www.nielsen-netratings.com/news.jsp?section=dat_gi.

650 Berkeley Universität: Raw Data, How much Information Project, www.sims.berkeley.edu/research/projects/how-much-info/internet/rawdata.html.

651 Eurostat, Internetnutzung (I).

652 Berkeley Universität: Email Details, How much Information Project, www.sims.berkeley.edu/research/projects/how-much-info/internet/emaildetails.html.

653 Nach NFO Infratest, Monitoring Informationswirtschaft (I), 15.

654 Uhe/Herrmann, Überwachung im Internet (I), 124 rechnen für Deutschland mit 150 Gigabyte pro Tag, allerdings ohne Berücksichtigung der Kompressionsmöglichkeit.

655 De Stempel, Camille (AOL), zitiert in BBC News Online: Rethink urged over net snooping laws, BBC News Online, 19.12.2002, news.bbc.co.uk/1/hi/technology/2588213.stm.

656 De Stempel, Camille (AOL), zitiert bei Loney, Matt: ISPs spell out true cost of data retention, 12.12.2002, news.zdnet.co.uk/story/0,,t295-s2127408,00.html.

657 Uhe/Herrmann, Überwachung im Internet (I), 123 f.

658 Uhe/Herrmann, Überwachung im Internet (I), 131.

659 Uhe/Herrmann, Überwachung im Internet (I), 131.

660 NFO Infratest, Monitoring Informationswirtschaft (I), 16.

Internetnutzungsvorgängen sind daher exponenzielle Steigerungsraten zu erwarten[661]. Gegenwärtig verdoppelt sich die Menge der über das Internet übertragenen Daten binnen eines Zeitraums von weniger als einem Jahr[662]. Auf der anderen Seite ist zu berücksichtigen, dass Speichermedien laufend leistungsfähiger und preisgünstiger werden.

Im Telefonbereich ist von erheblich geringeren Datenmengen auszugehen, die auf Vorrat gespeichert werden müssten. Bei den Telefondienstanbietern ist die für eine Aufzeichnung von Kommunikationsdaten erforderliche Hardware bereits weitgehend vorhanden, weil diese Verbindungsdaten bereits heute regelmäßig zu Abrechnungszwecken aufzeichnen (etwa Anschlussnummer, Zielnummer, Zeitpunkt und Dauer eines Anrufs). Auch hier wäre aber ein erheblicher Ausbau der vorhandenen Speicherkapazität erforderlich[663].

(2) Sonstige Kosten

Kosten in weit höherer Größenordnung als für die Speicherung fallen für die Verwaltung, Aufbereitung und Übermittlung gespeicherter Kommunikationsdaten an die Eingriffsbehörden an[664]. Es müsste etwa erst neue Software entwickelt werden, um die enormen Datenbestände zu verwalten und den Zugang zu gesuchten Daten zu gewährleisten[665]. Die Gewährleistung der Zugriffsmöglichkeit ist besonders kompliziert, wenn die Daten an verschiedenen Orten oder in verschiedenen Ländern anfallen oder gespeichert werden[666]. Sodann ist der Vorgang des Aufsuchens erwünschter und des Ausfilterns unerwünschter Daten mit erheblichem Aufwand verbunden. Vor allem fällt der höhere Personalaufwand ins Gewicht, der durch Bereitschaftsdienste, Prüfpflichten und die Datenadministration verursacht würde[667]. Eine generelle Vorratsspeicherung von Telekommunikationsdaten hätte zur Folge, dass die betroffenen Unternehmen ein Vielfaches der Kommunikationsdaten vorhalten müssten, die sie gegenwärtig speichern. Dies lässt einen entsprechenden Anstieg der Zahl von Auskunftsersuchen erwarten. Bereits bisher beschäftigt die Deutsche Telekom AG fünf Mitarbeiter allein zur Bearbeitung von Anfragen nach § 100g StPO[668]. Durch Auskünfte über Verbindungsdaten wird der Konzernetat Jahr für Jahr mit Beträgen im zweistelligen Millionenbereich belastet[669]. Hinzu kommen Aufwendungen für die Ausbildung des Personals[670].

Weitere Kosten können durch Haftungsfälle entstehen. Beispielsweise können Sanktionen für den Fall vorgesehen sein, dass Daten vorschriftswidrig nicht gespeichert oder aufbewahrt wurden. Weiterhin können Kunden das Unternehmen auf Schadensersatz verklagen, wenn es zu einem Missbrauch der bei dem Unternehmen gespeicherten Daten kommt. Unternehmensverbände argumentieren nicht zu Unrecht, dass sich solche Fälle nicht immer vermeiden lassen[671]. Selbst wenn im einzelnen Fall kein Verschulden des Unternehmens oder eines Mitarbeiters vorliegt, ist die Vorhaltung sensibler Daten eine gefahrenträchtige Tätigkeit, die notwendigerweise das Risiko von Verletzungen der Datensicherheit mit sich bringt. Es wäre falsch, dieses Risiko den Unternehmen oder, durch Haftungsbefreiung,

661 Queen Mary (University of London), Studie über Netzkriminalität (I).

662 Kommission, Sichere Informationsgesellschaft (I), 11.

663 VATM: Schriftliche Stellungnahme zur öffentlichen Anhörung am 09.02.2004 in Berlin zum Entwurf eines Telekommunikationsgesetzes (TKG), in Ausschussdrucksache 15(9)961, www.bitkom.org/files/documents/-StN_BITKOM_TKG_Wirtschaftsausschuss_03.02.04.pdf, 47 (68): die Speicherkapazitäten müssten mindestens verdoppelt werden; ebenso o2 (Germany) a.a.O., 140 (146).

664 BITKOM: Stellungnahme zur Gesetzesinitiative des Bundesrates vom 31.05.2002 (BR-Drs. 275/02), 12.08.2002, www.bitkom.org/files/documents/Position_BITKOM_Vorratsdatenspeicherung_u.a._12.08.2002.pdf, 8; NCIS Submission (I), Punkte 6.2.3 und 6.6.3; ICC/UNICE/EICTA/INTUG, Common Industry Statement on Storage of Traffic Data for Law Enforcement Purposes, 04.06.2003, www.statewatch.org/news/2003/jun/-CommonIndustryPositionondataretention.pdf, 8.

665 BITKOM: Stellungnahme zur Gesetzesinitiative des Bundesrates vom 31.05.2002 (BR-Drs. 275/02), 12.08.2002, www.bitkom.org/files/documents/Position_BITKOM_Vorratsdatenspeicherung_u.a._12.08.2002.pdf, 8; Home Office (UK), Retention (I), 2; Feather, Clive, zitiert bei Loney, Matt: ISPs spell out true cost of data retention, 12.12.2002, news.zdnet.co.uk/story/0,,t295-s2127408,00.html; ICC/UNICE/EICTA/INTUG, Common Industry Statement on Storage of Traffic Data for Law Enforcement Purposes, 04.06.2003, www.statewatch.org/news/2003/jun/-CommonIndustryPositionondataretention.pdf, 8.

666 G8 Workshop, Potential Consequences for Data Retention.

667 Schulzki-Haddouti, Lauscher unter Beschuss, c't 09/2001, 24 ff.; Home Office (UK), Retention (I), 5.

668 Königshofen, Thomas (Datenschutzbeauftragter der Deutschen Telekom AG), zitiert bei Krempl, Stefan: Datenschutz ade? Telepolis, Heise-Verlag, 29.12.2001, www.heise.de/tp/deutsch/inhalt/te/11456/1.html.

669 Königshofen, Thomas (Datenschutzbeauftragter der Deutschen Telekom AG), zitiert bei Krempl, Stefan: Datenschutz ade? Telepolis, Heise-Verlag, 29.12.2001, www.heise.de/tp/deutsch/inhalt/te/11456/1.html.

670 Home Office (UK), Retention (I), 5.

671 EuroISPA, Internet Service Providers' Association (Europe) / US ISPA, Internet Service Providers' Association (U.S.A.): Position on the Impact of Data Retention Laws on the Fight against Cybercrime, 30.09.2002, www.euroispa.org/docs/020930eurousispa_dretent.pdf, 2; Rohleder, Bernhard (Bitkom-Geschäftsführer) in Heise Verlag: IT-Branchenverband gegen Vorratsspeicherung von Verbindungsdaten, Meldung vom 19.08.2002, www.heise.de/-newsticker/data/hod-19.08.02-001/.

den Betroffenen aufzubürden. Dieses Risiko muss vielmehr der Staat tragen, wenn er im öffentlichen Interesse eine Vorratsspeicherung für geboten hält.

Es wird geschätzt, dass Überwachungskosten bereits heute bis zu 15% jeder Telefonrechnung ausmachen[672]. Im Telefonbereich ist insbesondere die Zielwahlsuche ein erheblicher Kostenfaktor, weil nach geltendem Recht für die dazu erforderliche Computerbenutzung keine Entschädigung gewährt wird[673]. Eine Zielwahlsuche wird erforderlich, wenn die Staatsanwaltschaft Auskunft darüber verlangt, wer in einem bestimmten Zeitraum einen bestimmten Anschluss angerufen hat (§ 100g Abs. 2 StPO). Die Erteilung einer solchen Auskunft ist technisch sehr aufwändig, weil sämtliche Verbindungen aller Kunden des befragten Unternehmens durchsucht werden müssen[674]. Die technischen Kosten für eine solche Suche werden auf 750 Euro pro überprüftem Tag und Anschluss beziffert[675]. Hohe Kosten entstehen auch dann, wenn die Staatsanwaltschaft darüber Auskunft verlangt, wer in einem bestimmten Zeitraum in einer bestimmten Gegend mit seinem Mobiltelefon telefoniert hat (so genannte Funkzellenabfrage, § 100h Abs. 1 S. 2 Var. 1 StPO).

Eine Reduktion der Kosten einer Vorratsspeicherung von Telekommunikationsdaten wäre möglich, wenn sämtliche Kommunikationsdaten an eine private oder öffentliche Zentralstelle zum Zweck der Erteilung von Auskünften an die Eingriffsbehörden übermittelt würden[676]. Die Vorhaltung von Personal und Einrichtungen wäre dann nur bei dieser Stelle erforderlich. Die Wirtschaft ist einer solchen Lösung zugeneigt[677]. Andererseits müssten die anfallenden Kommunikationsdaten ständig an die Zentralstelle übermittelt werden, um auch Verlangen nach Echtzeit-Übermittlung (Art. 20, 33 CCC) nachkommen zu können. Dies würde den kostensparenden Effekt mindestens dämpfen. Darüber hinaus würde die Schaffung einer solchen Zentraleinrichtung zulasten der Betroffenen gehen[678] und die Unverhältnismäßigkeit des Eingriffs in Art. 10 Abs. 1 Var. 3 GG weiter verstärken. Diese Lösung kann bei der folgenden Betrachtung daher außer Betracht bleiben. Das gleiche gilt für Ansätze, den Bedarfsträgern einen Online-Zugriff auf die Datenbanken der betroffenen Unternehmen zu eröffnen[679].

(3) Ergebnis

Fraglich ist, mit welchen Belastungen für die betroffenen Berufszweige eine Kommunikationsdatenspeicherungspflicht insgesamt verbunden wäre. Die Deutsche Telekom AG geht davon aus, dass eine Vorratsdatenspeicherungspflicht von sechs Monaten das Unternehmen im Festnetz- und Mobilfunkbereich zu Investitionen in Höhe von 180 Millionen Euro zwingen sowie jährliche Mehrkosten von weiteren 40 Millionen Euro verursachen würde[680]. Nach einer anderen Schätzung sind für jedes größere Festnetz- oder Mobilfunkunternehmen einmalige Investitionskosten in „dreistelliger Millionenhöhe“ sowie jährliche Mehrkosten von weiteren 50 Millionen Euro zu erwarten[681]. Im Internetbereich wird mit „um ein Vielfaches“ höheren Kosten als im Telefoniebereich gerechnet[682]. Konkrete Zahlen bezüglich der drohenden Gesamtkostenbelastung sind für Großbritannien verfügbar, wo es bereits konkrete Pläne zur Einführung einer Kommunikationsdatenspeicherungspflicht gibt. Bisher fallen bei den britischen Telekommunikationsunternehmen im Internet- und Telefonbereich Kosten in Höhe von etwa 14 Millionen Euro pro Jahr an, um kundenbezogene Daten zu speichern und zu verwalten[683]. Die zusätzlichen Kosten durch eine generelle Vorratsspeicherung von Telekommunikationsdaten werden im Internet-Bereich auf 60 Millionen Euro pro Jahr geschätzt[684]. Für die gesamte Telekommunikati-

672 Seeger, Martin vom Internet-Access-Provider Netuse, zitiert bei Klotz, Karlhorst: Die Polizei, dein Freund und Mixer, www.sueddeutsche.de/computer/artikel/382/6376/.

673 Etwa OLG Stuttgart, NStZ 2001, 158; OLG Köln, NStZ-RR 2001, 31.

674 Königshofen, Thomas (Datenschutzbeauftragter der Deutschen Telekom AG), zitiert bei Krempl, Stefan: Datenschutz ade? Telepolis, Heise-Verlag, 29.12.2001, www.heise.de/tp/deutsch/inhalt/te/11456/1.html.

675 Angabe bei LG Stuttgart, MMR 2001, 255 (257).

676 NCIS Submission (I), Punkt 6.2.3.

677 BMWi-Ressortarbeitsgruppe, Eckpunkte zur Anpassung der Regelungen des § 90 TKG (I), 6.

678 Seite 80.

679 Vgl. dazu NCIS Submission (I), Punkt 6.6.3.

680 Deutsche Telekom AG: Schriftliche Stellungnahme zur öffentlichen Anhörung am 09.02.2004 in Berlin zum Entwurf eines Telekommunikationsgesetzes (TKG), in Ausschussdrucksache 15(9)961, www.bitkom.org/files/documents/-StN_BITKOM_TKG_Wirtschaftsausschuss_03.02.04.pdf, 150 (163).

681 Bundesverband der Deutschen Industrie (BDI), BDI-Positionspapier zum Entwurf eines EU-Rahmenbeschlusses zur Einführung einer verbindlichen Vorratsdatenspeicherung, 07.07.2004, www.bdi-online.de/sbrecherche/-infostartpage.asp?InfoID={56A443EE-2C51-4E56-BA12-B5EEE890FEEE}, 6.

682 Bundesverband der Deutschen Industrie (BDI), BDI-Positionspapier zum Entwurf eines EU-Rahmenbeschlusses zur Einführung einer verbindlichen Vorratsdatenspeicherung, 07.07.2004, www.bdi-online.de/sbrecherche/-infostartpage.asp?InfoID={56A443EE-2C51-4E56-BA12-B5EEE890FEEE}, 6.

683 NCIS Submission (I), Punkt 6.6.4.

684 Perry, Roland (Director of Public Policy des London Internet Exchange, Linx), zitiert bei Grossman, Wendy: A new blow to our privacy, The Guardian, 06.06.2002, www.guardian.co.uk/Archive/Article/0,4273,4427430,00.html.

onsbranche ist von mehr als 150 Millionen Euro die Rede[685]. Die Kosten, die durch den Zugriff auf die Daten entstehen, sind in dieser Zahl noch nicht enthalten; insoweit ist in Großbritannien ein Entschädigungsanspruch der Unternehmen vorgesehen. Überträgt man die britische Zahl anhand der Einwohnerzahlen[686] auf Deutschland, dann ergäben sich Kosten von über 206 Millionen Euro pro Jahr[687]. Weitere indirekte Kosten können durch den Verlust an Kundenvertrauen entstehen, der zu einer generell reduzierten Inanspruchnahme von Diensten führen kann[688]. Im Internetbereich, wo bisher kaum Kommunikationsdaten gespeichert werden mussten, wird damit gerechnet, dass die Betriebskosten eines Internet-Access-Providers bei Einführung einer Kommunikationsdatenspeicherungspflicht um etwa 15-20% steigen würden[689].

In Anbetracht der schmalen Gewinnmargen in der Telekommunikationsbranche wäre eine Vorratsspeicherung von Telekommunikationsdaten daher mit hohen finanziellen Belastungen für die betroffenen Unternehmen verbunden. Angesichts der genannten Summen wird die Einführung einer Vorratsspeicherung von Telekommunikationsdaten teilweise als unverhältnismäßige Belastung der Unternehmen angesehen[690], gerade wenn keine Kostenerstattung vorgesehen ist[691].

Allerdings könnte bei der Verhältnismäßigkeitsprüfung zu berücksichtigen sein, dass Unternehmen Kostensteigerungen unter Umständen ausgleichen können, etwa indem sie von ihren Kunden höhere Entgelte verlangen. Im besten Fall können negative Auswirkungen auf die Ertragslage der Unternehmen sogar gänzlich verhindert werden. Fraglich ist, wie die Verhältnismäßigkeit einer Kommunikationsdatenspeicherungspflicht in diesem bestmöglichen Fall zu beurteilen wäre. Zwar können Berufsausübungsregelungen auch unabhängig von ihren finanziellen Auswirkungen mit Belastungen für die Betroffenen verbunden sein. Durch eine Vorratsspeicherungspflicht würden die betroffenen Unternehmen etwa zu staatlichen Hilfsdiensten verpflichtet, die ansonsten nicht Bestandteil ihrer Tätigkeit wären. Angesichts der Tatsache, dass ein Beruf vorwiegend zur Gewinnerzielung ausgeübt wird, wiegen solche Beeinträchtigungen aber weniger schwer, wenn trotz der staatlichen Inanspruchnahme gleich bleibende Gewinne zu erzielen sind. Im vorliegenden Zusammenhang kommt hinzu, dass Telekommunikationsanbieter schon heute regelmäßig Kommunikationsdaten speichern, es sich also nicht um eine ganz unternehmensfremde Tätigkeit handelt[692]. Wenn Unternehmen höhere Kosten dauerhaft durch höhere Einnahmen oder durch andere Maßnahmen ausgleichen können, entstehen ihnen daher letztlich keine wesentlichen Nachteile; in diesem Fall ist ihnen eine Vorratsspeicherungspflicht zumutbar.

Im Sinne eines effektiven Grundrechtsschutzes sind Möglichkeiten eines Kostenausgleichs allerdings nur insoweit zu berücksichtigen, wie ein Kostenausgleich jedenfalls typischerweise auch tatsächlich möglich ist[693]. Zwar mag die jeweilige Marktlage kein geeignetes Kriterium für die Verfassungsmäßigkeit eines Gesetzes sein[694]. Jedoch kann nicht außer Acht gelassen werden, wenn ein Auf-

685 APIG, Communications Data, 24.

686 Nach Eurostat Jahrbuch 2002, Menschen in Europa (I), 3.

687 Vgl. auch Wirtschaftsausschuss des Bundesrates in BR-Drs. 755/2/03, 37: „Erste entsprechende Schätzungen sprechen von einem Volumen von 200 Millionen Euro jährlich."

688 G8 Workshop, Potential Consequences for Data Retention.

689 Tim Snape (ISPA UK), zitiert bei BBC News Online, Net snooping laws ‚too costly'; Einzinger (Generalsekretär Internet Service Providers Austria), Brief an Bundeskanzler Dr. Wolfgang Schüssel; ISPA Austria: ISPA lehnt EU-Vorstoß für verpflichtende Datenspeicherung ab, 07.05.2004, www.ispa.at/www/getFile.php?id=452.

690 EDSB-Konferenz, Europäische Datenschutzbeauftragte: Statement at the International Conference in Cardiff (09.-11.09.2002) on mandatory systematic retention of telecommunication traffic data, BT-Drs. 15/888, 176; eco, Electronic Commerce Forum e.V., Verband der deutschen Internetwirtschaft: Pressemitteilung vom 31.05.2002 zur Gesetzesinitiative des Bundesrats vom 31.05.2002 (BR-Drs. 275/02), www.eco.de/presse/mitteilungen/2002/02-05-31_de.htm; eco, Electronic Commerce Forum e.V., Verband der deutschen Internetwirtschaft: Vorratsdatenspeicherung ist verfassungswidrig! Pressemitteilung vom 17.12.2003, www.eco.de/servlet/PB/menu/1236462_pcontent_l1/content.html; GDD, Gesellschaft für Datenschutz und Datensicherung e.V.: Bundesratsinitiative zur Vorratsdatenspeicherung verstößt gegen elementare Grundsätze des Datenschutzes, Pressemitteilung vom 05.06.2002, www.rainer-gerling.de/aktuell/vorrat.html; BITKOM: Stellungnahme zur Gesetzesinitiative des Bundesrates vom 31.05.2002 (BR-Drs. 275/02), 12.08.2002, www.bitkom.org/files/documents/Position_BITKOM_Vorratsdatenspeicherung_u.a._12.08.2002.pdf, 8; Einzinger (Generalsekretär Internet Service Providers Austria), Brief an Bundeskanzler Dr. Wolfgang Schüssel.

691 Wirtschaftsausschuss des Bundesrates in BR-Drs. 755/2/03, 37; eco, Electronic Commerce Forum e.V., Verband der deutschen Internetwirtschaft: Pressemitteilung vom 31.05.2002 zur Gesetzesinitiative des Bundesrats vom 31.05.2002 (BR-Drs. 275/02), www.eco.de/presse/mitteilungen/2002/02-05-31_de.htm: „wirtschaftlich untragbar"; vgl. auch allgemein Germann, 576: Zumutbar nur, wenn die zusätzlichen Kosten lediglich einen geringen Teil der Gesamtkosten des Unternehmens ausmachten.

692 Zu diesem Kriterium BVerfGE 30, 292 (324 f.).

693 A.A. BVerfGE 30, 292 (326): Es genüge, wenn keine rechtlichen Hindernisse für eine Abwälzung der Kosten bestünden; ebenso Friedrich, Verpflichtung, 178 m.w.N.

694 BVerfGE 30, 292 (326).

fangen von Mehrkosten nach den tatsächlichen wirtschaftlichen Gegebenheiten typischerweise und dauerhaft, also gerade unabhängig von der jeweiligen Marktlage, unmöglich ist.

Fraglich ist demnach, inwieweit den von einer Vorratsspeicherungspflicht potenziell betroffenen Unternehmen eine Umlegung ihrer Mehrkosten tatsächlich möglich wäre. Wie oben ausgeführt, sind die Kunden von Telekommunikationsdiensteanbietern regelmäßig auf deren Dienste angewiesen. Legt man eine Kostensteigerung um 15% infolge einer Kommunikationsdatenspeicherungspflicht zugrunde, dann wäre auch nicht zu befürchten, dass Kunden in großem Maßstab auf Anbieter aus Drittländern ausweichen würden. Es wäre dann davon auszugehen, dass zumindest große Unternehmen ihrer Mehrkosten weitgehend an ihre Kunden weitergeben könnten und dadurch keine erheblichen finanziellen Einbußen erleiden würden. In diesem Fall wäre in einer Vorratsspeicherungspflicht eine angemessene Beschränkung der freien Berufsausübung zu sehen.

Allerdings ist unklar, mit welchen Kosten eine generelle Vorratsspeicherung von Telekommunikationsdaten tatsächlich verbunden wäre und in welchem Maß die betroffenen Unternehmen diese Kosten auffangen könnten. Auch ohne die experimentelle Einführung einer Vorratsspeicherungspflicht lassen sich diese Fragen näher untersuchen. Zudem duldet die Frage Aufschub, weil eine Vorratsspeicherung von Telekommunikationsdaten nicht ausnahmsweise zur Abwendung schwerster Gefahren dringend erforderlich ist[695]. Weil eine Vorratsspeicherungspflicht im Einzelfall zu Insolvenzen und damit zu irreparablen Einbußen auf Seiten der Betroffenen führen könnte, ist der Gesetzgeber verpflichtet, die ihm zugänglichen Erkenntnisquellen vor Einführung einer Kommunikationsdatenspeicherungspflicht auszuschöpfen und die maßgeblichen Tatsachen vor einer Entscheidung prüfen zu lassen[696]. Ohne eine solche Prüfung ist den betroffenen Unternehmen eine Kommunikationsdatenspeicherungspflicht nicht zumutbar[697] und verstößt gegen Art. 12 Abs. 1 GG.

695 Seite 81.
696 Vgl. Seite 32.
697 Vgl. Breyer, Vorratsspeicherung, 264.

3. Die Eigentumsgarantie (Artikel 14 Abs. 1 GG)

Die §§ 110a, 110b TKG greifen insoweit in die Eigentumsgarantie ein, wie sie dazu führen, dass bisher zum Angebot von Telekommunikationsdiensten genutzte Einrichtungen von dem Nutzungsberechtigten nicht mehr genutzt werden können, weil die Einrichtungen eine Vorratsspeicherung von Telekommunikationsdaten nicht erlauben. Dieser Eingriff ist unverhältnismäßig, weil das Gesetz nicht sicherstellt, dass den betroffenen Unternehmen dadurch keine wesentlichen, unvermeidbaren finanziellen Nachteile entstehen.

Als „Eigentum" schützt Art. 14 Abs. 1 S. 1 GG jedes konkrete, gegenwärtig bestehende und vermögenswerte subjektive Recht[698]. Das Vermögen als solches ist grundsätzlich nicht geschützt[699]. Eine Ausnahme hiervon macht das Bundesverfassungsgericht für Maßnahmen, welche die Betroffenen übermäßig belasten und ihre Vermögensverhältnisse grundlegend beeinträchtigen würden[700]. Nach Art. 14 Abs. 1 S. 2 GG werden Inhalt und Schranken des Eigentums durch die Gesetze bestimmt. Geht eine solche gesetzliche Inhalts- oder Schrankenbestimmung zu Lasten eines Eigentümers, so liegt ein Eingriff in dessen Eigentumsrecht vor, wie es die Rechtsordnung bisher gewährleistete. Ein Eingriff in den Schutzbereich der Eigentumsgarantie des Art. 14 Abs. 1 GG liegt danach dann vor, wenn eine als Eigentum geschützte Rechtsposition dem bisher Berechtigten entzogen wird oder wenn ihre Nutzung, die Verfügung über sie oder ihre Verwertung behindert wird[701].

Teilweise wird vertreten, dass auch ein Unternehmen als eingerichteter und ausgeübter Gewerbebetrieb Eigentum im Sinne des Art. 14 Abs. 1 GG sei[702]. Unabhängig von der Frage der Richtigkeit dieser Ansicht sind jedenfalls Aussichten auf künftige Unternehmensgewinne vom Schutzbereich der Eigentumsgarantie auszunehmen. Nur auf diese Weise ist eine nachvollziehbare Abgrenzung zu Art. 12 Abs. 1 GG zu gewährleisten. Das Bundesverfassungsgericht hat zu diesem Zweck die Formel geprägt, dass Art. 12 GG den Erwerbsvorgang schütze und Art. 14 GG das bereits Erworbene[703].

Unberührt von der Frage des Schutzes von Unternehmen als eigenständigen Vermögenswerten bleibt der grundrechtliche Schutz des Eigentums von Unternehmen an einzelnen Vermögenswerten. Eine Kommunikationsdatenspeicherungspflicht könnte zur Folge haben, dass die zur Erfüllung dieser Pflicht herangezogenen Personen neue Anlagen anschaffen und bestehende Anlagen umgestalten oder sogar stilllegen müssten. Die Notwendigkeit einer Anschaffung neuer Anlagen betrifft lediglich das Vermögen der Betroffenen, so dass die Eigentumsgarantie insoweit nicht betroffen ist. Anders verhält es sich bei Anlagen, die Anbieter von Telekommunikationsdiensten bisher für ihr Gewerbe einsetzen und die infolge der Einführung einer Kommunikationsdatenspeicherungspflicht nicht mehr oder jedenfalls ohne Nachrüstung nicht mehr wirtschaftlich sinnvoll genutzt werden könnten. Insoweit kommt ein Eingriff in die Eigentumsgarantie in Betracht.

Die Anwendbarkeit des Art. 14 Abs. 1 GG hängt zunächst nicht davon ab, ob der Betreiber einer Telekommunikationsanlage auch deren Eigentümer ist. Selbst wenn es sich um gemietete, geleaste, unter Eigentumsvorbehalt gekaufte oder als Sicherheit übereignete Anlagen handelt, so kommt dem Betreiber der Anlagen jedenfalls ein Gebrauchsrecht an ihnen zu, welches Art. 14 GG als vermögenswertes Recht schützt[704].

Wenn die wirtschaftlich sinnvolle Nutzung einer Anlage überhaupt unmöglich wird, könnte man erwägen, ob eine Enteignung im Sinne von Art. 14 Abs. 3 GG vorliegt. Diese ist dann gegeben, wenn der Staat zur Erfüllung bestimmter öffentlicher Aufgaben eine als Eigentum geschützte Rechtsposition gezielt dem bisherigen Eigentümer entzieht[705]. Eine Kommunikationsdatenspeicherungspflicht hat nicht primär zum Ziel, den Verpflichteten die Rechte an ihren Anlagen zu entziehen. Sinn der Maßnahme ist es vielmehr, die Betreiber zur Anschaffung der für eine Vorratsspeicherung von Telekommunikationsdaten erforderlichen Geräte anzuhalten. Lediglich mittelbar kann eine Kommunikationsdatenspeicherungspflicht zum faktischen Verlust von als Eigentum geschützten Rechtspositionen führen, so dass keine Enteignung im Sinne von Art. 14 Abs. 3 GG vorliegt.

Es könnte aber ein Eingriff in Art. 14 Abs. 1 GG vorliegen. Zu bedenken ist, dass nicht jede hoheitliche Beeinträchtigung der Gebrauchsmöglichkeiten einer Sache als Eingriff in Art. 14 Abs. 1 GG anzusehen sein kann. Das Grundgesetz garantiert die Handlungsfreiheit in anderen Grundrechten um-

698 P/S, Rn. 903; J/P6-Jarass, Art. 14, Rn. 7 und 22 m.w.N.
699 J/P6-Jarass, Art. 14, Rn. 15 m.w.N.
700 So für Geldleistungspflichten etwa BVerfGE 14, 221 (241); BVerfGE 82, 159 (190).
701 P/S, Rn. 912 und 914; J/P6-Jarass, Art. 14, Rn. 29 f.
702 So BGH seit Z 23, 157 (162 f.); BVerwGE 62, 224 (226).
703 BVerfGE 30, 292 (335); BVerfGE 88, 366 (377).
704 Vgl. Dreier-Wieland, Art. 14, Rn. 38 f.
705 P/S, Rn. 922; J/P6-Jarass, Art. 14, Rn. 70 m.w.N.

fassend, und die Handlungsfreiheit schließt auch das Recht auf Gebrauch der eigenen Sachen ein[706]. Um einer Ausuferung des Anwendungsbereichs des Art. 14 GG vorzubeugen, erscheint es daher nötig, dessen Anwendungsbereich einzuschränken[707]: Eine hoheitliche Beeinträchtigung der Gebrauchsmöglichkeiten einer Sache wird erst dann einen Eingriff in Art. 14 Abs. 1 GG darstellen, wenn die öffentliche Gewalt eine sinnvolle Nutzung der Sache durch ihren Eigentümer überhaupt unmöglich macht.

Zwar schließt diese Definition Überschneidungen mit den Freiheitsgrundrechten nicht stets aus. Solche Grundrechtskollisionen sind aber allgemein nicht unüblich und unschädlich, wenn sie nicht zu Wertungswidersprüchen führen. Wenn die öffentliche Gewalt die sinnvolle Nutzung einer Sache durch ihren Eigentümer unmöglich macht, dann ist das Eigentum an der Sache zentral betroffen. Man kann insoweit von einer enteignungsähnlichen Wirkung sprechen[708]. In diesen Fällen erscheint es nicht gerechtfertigt, die Eigentumsgarantie hinter die Freiheitsgrundrechte zurücktreten zu lassen. Insbesondere wäre es dogmatisch nicht begründbar, anzunehmen, dass Art. 14 Abs. 1 GG nur vor finalen Eigentumsverkürzungen schütze. Wie bei den anderen speziellen Grundrechten müssen auch im Bereich der Eigentumsgarantie mittelbare Beeinträchtigungen unter den allgemeinen Voraussetzungen[709] zur Annahme eines Eingriffs genügen.

Dass eine Kommunikationsdatenspeicherungspflicht die sinnvolle Benutzung bestimmter Anlagen durch die bisher Berechtigten unmöglich machen könnte, weil mit einigen Anlagen eine Vorratsspeicherung von Telekommunikationsdaten nicht realisierbar ist, ist gut denkbar. In diesem Fall läge ein Eingriff in die Eigentumsgarantie vor, der den Betroffenen nur nach Maßgabe des Verhältnismäßigkeitsprinzips zuzumuten wäre. Anerkannt ist, dass das Verhältnismäßigkeitsgebot eine Entschädigung der von einem schwerwiegenden Eingriff in Art. 14 Abs. 1 GG Betroffenen gebieten kann[710], dass die Verhältnismäßigkeit eines solchen Eingriffs in Art. 14 Abs. 1 GG also von der Gewährung einer Entschädigung abhängen kann. Dies ist regelmäßig dann anzunehmen, wenn eine Norm in ihrer Wirkung einer Enteignung nahe oder gleich kommt[711]. Art. 14 Abs. 2 GG ändert daran nichts, denn wie sich aus Art. 14 Abs. 2 S. 2 GG ergibt, will die Norm den Gebrauch von Eigentum nur einschränken und nicht den entschädigungslosen Entzug sämtlicher Gebrauchsmöglichkeiten ermöglichen.

Wenn die sinnvolle Nutzung einer Sache durch ihren Eigentümer gänzlich unmöglich gemacht wird, wird man eine enteignungsähnliche Wirkung annehmen müssen, denn die Privatnützigkeit ist Wesensmerkmal des Eigentums[712]. Art. 14 Abs. 1 GG gebietet es daher, eine Entschädigung für unvermeidbare finanzielle Nachteile derjenigen Personen und Unternehmen vorzusehen, die infolge der Einführung einer Kommunikationsdatenspeicherungspflicht bisher genutzte Einrichtungen nicht mehr einsetzen können. Die Betroffenen sind grundsätzlich so zu stellen wie wenn eine Kommunikationsdatenspeicherungspflicht nicht eingeführt worden wäre. Der Eigentümer einer nicht mehr benutzbaren Anlage ist also beispielsweise finanziell in die Lage zu versetzen, eine Anlage mit vergleichbaren Nutzungsmöglichkeiten anzuschaffen, die den neuen gesetzlichen Anforderungen genügt. Bei der Bemessung der Entschädigung darf der Gesetzgeber allerdings einen – etwa durch Verkauf der Anlage in das Ausland – tatsächlich realisierbaren Restwert berücksichtigen. Wenn die Umrüstung einer Anlage möglich ist, kann die Höhe der Entschädigung auf die Umrüstungskosten begrenzt werden. Wäre eine Anlage aus anderen Gründen ohnehin bald ersetzt worden, so darf auch dies entschädigungsmindernd berücksichtigt werden. Zudem darf – parallel zu Art. 12 Abs. 1 GG[713] – von einer Entschädigung insoweit abgesehen werden, wie der Wertverlust von den Betroffenen durch zumutbare Maßnahmen aufgefangen werden kann, etwa durch Preissteigerungen.

4. Die Meinungsfreiheit, die Informationsfreiheit, die Rundfunkfreiheit und die Pressefreiheit (Artikel 5 Abs. 1 GG)

Die §§ 110a, 110b TKG verletzen auch die Meinungs-, die Informations- und die Rundfunkfreiheit aus Art. 5 Abs. 1 GG.

a) Schutzbereich der Meinungsfreiheit

Art. 5 Abs. 1 S. 1 Hs. 1 GG gewährleistet das Recht, Meinungen in Wort, Schrift und Bild äußern und verbreiten zu dürfen. Dies umfasst auch Meinungsäußerungen unter Benutzung der Medien Tele-

706 J/P6-Jarass, Art. 14, Rn. 5 m.w.N.
707 Ossenbühl, VVDStRL 29, 137 (179); J/P6-Jarass, Art. 14, Rn. 5 m.w.N.
708 Vgl. J/P6-Jarass, Art. 14, Rn. 46 m.w.N.
709 Seite 24.
710 J/P6-Jarass, Art. 14, Rn. 46.
711 J/P6-Jarass, Art. 14, Rn. 46.
712 Vgl. BVerfGE 100, 226 (241).
713 Seite 90.

fon („Wort“), Telefax („Schrift und Bild“) und Internet („Wort, Schrift und Bild“)[714]. Geschützt sind Meinungsäußerungen sowohl im Wege der Individual- wie auch der Massenkommunikation[715]. Die Äußerung und Verbreitung von Tatsachenbehauptungen ist dann geschützt, wenn die Kenntnis der Tatsachenbehauptungen Voraussetzung für die Meinungsbildung ist[716]. Weil die Kenntnis einer Tatsachenbehauptung stets unabdingbare Voraussetzung dafür ist, sich darüber eine Meinung bilden zu können, ist die Äußerung und Verbreitung von Tatsachen und Tatsachenbehauptungen umfassend geschützt.

Erwiesen oder bewusst unwahre Tatsachenbehauptungen sollen dem Bundesverfassungsgericht zufolge nicht von der Meinungsfreiheit erfasst sein[717]. Dabei geht das Gericht aber von Erfordernissen der „Mißbrauchsbekämpfung, nicht vom Schutzbedürfnis des Bürgers aus“ und argumentiert „folglich eingriffsorientiert“[718]. „Die Möglichkeit von Grundrechtsmißbräuchen kann ein rechtfertigender Grund für Grundrechtsbeschränkungen, nicht aber für Schutzbereichsbegrenzungen sein.“[719] Diese Erwägungen, die das Bundesverfassungsgericht an anderer Stelle anstellt, sind auf den Bereich der Meinungsfreiheit zu übertragen mit der Folge, dass auch erwiesen oder bewusst unwahre Tatsachenbehauptungen dem Schutzbereich der Meinungsfreiheit zuzuordnen sind. Auf die nicht eindeutig durchführbare und die Rechtsprechung stets von Neuem beschäftigende Abgrenzung von Tatsachenbehauptungen und Werturteilen kommt es unter dem Aspekt des Schutzbereiches der Meinungsfreiheit daher nicht an.

Demnach ist das Recht auf Verbreitung von Tatsachenbehauptungen und Werturteilen mittels Telekommunikation durch Art. 5 Abs. 1 S. 1 Hs. 1 GG umfassend gewährleistet. Im Bereich des Internet können alle Dienste zur Verbreitung von Tatsachen und Werturteilen genutzt werden (insbesondere WWW, FTP, Usenet und E-Mail). Allerdings werden das Internet und die genannten Dienste nicht stets zur Verbreitung von Tatsachenbehauptungen oder Werturteilen genutzt. Werden sonstige Arten von Daten über das Internet ausgetauscht, so handelt es sich lediglich um eine Transaktion, die mit dem Austausch materieller Gegenstände vergleichbar ist. Insoweit ist die Meinungsfreiheit nicht einschlägig. So wird es sich etwa regelmäßig bei dem Angebot von Software oder Computerspielen über das Internet verhalten.

Die Meinungsfreiheit gewährleistet auch das Recht, die Umstände – also etwa die Zeit und den Ort – der Meinungskundgabe frei zu bestimmen[720]. Daraus ergibt sich, dass auch das Recht der Inanspruchnahme Dritter zur Verbreitung eigener Tatsachenbehauptungen oder Meinungen gewährleistet ist. Dieser Schutz wirkt allerdings nur zugunsten dessen, der seine Meinung äußert und verbreitet, nicht zugunsten des Nachrichtenmittlers[721]. Von der Meinungsfreiheit nicht geschützt sind daher etwa Telefonnetzbetreiber, Anbieter von Internetzugängen und Webhosting-Anbieter.

Fraglich ist, ob Art. 10 GG gegenüber der Meinungsfreiheit speziell ist und sie verdrängt[722]. Dass Art. 10 GG nicht in jedem Fall das speziellere Grundrecht ist, ergibt sich daraus, dass Art. 10 GG die Übermittlung aller Arten von Informationen schützt und nicht nur die Verbreitung von Tatsachenbehauptungen und Meinungen. Aber auch in Fällen, in denen sowohl ein Grundrecht aus Art. 10 GG als auch die Meinungsfreiheit einschlägig ist, weisen die Grundrechte unterschiedliche Schutzrichtungen auf: Während das Fernmelde- und das Briefgeheimnis die Vertraulichkeit der Kommunikation schützen sollen, schützt die Meinungsfreiheit das Recht, Tatsachenbehauptungen und Meinungen überhaupt frei äußern und verbreiten zu dürfen. Vor staatlicher Kenntnisnahme einer Äußerung schützt die Meinungsfreiheit nicht. Umgekehrt schützt das Fernmelde- und das Briefgeheimnis nicht das Recht der freien Meinungsäußerung. Es ist nicht gerechtfertigt, durch die Annahme eines Spezialitätsverhältnisses die Meinungsfreiheit auf dem Gebiet der räumlich distanzierten Kommunikation quasi aufzuheben, zumal Art. 5 Abs. 1 S. 1 Hs. 1 GG die freie Wahl des für eine Meinungsäußerung eingesetzten Mediums gewährleistet[723]. In Anbetracht der unterschiedlichen Schutzzwecke müssen die Grundrechte aus Art. 10 GG einerseits und die Meinungsfreiheit andererseits daher nebeneinander anwendbar sein (Idealkonkurrenz).

714 BVerfG EuGRZ 1997, 446 (446) für das Internet.
715 Für Meinungsäußerungen in der Presse BVerfGE 85, 1 (11 f.); BVerfGE 86, 122 (128).
716 BVerfGE 94, 1 (7); BVerfGE 65, 1 (41); BVerfGE 61, 1 (8).
717 BVerfG seit E 54, 208 (219).
718 Vgl. BVerfGE 85, 386 (397).
719 Vgl. BVerfGE 85, 386 (397).
720 P/S, Rn. 556 m.w.N.
721 Vgl. P/S, Rn. 558.
722 So J/P7-Jarass, Art. 10, Rn. 2; M/D-Dürig, Art. 10, Rn. 29; Brenner, Die strafprozessuale Überwachung des Fernmeldeverkehrs mit Verteidigern, 33.
723 Seite 94.

In Idealkonkurrenz stehen auch Meinungs- und Berufsfreiheit[724], da auch diese Grundrechte unterschiedliche Schutzrichtungen aufweisen. Das Konkurrenzverhältnis zwischen Meinungs- und Berufsfreiheit wird dann relevant, wenn Tatsachen oder Meinungen gewerbsmäßig oder in Gewinnerzielungsabsicht verbreitet werden (z.B. durch ein Presseunternehmen oder ein Online-Nachrichtenmagazin).

b) Schutzbereich der Informationsfreiheit

Art. 5 Abs. 1 S. 1 Hs. 2 GG gewährleistet das Recht, sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Erfasst ist sowohl die Unterrichtung über Meinungen als auch über Tatsachenbehauptungen[725]. Gerade das Recht auf freie Unterrichtung über Tatsachen ist Funktionsbedingung einer Demokratie[726], die von der Mitwirkung bei und der Kontrolle von staatlichen Entscheidungen durch die Öffentlichkeit lebt. Kann eine Informationsquelle nur mit Hilfe von technischen Vorrichtungen genutzt werden, dann gewährleistet die Informationsfreiheit auch das Recht zur Anschaffung und Nutzung der erforderlichen Vorrichtungen[727].

Allgemein zugänglich ist eine Informationsquelle jedenfalls dann, wenn sie technisch dazu geeignet und bestimmt ist, einem individuell nicht bestimmbaren Personenkreis Informationen zu verschaffen[728]. Diese Definition des Bundesverfassungsgerichts ist allerdings insoweit unglücklich, als es statt „individuell bestimmbar“ „individuell bestimmt“ heißen muss: Einschlägig ist die Informationsfreiheit nur dann nicht, wenn der Adressatenkreis einer Quelle nach dem Willen ihres Inhabers abschließend feststeht und nicht erweiterbar ist[729]. Demgegenüber ist es für den Schutzzweck der Informationsfreiheit unerheblich, ob eine Informationsquelle nach dem Willen ihres Inhabers nur einem bestimmten, nach allgemeinen Merkmalen abgegrenzten Adressatenkreis offen stehen soll oder der Allgemeinheit. Beispielsweise soll eine Zeitung regelmäßig nur an zahlende Käufer abgegeben werden und jugendgefährdende Schriften nur an Volljährige. In derartigen Fällen müssen sich all diejenigen Personen auf das Grundrecht der Informationsfreiheit berufen können, welche die von dem Inhaber der Informationsquelle geforderten Merkmale erfüllen. Das Wort „zugänglich“ in Art. 5 Abs. 1 S. 1 Hs. 2 GG bezieht sich nach allgemeinem Sprachverständnis allein auf die faktische oder technische Erreichbarkeit, so dass auch nur diese „allgemein“, also für jedermann, gegeben sein muss. Nicht erforderlich ist, dass der Inhaber einer Informationsquelle diese voraussetzungslos für jedermann eröffnet.

Art. 5 Abs. 1 S. 1 Hs. 2 GG ist hinsichtlich Internetdiensten regelmäßig einschlägig. Dies gilt sowohl im Bereich des World Wide Web[730], soweit Informationen nicht nur an einen im Voraus abschließend bestimmten Adressatenkreis gerichtet sind (z.B. individuelle elektronische Grußkarten), als auch für die Dienste FTP (File Transfer Protocol) und Usenet (Newsgroups). E-Mails werden oft an einen abschließend bestimmten Adressatenkreis gerichtet sein mit der Folge, dass Art. 5 Abs. 1 S. 1 Hs. 2 GG keine Anwendung findet. Der Versand von E-Mails kann aber auch als Informationsdienst ausgestaltet sein, dessen Inanspruchnahme jedermann oder jedenfalls bestimmten Personenkreisen offen steht (z.B. so genannte Newsletter). In diesem Fall ist die Informationsfreiheit einschlägig.

Entsprechend den Ausführungen zur Meinungsfreiheit erfasst auch die Informationsfreiheit nicht den Bezug bloßer Daten, in denen weder Tatsachen noch Werturteile zum Ausdruck kommen. Zwischen der Informationsfreiheit einerseits und dem Fernmeldegeheimnis und der Berufsfreiheit andererseits besteht Idealkonkurrenz[731].

c) Schutzbereich der Rundfunkfreiheit

Die besondere Gewährleistung der Rundfunkfreiheit in Art. 5 Abs. 1 S. 2 Var. 2 GG entspricht der herausragenden Bedeutung des Rundfunks in einer freiheitlichen Demokratie. Ein freier Rundfunk vermittelt umfassend Tatsachen und Meinungen und dient damit mittelbar der Meinungsbildung der Bürger[732]. Das Bundesverfassungsgericht bezeichnet die Freiheit der Medien dementsprechend als konstituierend für die freiheitliche demokratische Grundordnung[733].

724 V. Münch/Kunig-Gubelt, Art. 12, Rn. 95; Sachs-Tettinger, Art. 12, Rn. 167; vgl. auch BVerfGE 30, 336 (352) für die Einschlägigkeit der Meinungsfreiheit bei der Verbreitung von Meinungen zur Gewinnerzielung; BVerfGE 85, 1 (11 f.) und BVerfGE 86, 122 (128) für die Einschlägigkeit der Meinungsfreiheit bei Presseunternehmen.

725 Dreier-Schulze-Fielitz, Art. 5 I, II, Rn. 57; J/P6-Jarass, Art. 5, Rn. 15 m.w.N.

726 Hornung, MMR 2004, 3 (5) m.w.N.

727 BVerfGE 90, 27 (32).

728 BVerfGE 27, 71 (83); BVerfGE 33, 52 (65).

729 Für die Anwendung dieses Kriteriums im Bereich der Rundfunkfreiheit plädiert J/P6-Jarass, Art. 5, Rn. 36.

730 Vgl. Hornung, MMR 2004, 3 (5).

731 Vgl. Nachweise auf Seiten 94-95 zur Meinungsfreiheit.

732 BVerfGE 57, 295 (319); BVerfGE 74, 297 (323).

733 St. Rspr. seit BVerfGE 7, 198 (208).

Ihrem traditionellen Verständnis nach schützt die Rundfunkfreiheit nur die Vorbereitung und Produktion von Rundfunksendungen im engeren Sinne, also von Hörfunk und Fernsehen[734]. Seinem Schutzzweck nach ist das Grundrecht aber auch für neuere Abruf- und Zugriffsdienste[735] wie Video- oder Teletext[736] und das Internet[737] einschlägig. Dass die Übertragung per „Funk“ keine Voraussetzung des verfassungsrechtlichen Runkfunkbegriffs ist, zeigt bereits die Existenz des Kabelfernsehens, dessen Eigenschaft als Rundfunk allgemein anerkannt ist[738]. Maßgeblich für den verfassungsrechtlichen Rundfunkbegriff ist allein, dass Ziel des Unternehmens die Verbreitung von Informationen an eine unbestimmte[739] Vielzahl von Personen mittels elektrischer Schwingungen ist[740].

Art. 5 Abs. 1 S. 2 Var. 2 GG gewährleistet die Freiheit des gesamten Produktionsvorgangs von Rundfunkprogrammen, von der Informationsbeschaffung bis hin zur Verbreitung des fertigen Erzeugnisses[741]. Geschützt ist nicht nur die Berichterstattung über Tatsachen, sondern auch die Verbreitung von Meinungen[742]. Die Verbreitung sonstiger Daten ist dagegen wiederum nicht erfasst.

Von Art. 5 Abs. 1 S. 2 Var. 2 GG geschützt ist der Rundfunk als Medium der Informationsvermittlung. Die Rundfunkfreiheit gewährleistet daher lediglich den Rahmen für die Vermittlung von Inhalten, während für die vermittelten Inhalte selbst allein die Meinungsfreiheit gilt[743]. Weil der Rundfunk gerade als Medium geschützt ist, wird man eine gewisse Dauerhaftigkeit voraussetzen müssen, wenn ein Dienst als Rundfunk im Sinne des Art. 5 Abs. 1 S. 2 Var. 2 GG gelten soll. Man wird daher wenigstens verlangen müssen, dass die Verbreitung der Informationen geschäftsmäßig, also nicht nur vorübergehend oder punktuell, erfolgt.

Im Telekommunikationsbereich kann sich auf die Rundfunkfreiheit demnach nur berufen, wer einem nicht abschließend bestimmten Personenkreis eigene oder fremde Tatsachen oder Meinungen geschäftsmäßig zum Abruf anbietet. In diesem Rahmen ist auch das Angebot von Tele- und Mediendiensten von Art. 5 Abs. 1 S. 1 Hs. 1 GG geschützt. Im Internet existiert ein großer Kreis von Rundfunkanbietern, weil die Veröffentlichung von Tatsachen oder Meinungen dort nur mit geringem Aufwand verbunden ist und weil Informationen meistens über längere Zeit abrufbar bleiben, so dass das Merkmal der Geschäftsmäßigkeit regelmäßig erfüllt sein wird. Daraus folgt, dass sich beispielsweise bereits der Betreiber einer privaten Homepage auf die Rundfunkfreiheit berufen kann, wenn er einer unbestimmten Vielzahl von Personen Tatsachen oder Meinungen zum Abruf anbietet.

Entsprechend den Ausführungen zur Meinungsfreiheit besteht auch zwischen der Rundfunkfreiheit einerseits und dem Fernmeldegeheimnis und der Berufsfreiheit andererseits Idealkonkurrenz[744].

d) Schutzbereich der Pressefreiheit

Art. 5 Abs. 1 S. 2 Var. 1 GG schützt die Freiheit der Presse. Traditionell werden als „Presse“ nur Druckerzeugnisse angesehen[745]. Definiert man den Schutzbereich der Rundfunkfreiheit so umfassend wie oben geschehen, dann ist es unschädlich, elektronisch verbreitete Informationen vom Schutzbereich der Pressefreiheit auszunehmen. Zugleich ist auf diese Weise eine zuverlässige Abgrenzung der beiden Grundrechte anhand des jeweiligen Trägermediums gewährleistet. Die Pressefreiheit ist im vorliegenden Zusammenhang daher nicht einschlägig.

e) Eingriff

Der Staat greift in die Meinungs-, Informations- oder Rundfunkfreiheit ein, wenn er Private zu einer generellen Vorratsspeicherung von Telekommunikationsdaten ihrer Kunden verpflichtet, ohne die dadurch entstehenden Kosten zu erstatten. Es wurde bereits dargelegt, dass ein solches Vorgehen zumindest zu erheblich höheren Preisen der betroffenen Unternehmen führen würde[746]. Dies wiederum hätte zur Folge, dass gerade weniger finanzkräftige Bürger, Unternehmen und Organisationen zu einer Einschränkung des Abrufs und der Verbreitung von Tatsachenbehauptungen und Meinungen über

734 BVerfGE 12, 205 (226).
735 BVerfGE 74, 297 (345); BVerfGE 83, 238 (302).
736 BVerfGE 74, 297 (345).
737 Offen gelassen in BVerfG EuGRZ 1997, 446.
738 Vgl. BVerfGE 74, 297 (351): Übertragung „ohne Verbindungsleitung oder längs oder mittels eines Leiters“.
739 Zu dem Begriff vgl. Seite 95.
740 P/S, Rn. 573.
741 BVerfGE 77, 65 (74); BVerfGE 91, 125 (135).
742 BVerfGE 35, 202 (222); BVerfGE 57, 295 (319).
743 So für die Pressefreiheit BVerfGE 85, 1 (11 f.); BVerfGE 86, 122 (128).
744 Für Rundfunk- und Berufsfreiheit M/D-Scholz, Art. 12, Rn. 161 und 165; für Presse- und Berufsfreiheit v. Münch/Kunig-Wendt, Art. 5, Rn. 115 und Sachs-Bethge, Art. 5, Rn. 89a; J/P, Art. 5, Rn. 24; M/D-Herzog, Art. 5 Abs. I, II, Rn. 142.
745 BVerfGE 95, 28 (35).
746 Seiten 89-91.

Telekommunikationsnetze gezwungen wären. Einzelpersonen und Non-Profit-Organisationen, die Kostensteigerungen nicht tragen können, wären zum Teil gezwungen, eigene Internetangebote einzustellen und von der Nutzung zentraler Kommunikationsdienste wie E-Mail abzusehen[747]. Dienste im Internet, die sich bisher werbefinanzieren und ihre Leistungen daher unentgeltlich anbieten konnten (z.B. E-Mail-Konten, Suchmaschinen, Webhosting), müssten teilweise eingestellt werden.

Der Kostensteigerungseffekt kann nicht dadurch aufgefangen werden, dass preislich günstige Telekommunikationsdienste aus denjenigen Ländern weiter angeboten oder in Anspruch genommen werden könnten, die eine generelle Vorratsspeicherung von Telekommunikationsdaten ablehnen (wie z.B. die USA). Ein Ausweichen auf Telekommunikationsdienste aus Drittländern wäre oft mit noch höheren Kosten verbunden als die Nutzung deutscher Dienste. Einzelpersonen und kleine Organisationen würden in vielen Fällen auch nicht mit den Querelen zurecht kommen, die mit der Nutzung ausländischer Angebote verbunden sind (z.B. andere Sprache, unbekanntes Rechtssystem). Die Verlagerung eines gesamten Unternehmens in das Ausland wird erst recht nur für größere Unternehmen in Betracht kommen.

Höhere Kosten würden also letztlich zu einer Beeinträchtigung des Austausches von Meinungen und Tatsachen mittels Telekommunikation führen. Die Betroffenen haben heutzutage in vielen Fällen keine zumutbaren Ausweichmöglichkeiten außerhalb der Telekommunikationsnetze, so dass insgesamt eine merklichen Beeinträchtigung des Austausches von Meinungen und Tatsachen in unserer Gesellschaft droht.

Fraglich ist, ob dies dem Staat als Eingriff zuzurechnen ist. Ein Grundrechtseingriff liegt jedenfalls dann vor, wenn der Staat in gezielter und gewollter Weise, rechtlich verbindlich und unmittelbar grundrechtsgeschütztes Verhalten beeinträchtigt (klassischer Eingriffsbegriff)[748]. Eine gesetzliche Verpflichtung zur Vorratsspeicherung stellt zwar einen Rechtsakt dar, dieser Rechtsakt ist seiner Intention nach aber nicht darauf gerichtet, den Informationsaustausch mittels Telekommunikation zu erschweren. Zudem hat er nur mittelbar grundrechtsbeeinträchtigende Wirkung. Ein Grundrechtseingriff im klassischen Sinne liegt daher nicht vor.

Nach neuerem Verständnis schützen die speziellen Grundrechte jedoch auch vor unbeabsichtigten und mittelbaren Grundrechtsverkürzungen durch staatliche Maßnahmen, wenn diese die Beeinträchtigung eines grundrechtlich geschützten Verhaltens typischerweise und vorhersehbar zur Folge haben oder wenn sie eine besondere Beeinträchtigungsgefahr in sich bergen, die sich jederzeit verwirklichen kann[749]. In einem solchen Fall darf sich der Staat dem objektiv zu Erwartenden nicht verschließen.

Im vorliegenden Zusammenhang sind die wirtschaftlichen Auswirkungen einer Vorratsspeicherungspflicht ohne finanzielle Kompensation anerkannt. Dass ein höherer Preis zu einer geringeren Nachfrage führt als ein niedrigerer Preis oder gar ein kostenloses Angebot, liegt als wirtschaftswissenschaftliche Grundkenntnis ebenfalls auf der Hand. Der verminderte Austausch von Meinungen und Informationen ist daher typische und vorhersehbare Folge der Einführung einer Vorratsspeicherungspflicht ohne finanzielle Kompensation der Betroffenen. Damit greift eine solche Maßnahme in die Meinungs-, Informations- und die Rundfunkfreiheit ein.

Unabhängig von der Kostenfrage liegt ein Eingriff in die genannten Grundrechte auch insoweit vor, wie eine generelle Vorratsspeicherung von Kommunikationsdaten Telekommunikationsvorgänge zurückverfolgbar macht und dies Anbieter wie Nutzer von Informationen abschrecken kann[750]. Ein solcher Effekt ist gerade in Bezug auf staatskritische Informationen zu erwarten, deren freier Austausch in einer Demokratie von besonders hohem Wert ist[751]. Dieser Abschreckungseffekt kann nicht durch Möglichkeiten anonymer Telekommunikationsnutzung aufgefangen werden, weil die Nutzung dieser Möglichkeiten zusätzliche Kosten verursachen kann, die verfügbaren Dienste in ihrer Wirkung teilweise intransparent sind und weil zu ihrer Nutzung meist ein gewisses technisches Grundverständnis erforderlich ist, über das nicht jeder verfügt. Eine generelle Vorratsspeicherung von Telekommunikationsdaten behindert somit auch durch ihre abschreckende Wirkung typischerweise und vorhersehbar den Austausch von Meinungen und Tatsachenbehauptungen[752]. Ein Eingriff in die Meinungsfreiheit, Informationsfreiheit und Rundfunkfreiheit liegt somit auch insoweit vor.

747 Bäumler, Helmut / Leutheusser-Schnarrenberger, Sabine / Tinnefeld, Marie-Theres: Grenzenlose Überwachung des Internets? Steht die freie Internetkommunikation vor dem Aus? Stellungnahme zum Gesetzesentwurf des Bundesrates vom 31. Mai 2002, www.rainer-gerling.de/aktuell/vorrat_stellungnahme.html, Punkt 1.

748 Windthorst, § 8, Rn. 27.

749 Windthorst, § 8, Rn. 50 und 52 m.w.N.

750 Seite 73 ff.

751 Seite 73 ff.

752 Seite 73 ff.

f) Verfassungsmäßige Rechtfertigung

Der Eingriff ist auch nicht verfassungsmäßig gerechtfertigt. Maßgeblich für die Beurteilung der Verfassungsmäßigkeit ist wiederum das allgemeine Verhältnismäßigkeitsgebot. Was den Nutzen einer Vorratsspeicherung angeht, kann auf die Ausführungen zu Art. 10 Abs. 1 Var. 3 GG verwiesen werden[753]. Auch der drohende Schaden einer solchen Regelung für die Freiheit der Meinungsäußerung, der Information und des Rundfunks wurde bereits untersucht[754]. Speziell im Bereich des Internet ist zu beachten, dass dieses Medium wie kein anderes die umfassende Verbreitung von und Unterrichtung über Tatsachen und Meinungen auf einfache und kostengünstige Art und Weise ermöglicht. Meinungsfreiheit, Informationsfreiheit und Rundfunkfreiheit sind konstituierend für eine freiheitliche Demokratie[755] und für das Gemeinwohl von fundamentaler Bedeutung[756]. Daraus folgt, dass speziell das Internet und seine Dienste heutzutage für das Gemeinwohl von höchster Bedeutung ist und der Erhaltung und dem Ausbau seiner Funktionsweise ein verfassungsrechtlich hoher Stellenwert zukommt[757]. Das Gleiche gilt für die sonstigen Telekommunikationsnetze, die vor allem den individuellen Austausch von Tatsachen und Meinungen erheblich fördern und erleichtern.

Ein besonderer Gemeinwohlbezug der Telekommunikation ist nicht nur in totalitären Staaten anzuerkennen, in denen die Bedeutung eines (möglichst überwachungsfreien) Zugangs zu Telekommunikation und Internet von kaum zu überschätzender Bedeutung für die Förderung von Demokratie und Menschenrechten ist[758]. Auch in Deutschland ist der Wert eines freien Austausches von Tatsachenbehauptungen und Meinungen über Telekommunikationsnetze von höchster Bedeutung. Gerade im Internet werden in besonderem Maße öffentliche Missstände aufgedeckt, ansonsten unzugängliche öffentliche Dokumente veröffentlicht und politische Fragen kontrovers diskutiert[759]. Selbst kleine Menschen- oder Bürgerrechtsgruppen und sogar Einzelpersonen mit sehr beschränkten technischen und finanziellen Ressourcen können der Allgemeinheit über das Internet äußerst interessante Informationen zur Verfügung stellen. Per Internet oder Telekommunikation können über weite Entfernungen hinweg auch vertrauliche Tatsachen mitgeteilt werden, etwa zwischen verschiedenen Sektionen einer Menschenrechtsorganisation oder den Teilnehmern an einer Demonstration[760].

Wägt man die drohende Beeinträchtigung dieses gesamtgesellschaftlichen Informationsaustausches und den graduellen Nutzen, den eine generelle Vorratsspeicherung von Telekommunikationsdaten bestenfalls bewirken kann[761], gegeneinander ab, so kommt man nicht umhin, auch den Eingriff in Meinungsfreiheit, Informationsfreiheit und Rundfunkfreiheit, der in einer generellen Vorratsspeicherung von Telekommunikationsdaten liegen würde, als unverhältnismäßig und für die Betroffenen unzumutbar zu bewerten. Eine generelle Vorratsspeicherung von Telekommunikationsdaten ist daher mit Meinungsfreiheit, Informationsfreiheit und Rundfunkfreiheit unvereinbar.

753 Seite 34 ff.
754 Seite 73 ff.
755 BVerfGE 62, 230 (247) für die Meinungsfreiheit.
756 Vgl. BVerfGE 7, 198 (208) für die Meinungsfreiheit; BVerfGE 27, 71 (81 f.) für die Informationsfreiheit; BVerfGE 77, 65 (74) für die Rundfunkfreiheit.
757 Vgl. Hornung, MMR 2004, 3 (5).
758 Vgl. Heise Verlag: Schranken der Informationsfreiheit im Internet, Meldung vom 19.06.2003, www.heise.de/-newsticker/data/anw-19.06.03-001/.
759 Simitis, Internet, 291 m.w.N.: Dem Internet komme gerade beim politischen Diskurs eine kaum zu unterschätzende Bedeutung zu.
760 Weitere Beispiele für die Grundrechtsverwirklichung durch Telekommunikation finden sich auf Seite 75.
761 Seite 54; ebenso ICC/UNICE/EICTA/INTUG, Common Industry Statement on Storage of Traffic Data for Law Enforcement Purposes, 04.06.2003, www.statewatch.org/news/2003/jun/CommonIndustryPositionondataretention.pdf, 6.

5. Der allgemeine Gleichheitssatz (Artikel 3 Abs. 1 GG)

Die §§ 110a, 110b TKG verletzen den allgemeinen Gleichheitssatz (Artikel 3 Abs. 1 GG) in mehrfacher Hinsicht.

a) Ungleichbehandlung des Informationsaustausches über Telekommunikationsnetze gegenüber dem räumlich-unmittelbaren Informationsaustausch

aa) Individualkommunikation

(1) Eingriff in den Schutzbereich des Art. 3 Abs. 1 GG

Art. 3 Abs. 1 GG gewährleistet, dass der Staat Sachverhalte, die im Wesentlichen gleich sind, auch gleich behandelt[762]. Diese Pflicht trifft nach Art. 1 Abs. 3 GG auch den Gesetzgeber[763]. Im Wesentlichen gleich sind zwei Sachverhalte dann, wenn sie sich einem gemeinsamen Oberbegriff zuordnen lassen[764]. Der Oberbegriff muss die Sachverhalte vollständig erfassen[765]. Nicht erforderlich ist dagegen, dass der Oberbegriff ausschließlich die beiden zu vergleichenden Sachverhalte umfasst. Die Vergleichbarkeit zweier Sachverhalte, die sich einem gemeinsamen Oberbegriff zuordnen lassen, kann allenfalls dann verneint werden, wenn die Sachverhalte unterschiedlichen rechtlichen Ordnungsbereichen angehören und in anderen systematischen und sozialgeschichtlichen Zusammenhängen stehen[766].

Eine generelle Vorratsspeicherung von Telekommunikationsdaten führt zur unterschiedlichen Behandlung von Telekommunikation einerseits und räumlich-unmittelbarer Kommunikation andererseits, weil Kommunikationsvorgänge nur im ersten Fall ihren Umständen nach festgehalten würden. Beide Sachverhalte unterscheiden sich dadurch, dass ein Kommunikationsvorgang im einen Fall über eine räumliche Distanz hinweg und unter Nutzung von Telekommunikationstechnik stattfindet, im anderen Fall in räumlicher Gegenwart der Beteiligten. Dieser Unterschied ändert jedoch nichts daran, dass es sich in beiden Fällen um menschliche Kommunikation handelt. Gemeinsamer Oberbegriff ist daher die menschliche Kommunikation. Die Telekommunikation und die räumlich-unmittelbare Kommunikation gehören auch nicht unterschiedlichen rechtlichen Ordnungsbereichen an, so dass sie vergleichbar sind. Der Schutzbereich des Art. 3 Abs. 1 GG ist durch eine generelle Vorratsspeicherung allein von Telekommunikationsdaten demnach betroffen.

Ein Eingriff in Art. 3 Abs. 1 GG liegt vor, wenn eine Person durch eine Ungleichbehandlung von wesentlich Gleichem nachteilig betroffen ist[767]. Dies ist bei einer Vorratsspeicherung von Telekommunikationsdaten bei denjenigen Menschen der Fall, die sich des Mittels der Telekommunikation bedienen und deren Kommunikation dabei durchgängig registriert wird, während dies im Bereich der räumlich-unmittelbaren Kommunikation nicht geschieht. Damit stellt eine Vorratsspeicherung von Telekommunikationsdaten einen rechtfertigungsbedürftigen Eingriff in das Grundrecht der Telekommunikationsnutzer aus Art. 3 Abs. 1 GG dar.

(2) Rechtfertigungsmaßstab

Unter welchen Umständen eine Ungleichbehandlung verfassungsrechtlich gerechtfertigt ist, hängt nach der Rechtsprechung des Bundesverfassungsgerichts von dem jeweiligen Regelungsgegenstand und Differenzierungsmerkmal ab[768]. In manchen Fällen lässt das Bundesverfassungsgericht jeden sachlichen Grund als Rechtfertigung genügen[769]. Für eine bloße Willkürprüfung spricht es etwa, wenn eine Ungleichbehandlung von Sachverhalten ohne engen menschlichen Bezug vorliegt[770], wenn der Bereich der gewährenden Staatstätigkeit betroffen ist[771], es sich um wirtschaftsordnende Maßnahmen handelt[772] oder wenn eine Differenzierung bereits im Grundgesetz angelegt ist[773].

Dasselbe soll im Bereich vielgestaltiger Sachverhalte gelten, die im Einzelnen noch nicht bekannt sind[774]. Richtigerweise handelt es sich hierbei allerdings um eine Erscheinungsform des allgemeinen

762 St. Rspr. seit BVerfGE 1, 14 (52).
763 BVerfGE 1, 14 (52).
764 P/S, Rn. 431 ff.
765 P/S, Rn. 435.
766 J/P6-Jarass, Art. 3, Rn. 4 m.w.N.
767 Vgl. BVerfGE 67, 239 (244).
768 BVerfGE 88, 87 (96); BVerfGE 95, 267 (316).
769 BVerfGE 88, 87 (96); BVerfGE 95, 267 (316).
770 Etwa BVerfGE 38, 225 (229).
771 Etwa BVerfGE 49, 280 (282).
772 Etwa BVerfGE 18, 315 (331).
773 J/P6-Jarass, Art. 3, Rn. 23; vgl. etwa BVerfGE 52, 303 (346) für Beamte.
774 BVerfGE 33, 171 (189 f.); BVerfGE 78, 249 (288).

Problems der Behandlung unbekannter Tatsachen im Rahmen der verfassungsrechtlichen Prüfung, das differenziert zu lösen ist[775]. Tatsächliche Unsicherheiten rechtfertigen einen Einschätzungsspielraum des Gesetzgebers nur hinsichtlich der Einschätzung der unbekannten Tatsachen[776]. Auswirkungen auf den generellen Kontrollmaßstab können sie dagegen nicht haben[777].

In anderen Fallgruppen wendet das Bundesverfassungsgericht einen strengeren Prüfungsmaßstab an, dem zufolge zu untersuchen ist, ob ein sachlicher Grund von solcher Art und solchem Gewicht vorliegt, dass er die Ungleichbehandlung rechtfertigt[778]. Im Kern handelt es sich um eine Prüfung der Verhältnismäßigkeit[779]. Für die Vornahme einer Verhältnismäßigkeitsprüfung spricht es etwa, wenn die diskriminierende Maßnahme in ein Freiheitsgrundrecht eingreift[780] oder wenn die Diskriminierten keinen Einfluss auf ihre Behandlung nehmen können[781]. Insgesamt wird die Verhältnismäßigkeit insbesondere in denjenigen Fällen zu prüfen sein, in denen von einer Ungleichbehandlung erhebliche Belastungen für die Betroffenen ausgehen.

Misst man eine generelle Kommunikationsdatenspeicherung an den genannten Kriterien, so fragt sich zunächst, ob diese lediglich eine Ungleichbehandlung von Sachverhalten ohne engen menschlichen Bezug darstellt, was für eine bloße Willkürprüfung sprechen würde. Für diese Annahme könnte man anführen, dass die meisten Menschen sowohl Telekommunikation einsetzen wie auch räumlich-unmittelbar kommunizieren. Ein strikter Personenbezug in dem Sinn, dass ein Sachverhalt ausschließlich eine bestimmte Gruppe von Menschen und der andere Sachverhalt ausschließlich eine andere Menschengruppe betrifft, liegt nicht vor. Fraglich ist aber, ob dies Voraussetzung für die Annahme eines „engen menschlichen Bezugs“ ist oder ob es nicht auch genügt, dass bestimmte Personengruppen von der Ungleichbehandlung typischerweise stärker betroffen sind als andere. Von einer Vorratsspeicherung von Telekommunikationsdaten sind etwa Berufstätige und Personen, die weit von ihrer Familie entfernt leben, stärker betroffen als andere Personengruppen, die nicht im gleichen Maße auf Telekommunikation angewiesen sind.

Überhaupt haben die von einer Vorratsspeicherung Betroffenen in vielen Fällen keine Ausweichmöglichkeit. Dass in der heutigen Informationsgesellschaft ein Leben ohne Telekommunikationsnetze kaum noch denkbar ist, beruht keineswegs nur auf Bequemlichkeit und Komfort. Die moderne Arbeitsgesellschaft beispielsweise zwingt zu immer mehr räumlicher Mobilität und bringt vielfach unfreiwillige und kaum überwindbare Trennungen selbst von sich nahe stehenden Personen mit sich. Auch bestimmte Berufsgruppen, etwa Journalisten, sind in hohem Maße auf die Nutzung von Telekommunikationsnetzen angewiesen. Unternehmen, die ein auf den Fernabsatz ausgerichtetes Vertriebs- oder Dienstleistungssystem anbieten, werden oftmals zur Nutzung der Telekommunikationsnetze gezwungen sein, weil nur diese Nische ihr ökonomisches Überleben sichert. Auch Kunden können auf die Leistungen solcher Unternehmen angewiesen sein, etwa wenn jemand spezielle Waren oder Dienstleistungen benötigt, die in seinem räumlichen Umkreis nicht angeboten werden.

Festzuhalten ist somit, dass vielen Menschen in weiten Bereichen keine zumutbare Alternative zur Telekommunikation zur Verfügung steht und dass dies zumeist nicht auf einer freien Willensentscheidung beruht. Dies spricht nach den Kriterien des Bundesverfassungsgerichts für die Vornahme einer Verhältnismäßigkeitsprüfung. Zudem stellt eine Vorratsspeicherung von Telekommunikationsdaten einen schwerwiegenden Eingriff in verschiedene Freiheitsgrundrechte dar (Fernmeldegeheimnis oder Recht auf informationelle Selbstbestimmung, Berufsfreiheit, Meinungsfreiheit, Informationsfreiheit und Rundfunkfreiheit)[782]. Unabhängig davon, ob man einen engen menschlichen Bezug der Ungleichbehandlung annimmt oder nicht, überwiegen damit jedenfalls die Gesichtspunkte, die für eine Verhältnismäßigkeitsprüfung sprechen. Prüfungsmaßstab ist daher, ob ein sachlicher Grund von solcher Art und solchem Gewicht existiert, dass er es rechtfertigt, die näheren Umstände der Kommunikation über Telekommunikationsnetze generell zu erfassen, die näheren Umstände der räumlich-unmittelbaren Kommunikation dagegen nicht.

775 Seiten 31 ff.
776 Seiten 31 ff.
777 Chryssogonos, Verfassungsgerichtsbarkeit und Gesetzgebung, 189.
778 Vgl. allgemein BVerfGE 87, 234 (255); BVerfGE 91, 389 (401); BVerfGE 95, 267 (317).
779 Vgl. nur BVerfGE 82, 126 (146) und J/P7-Jarass, Art. 3, Rn. 27.
780 Für das allgemeine Persönlichkeitsrecht BVerfGE 60, 123 (134); BVerfGE 88, 87 (97).
781 Vgl. BVerfGE 88, 87 (96); BVerfGE 97, 169 (181).
782 Seite 19 ff.

(3) Machbarkeit und Finanzierbarkeit als Rechtfertigungsgrund

Zunächst kann die höhere Praktikabilität einer Regelung einen sachlichen Grund für eine damit verbundene Ungleichbehandlung darstellen[783]. Im vorliegenden Zusammenhang liegt es auf der Hand, dass eine Erfassung der Umstände der räumlich-unmittelbaren Kommunikation nicht nur weniger praktikabel wäre als eine Vorratsspeicherung von Telekommunikationsdaten. Eine ähnlich umfassende Erfassung des Kommunikationsverhaltens der Bevölkerung wie im Telekommunikations- und Onlinebereich wäre im Bereich der unmittelbaren Kommunikation schlichtweg nicht machbar. Selbst Überwachungsapparate wie das mit unvorstellbaren personellen und finanziellen Ressourcen ausgestattete Ministerium für Staatssicherheit der DDR konnten die unmittelbare Kommunikation in der Bevölkerung immer nur bruchstückhaft erfassen.

Auch finanzielle Vorteile einer Regelung können einen sachlichen Grund für eine damit verbundene Ungleichbehandlung bilden[784]. Eine Erfassung des räumlich-unmittelbaren Kommunikationsverhaltens der Bevölkerung würde jedenfalls an finanziellen Gesichtspunkten scheitern. Zwar sind bei der Bemessung der finanziellen Folgen einer Vorratsspeicherung von Kommunikationsdaten richtigerweise auch die mittelbar damit verbundenen Kosten zu berücksichtigen, die bei den Telekommunikationsunternehmen und den Endverbrauchern anfallen[785]. Dennoch sind diese Kosten immer noch ungleich geringer als die Kosten des Aufbaus und der Unterhaltung einer Überwachungsstruktur im Bereich der unmittelbaren Kommunikation, soweit dies überhaupt möglich wäre. Somit hat das Finanzierungsargument ebenfalls eine gewisse Berechtigung.

Es fragt sich allerdings, ob Gesichtspunkte der Machbarkeit und Finanzierbarkeit in der Abwägung die schwerwiegende Ungleichbehandlung überwiegen können, die eine Vorratsspeicherung ausschließlich von Telekommunikationsdaten mit sich bringt. Angesichts der tief greifenden, nicht zu kompensierenden Freiheitseinbußen durch eine solche Maßnahme[786] sowie der Tatsache, dass die Betroffenen heutzutage oftmals zu einer Nutzung von Telekommunikationsnetzen gezwungen sind[787], ist dies zu verneinen. Allein die Tatsache, dass sich das Verhalten der Menschen in Telekommunikationsnetzen umfassend überwachen lässt und sich die dazu erforderlichen materiellen Ressourcen in Grenzen halten, kann zur Rechtfertigung dieser massiven Ungleichbehandlung gegenüber der unmittelbaren Kommunikation nicht genügen[788].

(4) Erschwerung der staatlichen Aufgabenwahrnehmung als Rechtfertigungsgrund

Zur Rechtfertigung einer generellen Kommunikationsdatenspeicherung wird ferner angeführt, dass die besonderen Eigenschaften der Telekommunikationsnetze die Tätigkeit der Gefahrenabwehr- und Strafverfolgungsbehörden erschwerten[789]. In der Tat führt elektronische Kommunikation nicht selten dazu, dass Spuren entweder von Anfang an nicht entstehen – beispielsweise bei anonymer Telekommunikation – oder nachträglich beseitigt werden – beispielsweise durch Datenlöschung nach Begleichung der Rechnung[790]. Von staatlicher Seite wird teilweise vorgebracht, dass sich in der wirklichen Welt oftmals Zeugen oder andere Beweismittel für begangene Straftaten finden ließen. Diese Möglichkeit scheide im Bereich der Telekommunikationsnetze von vornherein und generell aus, wenn keine Telekommunikationsdaten gespeichert würden, wie es gegenwärtig bei vorausbezahlten oder pauschal berechneten Abrechnungsmodellen oder bei kostenlosen Diensten der Fall sei[791].

Dieser Argumentation ist entgegenzusetzen, dass sich auch im Bereich der räumlich-unmittelbaren Kommunikation Zeugen oder andere Beweismittel typischerweise nur für auffälliges Verhalten außerhalb der Privatsphäre der Straftäter finden lassen. Geht es um die Vorbereitung einer Straftat oder um Verhalten im Anschluss an die Tatbegehung, dann kann die Nutzung von Telekommunikationsnetzen für Straftäter zwar auch nützlich sein. Auch ohne sie lassen sich diese Aktivitäten aber konspirativ und

783 BVerfGE 17, 337 (354); BVerfGE 41, 126 (288); im Einzelfall ablehnend BVerfGE 55, 159 (169); BVerfGE 60, 68 (78).

784 BVerfGE 3, 4 (11); BVerfGE 75, 40 (72); BVerfGE 87, 1 (45); im Einzelfall ablehnend BVerfGE 61, 43 (63); BVerfGE 87, 1 (46); BVerfGE 92, 53 (69).

785 Allgemein zur Berücksichtigung von mittelbaren Kosten eines Gesetzes Scholz, ZRP 2002, 361 (361).

786 Seite 79 ff.

787 Seite 100.

788 Bäumler, DuD 2001, 348 (349).

789 Sieber, COMCRIME-Studie (I), 60.

790 NCIS Submission (I), Summary Punkt 2.1.3.

791 Tony Hutchings, UK National Hi-Tech Crime Project Team, zitiert in Kommission, Cybercrime-Anhörung (I); Kronqvist, Leiter der IT-Kriminalitätsgruppe der nationalen schwedischen Strafverfolgungsbehörde, Cybercrime-Anhörung; Graf, Jürgen (Generalbundesanwalt), zitiert bei Neumann, Andreas: Internet Service Provider im Spannungsfeld zwischen Strafverfolgung und Datenschutz, Bericht von der Veranstaltung in Bonn am 26./27.02.2002, www.artikel5.de/-artikel/ecoveranstaltung2002.html; NCIS Submission (I), Summary Punkt 2.1.3.; a.A. Schmitz, MMR 2003, 214 (216): keine generell schlechtere Beweislage.

geheim durchführen. Das Auge des Gesetzes ist offline nicht überall, so dass es keinen Grund gibt, warum dies online anders sein müsste[792].

Schon die Annahme, dass die Wahrnehmung staatlicher Aufgaben unter den besonderen Umständen der Telekommunikationsnetze leide, ist kritisch zu hinterfragen. In Fällen, in denen Telekommunikationsnetze eine ordnungsgemäße Aufgabenwahrnehmung nur erschweren (etwa durch die Erforderlichkeit qualifizierten Personals oder sonstiger Mittel wie Zeit und Geld), in denen aber auch ohne einen Zugriff auf vorratsgespeicherte Kommunikationsdaten erfolgreich eingeschritten werden kann, rechtfertigt die bloße Erleichterung der Aufgabenwahrnehmung in Anbetracht der hohen Eingriffsintensität keine generelle Vorratsspeicherung[793]. In Fällen, in denen die Aufgabenwahrnehmung mangels Kommunikationsdaten vereitelt wird, ist es nicht sicher, ob eine Vorratsspeicherung tatsächlich weiter geholfen hätte. Auch im Rahmen des Art. 3 Abs. 1 GG ist zu berücksichtigen, dass eine Vorratsspeicherung von Telekommunikationsdaten nur in begrenztem Maße von Nutzen ist[794].

Im Übrigen darf nicht außer Acht gelassen werden, dass Telekommunikationsnetze den Behörden die Wahrnehmung ihrer Aufgaben ungemein erleichtern[795]. Vor 100 Jahren hatten die Eingriffsbehörden keine Chance, verdächtige Personen so unbemerkt, kostengünstig und personalsparend zu überwachen wie heute. Im Vergleich zu den Möglichkeiten der Telekommunikationsüberwachung ist eine Überwachung von unmittelbarer Kommunikation erheblich schwerer. Was die Beweislage angeht, so werden Telekommunikationsdaten, wenn sie vorliegen und soweit ihr Informationsgehalt reicht, meist aussagekräftiger und zuverlässiger sein als Zeugenaussagen oder andere Beweismittel für räumlich-unmittelbare Kommunikation. Der Nutzen des staatlichen Zugriffs auf Kommunikationsdaten wird zudem durch eine generelle Vorratsspeicherung unterminiert, weil dieses Verfahren Straftätern eindringlich ins Bewusstsein ruft, die Benutzung von Telekommunikationsnetzen zu meiden. Letztlich gefährdet eine Vorratsspeicherung von Telekommunikationsdaten dadurch den Erfolg der bisher bestehenden Überwachungsbefugnisse im Einzelfall[796].

Insgesamt ist unklar, ob die staatliche Aufgabenwahrnehmung durch die Möglichkeit der Kommunikation über Telekommunikationsnetze tatsächlich erschwert wird. Ohnehin kann richtigerweise nicht schon die abstrakte Erschwerung der staatlichen Aufgabenwahrnehmung eine Ungleichbehandlung der Telekommunikationsnutzung rechtfertigen, sondern erst erhöhte, dadurch verursachte Gefahren für konkrete Rechtsgüter[797]. Auf dem Gebiet der Strafverfolgung stellt sich damit immer noch das Problem, dass eine gewisse Steigerung der Aufklärungsrate infolge einer generellen Kommunikationsdatenspeicherung keine merkliche Senkung des Kriminalitätsniveaus und damit keinen nennenswert verbesserten Rechtsgüterschutz erwarten lässt[798].

(5) Erhöhtes Gefahrenpotenzial durch besondere Eigenschaften der Telekommunikation als Rechtfertigungsgrund

Zur Rechtfertigung einer Ungleichbehandlung der Telekommunikation könnte weiter vorgebracht werden, dass die Kommunikation über Telekommunikationsnetze größere Gefahren für Rechtsgüter mit sich bringe als die räumlich-unmittelbare Kommunikation. Ob dies der Fall ist, ist umstritten[799] und empirisch noch nicht untersucht worden. Für eine höhere Gefährlichkeit der Telekommunikation sprechen ihre besonderen Eigenschaften, die in bestimmten Fällen die Begehung von Straftaten begünstigen können[800]. Telekommunikationsnetze erleichtern den Austausch von Informationen und ermöglichen diesen kostengünstig, einfach, schnell, vertraulich und über weite Entfernungen – auch Ländergrenzen – hinweg.

Dass die besonderen Eigenschaften der Telekommunikation die Gefährdung von Rechtsgütern in einzelnen Fällen begünstigen, bedeutet indes nicht zwangsläufig, dass sie dies auch in höherem Maße

792 Artikel-29-Gruppe der EU, Anonymität, 7.

793 Vgl. allgemein J/P7-Jarass, Art. 3, Rn. 16 a.E.; für die geheime Erhebung von Daten L/D3-Bäumler, J 37.

794 Seiten 43-55.

795 Breyer, Vorratsspeicherung, 27 f.; siehe auch Seite 62 oben; vgl. ferner MDG, Entwurf für Schlussfolgerungen des Rates zur Informationstechnologie (I), 3: „Der Rat der Europäischen Union [...] stellt fest, dass die beträchtliche Zunahme der Möglichkeiten elektronischer Kommunikation dazu geführt hat, dass Daten über die Verwendung elektronischer Kommunikation heutzutage ein besonders wichtiges und hilfreiches Mittel bei der Aufklärung und Verfolgung von Straftaten, insbesondere von organisierter Kriminalität, darstellen“.

796 Ausführlich hierzu Seiten 77-78.

797 Seiten 34 ff.

798 Seiten 43-55.

799 Vgl. etwa Weßlau, ZStW 113 (2001), 681 (703), wonach weder Internet-Provider noch Internet-Nutzer gefahrenträchtig handelten; ebenso Bäumler, DuD 2001, 348 (349) und Werner, Befugnisse der Sicherheitsbehörden, 51 für das Telekommunikationsnetz; meist unausgesprochen a.A. sind die Vertreter der Eingriffsbehörden.

800 Sieber, COMCRIME-Studie (I), 60.

tun als die Kommunikation in räumlicher Gegenwart der Beteiligten[801]. Bei der Untersuchung dieser Frage ist richtigerweise zu berücksichtigen, wie viele Kommunikationsvorgänge insgesamt über Telekommunikationsnetze oder räumlich-unmittelbar abgewickelt werden. Nur auf diese Weise ist feststellbar, inwieweit höhere Gefahren infolge einer Kommunikationsweise (Telekommunikation oder räumlich-unmittelbare Kommunikation) auf die Eigenart der jeweiligen Kommunikationsweise und nicht bloß auf das Maß an Nutzung der jeweiligen Kommunikationsform zurückzuführen sind. Zu vergleichen ist also das relative Maß an Rechtsgutsgefährdung. Es ist darauf abzustellen, in welchem Maß der durchschnittliche Kommunikationsvorgang Rechtsgüter gefährdet.

Dies hat unter anderem zur Folge, dass die absolut steigende Zahl der Fälle von Netzkriminalität im weiteren Sinn in Verhältnis zu setzen ist zu dem Maß, in dem Telekommunikationsnetze insgesamt genutzt werden. Die bisher vorliegenden Zahlen zur Computerkriminalität im engeren Sinne etwa sind in den vergangenen Jahren weit weniger stark gestiegen als die Internetnutzung insgesamt[802]. Zu berücksichtigen ist auch, in welchem Maße es jeweils zur Gefährdung von Rechtsgütern kommt. Bisher existieren keine Statistiken oder Untersuchungen über das Ausmaß der Schäden, die durch die Inanspruchnahme von Telekommunikationsnetzen durch Straftäter entstehen[803]. Nach Ermittlung des relativen Gefahrenpotenzials der Telekommunikationsnetze ist dieses mit der Situation im Bereich der räumlich-unmittelbaren Kommunikation zu vergleichen. Zahlen insoweit liegen bisher nicht vor. Die Behauptung, dass Telekommunikation Rechtsgüter in höherem Maße gefährdete als räumlich-unmittelbare Kommunikation, stellt aus diesem Grund lediglich eine Hypothese dar, deren Richtigkeit bisher noch nicht untersucht worden ist.

Die von der Polizeistatistik ausgewiesenen Fallzahlen der allgemeinen Kriminalität sind in den letzten Jahren ungefähr stabil geblieben, so dass sich nicht feststellen lässt, dass der Einzug der Telekommunikationsnetze in das tägliche Leben insgesamt zu mehr Straftaten geführt hat. Unter der Voraussetzung, dass die Entwicklung der Polizeistatistik der tatsächlichen Kriminalitätsentwicklung entspricht, ist dies ein Indiz für die These, dass mittels Telekommunikation begangene Straftaten ohne die Möglichkeiten der Telekommunikation mittels unmittelbarer Kommunikation begangen würden, dass die Telekommunikationsnetze also nur zu einer Kriminalitätsverlagerung geführt haben[804].

Zwar können Telekommunikationsnetze durchaus als „gefährliche Werkzeuge“ oder Hilfsmittel bei der Gefährdung von Rechtsgütern eingesetzt werden. Allerdings kann prima facie und ohne nähere Untersuchungen nicht davon ausgegangen werden, dass die Telekommunikation zu größeren Schäden führt oder mit weitergehenden Gefahren verbunden ist als die unmittelbare Kommunikation. In Anbetracht der Tatsache, dass sich Telekommunikation leichter überwachen lässt, ist auch das Gegenteil denkbar. In diesem Fall aber sind weitergehende Überwachungsmaßnahmen als im Bereich der unmittelbaren Kommunikation nicht gerechtfertigt.

(6) Höherer Nutzen der Telekommunikationsüberwachung als Rechtfertigungsgrund

Weiterhin könnte eine Vorratsspeicherung allein von Telekommunikationsdaten dadurch gerechtfertigt sein, dass die Kenntnis der näheren Umstände von Telekommunikationsvorgängen typischerweise von größerem Nutzen für den Rechtsgüterschutz sein könnte als die Kenntnis der näheren Umstände von unmittelbaren Kommunikationsvorgängen. Beispielsweise lässt sich denken, dass Straftäter sensible Informationen über geplante oder abgeschlossene Straftaten öfter telefonisch austauschen könnten als im unmittelbaren Gespräch. Diese Annahme erscheint allerdings unzutreffend. Straftäter werden sich heutzutage regelmäßig des Instruments der Telekommunikationsüberwachung bewusst sein und die unmittelbare Kommunikation einem Einsatz von Telekommunikation daher wann immer möglich vorziehen. Auch sonst ist nicht ersichtlich, dass die Kenntnis der näheren Umstände von Telekommunikationsvorgängen typischerweise einen größeren Nutzen für den Rechtsgüterschutz aufweist als die Kenntnis der Umstände von unmittelbaren Kommunikationsvorgängen. Ein Rechtfertigungsgrund kann hierin daher nicht erblickt werden.

(7) Unterschiedliche Schutzwürdigkeit als Rechtfertigungsgrund

Als Rechtfertigungsgrund kommt schließlich in Betracht, dass die Umstände unmittelbarer Kommunikation schutzwürdiger sein könnten als die Umstände von Telekommunikation. Für diese These könnte angeführt werden, dass sich Menschen bei Einsatz von Telekommunikationsnetzen ihrer Kommunikation willentlich entäußern und dass sie dementsprechend mit einem höheren Maß an Überwachung rechnen müssten als im Fall unmittelbarer Kommunikation. Wie bereits gezeigt, kann die bloße

801 In diese Richtung allerdings Sieber, COMCRIME-Studie (I), 61: „computer crime and the Internet have become especially attractive for organised crime groups“.

802 Seite 39.

803 Seite 38.

804 In diesem Sinne Pfitzmann, Andreas in Bundestag, Öffentliche Anhörung zum Thema Cyber-Crime/TKÜV (I), 52.

Tatsache, dass sich Telekommunikation einfacher überwachen lässt, zur Rechtfertigung einer generellen Kommunikationsdatenspeicherung aber nicht genügen[805]. Ebenso wenig kann daraus eine verminderte Schutzwürdigkeit von Telekommunikation hergeleitet werden. Wenn Menschen miteinander telekommunizieren, vertrauen sie typischerweise darauf, ebenso ungestört zu sein wie im Fall unmittelbarer Kommunikation. Hinzu kommt, dass heutzutage in vielen Situationen keine Möglichkeit unmittelbarer Kommunikation mehr besteht[806]. Dieser Umstand darf nicht zulasten der Betroffenen gehen.

Für eine verminderte Schutzwürdigkeit von Telekommunikation könnte weiterhin angeführt werden, dass vertrauliche Gespräche zumeist in Wohnungen geführt würden, dass Telekommunikation den Bereich einer Wohnung dagegen stets verlässt. Auch diese Tatsache scheint indes nicht geeignet, die Schutzwürdigkeit von Telekommunikation zu reduzieren[807]. Die Funktion eines Gespräches innerhalb einer Wohnung unterscheidet sich nicht von der Funktion eines Telefongesprächs zwischen zwei Wohnungen.

Die hohe Sensibilität und Aussagekraft von Telekommunikationsdaten wurde bereits ausführlich dargestellt[808]. Es sind keine Anhaltspunkte dafür ersichtlich, dass Telekommunikation typischerweise weniger sensibel ist als räumlich-unmittelbare Kommunikation. Dementsprechend kann von einer verminderten Schutzwürdigkeit von Telekommunikation nicht ausgegangen werden.

(8) Abwägung und Ergebnis

Festzuhalten ist, dass sich eine generelle Vorratsspeicherung allein von Telekommunikationsdaten nur dann rechtfertigen lässt, wenn der durchschnittliche Telekommunikationsvorgang Rechtsgüter in erheblich höherem Maß gefährdet als der typische räumlich-unmittelbare Kommunikationsvorgang. Als Unterfall der Gefährdung von Rechtsgütern ist es dabei anzusehen, wenn der Schutz von Rechtsgütern durch die Eingriffsbehörden vereitelt wird, weil diese keine Kenntnis von den Umständen eines Kommunikationsvorgangs haben.

Ob die Kommunikation über Telekommunikationsnetze Rechtsgüter tatsächlich in überdurchschnittlichem Maße gefährdet, ist unbekannt. Bei der Einschätzung dieser Tatsache kommt dem Gesetzgeber ein gewisser Spielraum zu, dessen Ausmaß sich nach den oben diskutierten Kriterien bestimmt[809]. Wegen der hohen Eingriffsintensität einer generellen Kommunikationsdatenspeicherung ist zu verlangen, dass der Gesetzgeber eine vertretbare Entscheidung trifft[810] und die ihm zugänglichen Erkenntnisquellen vor der Einführung einer solchen Maßnahme ausschöpft[811], etwa durch Einholung einer wissenschaftlichen Vergleichsstudie. Es liegt keine besondere Dringlichkeitssituation vor, in der von der vorherigen Analyse der maßgeblichen Tatsachen abgesehen werden könnte[812]. Ebenso wenig verspricht die Einführung einer Vorratsspeicherung von Telekommunikationsdaten einen Erkenntnisgewinn bezüglich des Maßes an Rechtsgutsgefährdung durch Telekommunikation oder räumlich-unmittelbare Kommunikation, so dass sich eine solche Maßnahme auch nicht als notwendiges Experiment rechtfertigen lässt[813]. Da der Gesetzgeber ausreichende Aufklärungsmaßnahmen versäumt hat, verstoßen die §§ 110a, 110b TKG gegen Art. 3 Abs. 1 GG.

Auf der Basis des gegenwärtigen Erkenntnisstandes ist nicht ersichtlich, dass der durchschnittliche, über Telekommunikationsnetze abgewickelte Kommunikationsvorgang Rechtsgüter in höherem Maße gefährdet als der typische räumlich-unmittelbare Kommunikationsvorgang. Wie oben gezeigt[814], legt die leichtere Überwachbarkeit der Telekommunikation eher den umgekehrten Schluss nahe. Ohne entsprechende empirische Befunde ist die Unterstellung einer besonderen Rechtsgutsgefährdung durch menschliche Kommunikation über Telekommunikationsnetze angesichts dessen unvertretbar. Ausgehend von den derzeit vorliegenden Erkenntnissen ist die Einführung einer Vorratsspeicherung von Telekommunikationsdaten daher mit Art. 3 Abs. 1 GG unvereinbar.

bb) Massenkommunikation

Telekommunikationsnetze stellen nicht nur ein Medium für Individual- sondern auch für Massenkommunikation dar. Für das Angebot und die Nutzung von Informationen, die an eine unbestimmte

805 Seite 101.
806 Seite 100.
807 Vgl. auch Breyer, Vorratsspeicherung, 118 f.
808 Seiten 61-79.
809 Seiten 31-32.
810 Seiten 33-34.
811 Seite 81.
812 Seite 81.
813 Vgl. dazu Seiten 32-33.
814 Seite 103.

Vielzahl von Personen gerichtet sind, eignet sich insbesondere das Internet. Eine generelle Vorratsspeicherung von Telekommunikationsdaten in Verbindung mit der verbreiteten freiwilligen Protokollierung des Internetnutzungsverhaltens führt dazu, dass die Nutzung telekommunikativer Informationsangebote ihren Umständen nach festgehalten wird, während die räumlich-unmittelbare Nutzung traditioneller Massenmedien (z.B. Zeitschriften, Bücher, Fernsehen) überwachungsfrei bleibt. Wegen der Frage, ob diese Ungleichbehandlung gerechtfertigt ist, kann weitgehend auf die obigen Ausführungen zur Individualkommunikation verwiesen werden[815].

Eine stärkere Überwachung der Massenkommunikation über Telekommunikationsnetze ist nur dann gerechtfertigt, wenn aus dieser – gemessen an der Gesamtzahl von Nutzungsvorgängen – überproportional hohe Gefahren erwachsen. Vergleichsmaßstab ist das Gefahrenpotenzial von räumlich-unmittelbarer Massenkommunikation. Für ein höheres Gefahrenpotenzial der Telekommunikationsnetze könnte sprechen, dass Telekommunikationsnetze und insbesondere das Internet nicht selten zum Angebot und zur Nutzung illegaler Informationen eingesetzt werden und dass sich insbesondere das Internet hierzu besser eignet als Printmedien und andere traditionelle Massenmedien. Telekommunikationsnetze erleichtern aber andererseits auch das Angebot und die Nutzung legaler Informationen. Speziell das Internet wird in hohem Maße zur Verbreitung legaler und sogar nützlicher und politisch wichtiger Informationen genutzt[816]. Aus diesem Grund können steigende Zahlen hinsichtlich der Verbreitung illegaler Informationen über das Internet dessen stärkere Überwachung für sich genommen nicht rechtfertigen. Zu berücksichtigen ist stets die Entwicklung des gesamten Telekommunikationsaufkommens und die Situation im Bereich der traditionellen Massenmedien.

Ob über Telekommunikationsnetze abgewickelte Massenkommunikation prozentual öfter illegalen Zwecken dient als traditionelle Massenkommunikation, ist bisher noch nicht empirisch untersucht worden, obwohl dies in gewissem Maße möglich wäre. Beispielsweise könnten die Erkenntnisse des Bundesamts für Verfassungsschutz über die Verbreitung verfassungsfeindlicher Druckschriften mit den Angaben von Internet-Suchmaschinen über die Verbreitung solcher Angebote im Internet verglichen werden. Angesichts der unüberschaubaren Vielzahl legaler Angebote im Internet ist es nicht vertretbar, über Telekommunikationsnetze verbreitete Massenkommunikation ohne stichhaltige, dahin gehende Anhaltspunkte als schadensträchtiger anzusehen als die traditionelle Massenkommunikation. Aus diesem Grund ist die Einführung einer Vorratsspeicherung von Telekommunikationsdaten auf der Grundlage des gegenwärtigen Kenntnisstandes mit Art. 3 Abs. 1 GG unvereinbar.

cc) Computerdaten

Außer als Medium für die zwischenmenschliche Kommunikation können Telekommunikationsnetze auch zur Übertragung von Computerdaten (z.B. Musik, Software) eingesetzt werden. Technisch geschieht dies, indem fremde Computer (so genannte Server) zur Übermittlung von Daten angewiesen werden oder indem Daten an diese Computer übermittelt werden. Auch im Bereich der Netzkriminalität im engeren Sinne werden Telekommunikationsnetze als Mittel zur Steuerung anderer Computersysteme eingesetzt.

Eine generelle Vorratsspeicherung von Telekommunikationsdaten zeichnet nur die telekommunikative Computerbenutzung ihren Umständen nach auf, nicht dagegen die unmittelbare Benutzung eines Computers. Als unmittelbare Computerbenutzung ist dabei auch der Zugriff mittels selbst betriebener Netzwerke (z.B. Unternehmensnetzwerke) anzusehen, der keine Telekommunikation im Sinne des TKG darstellt. Der gemeinsame Oberbegriff liegt in der Benutzung von Computern, so dass die Vergleichbarkeit der Sachverhalte gegeben ist. Da im Fall einer Vorratsspeicherung von Telekommunikationsdaten nur die telekommunikative Computerbenutzung ihren Umständen nach aufgezeichnet wird, werden diejenigen Personen benachteiligt, die Computer mittels Telekommunikation und nicht unmittelbar benutzen. Ein Eingriff in das Grundrecht dieser Personen aus Art. 3 Abs. 1 GG liegt damit vor.

Fraglich ist, welcher Maßstab bei der Rechtfertigungsprüfung anzuwenden ist. Wie im Bereich der zwischenmenschlichen Kommunikation[817] gibt es viele Menschen und Berufsgruppen, die auf die telekommunikative Computerbenutzung angewiesen sind, ohne zumutbarerweise auf die unmittelbare Computerbenutzung ausweichen zu können. Gerade das Internet ermöglicht die Nutzung von Computern in der ganzen Welt, zu denen kein unmittelbarer Zugang besteht. Im Berufsleben sind auch Direktverbindungen von Berufstätigen mit dem Computer ihres Arbeitgebers üblich, um Daten auszutauschen. Da viele Berufe die räumliche Trennung von dem jeweiligen Arbeitgeber mit sich bringen, ist Telekommunikation in diesen Bereichen unersetzlich. Eine generelle Kommunikationsdatenspeiche-

815 Seiten 101-104.
816 Seite 98.
817 Seite 100.

rung stellt darüber hinaus einen schweren Eingriff in verschiedene Freiheitsgrundrechte dar[818], was ebenfalls für eine strikte Prüfung spricht. Insgesamt ergibt sich wiederum[819], dass eine Verhältnismäßigkeitsprüfung durchzuführen ist.

Auf dem Gebiet der Computerbenutzung kann nicht geltend gemacht werden, dass eine Aufzeichnung und Vorhaltung von Daten über die näheren Umstände der unmittelbaren Computerbenutzung nicht realisierbar sei. In vielen Unternehmen gibt es bereits Mechanismen, um die Computernutzung durch Mitarbeiter zu protokollieren. Diese Verfahren könnten auf sämtliche Computer ausgedehnt werden. Dass eine Vorratsspeicherung im Bereich der Benutzung einzelner Computer mit höherem Aufwand verbunden wäre als im Bereich der Telekommunikation, kann entsprechend den obigen Ausführungen[820] auch hier nicht die gravierende Ungleichbehandlung rechtfertigen, die mit einer generellen Vorratsspeicherung allein von Telekommunikationsdaten verbunden ist.

Als Rechtfertigungsgrund kommt weiterhin in Betracht, dass von der telekommunikativen Computerbenutzung ein höheres Gefährdungspotenzial ausgehen könnte als von der unmittelbaren Computerbenutzung. Ob dies der Fall ist, ist bisher nicht bekannt. Einerseits lassen sich beispielsweise Computerangriffe über das Internet über weitere Entfernungen hinweg vornehmen als wenn unmittelbar auf einen Computer des Opfers zugegriffen werden müsste. Zudem sind Computer nur für einen eingeschränkten Personenkreis unmittelbar zugänglich. Andererseits wurde bereits ausgeführt, dass ein großer Teil der durch Netzkriminalität im engeren Sinne verursachten Schäden auf Mitarbeiter der betroffenen Unternehmen zurückzuführen ist und dass Telekommunikationsnetze insoweit nur selten zum Einsatz kommen[821]. Wo die Möglichkeit eines unmittelbaren Computerzugriffs besteht, werden Straftäter die Benutzung von Telekommunikationsnetzen schon deshalb meiden, weil ihnen regelmäßig bekannt sein wird, dass dabei Kommunikationsdaten anfallen können. Ohne entsprechende empirische Erkenntnisse kann mithin nicht unterstellt werden, dass der typische Telekommunikationsvorgang öfter dem Angriff auf Computersysteme dient als die durchschnittliche unmittelbare Computernutzung. Es spricht vielmehr einiges für die Annahme, dass die unmittelbare wie die telekommunikative Benutzung von Computern gleichermaßen ganz überwiegend zu legitimen Zwecken und nur äußerst selten zum Zweck von Computerangriffen erfolgt.

Die Ausnahme der unmittelbaren Computerbenutzung von einer Vorratsspeicherungspflicht könnte ferner damit gerechtfertigt werden, dass es jeder Betreiber eines Computersystems in der Hand habe, den unmittelbaren Zugriff auf sein System zu unterbinden oder zu kontrollieren, dass er den Zugriff mittels Telekommunikationsnetzen dagegen nicht in gleichem Maße kontrollieren könne. Gegen diese Argumentation ist einzuwenden, dass sich der Personenkreis, der unmittelbaren Zugriff auf Computersysteme hat, zwar einschränken lässt (z.B. durch Eingangskontrollen), dass es aber auch im Bereich der Telekommunikationsnetze Mechanismen gibt, welche das sichere Authentifizieren von Benutzern ermöglichen. Computerkriminalität im engeren Sinne wird zudem oft von Mitarbeitern des Geschädigten begangen, die legalen räumlichen Zugang zu den angegriffenen Systemen haben. Nicht selten sind diese Personen technisch äußerst versiert und können dadurch Schutzmechanismen umgehen. Oft wird Computerkriminalität im engeren Sinne auch gerade von denjenigen Personen begangen, die für die Sicherheit der angegriffenen Systeme sorgen sollen (Administratoren). Im Gegensatz dazu gestaltet sich der Angriff auf Computersysteme mittels Telekommunikationsnetzen regelmäßig schwieriger. Der Betreiber hat es insoweit in hohem Maße in der Hand, Computerangriffen durch technische Maßnahmen vorzubeugen. Wenn die eingesetzte Software regelmäßig aktualisiert wird, lassen sich Schäden infolge von „Hacking“ weitgehend ausschließen. Jedenfalls lässt sich nicht ohne genauere Untersuchungen behaupten, dass der Schutz vor unmittelbaren Zugriffen einfacher möglich sei als der Schutz vor Angriffen mittels Telekommunikationsnetzen.

In Anbetracht der insoweit bestehenden Unsicherheitsfaktoren bemisst sich der Einschätzungsspielraum des Gesetzgebers nach den oben diskutierten Kriterien[822]. Wegen der Eingriffsintensität einer Vorratsspeicherung von Kommunikationsdaten ist zu verlangen, dass der Gesetzgeber eine vertretbare Entscheidung trifft und die für die Beurteilung der Verfassungsmäßigkeit relevanten Tatsachen zuvor möglichst vollständig ermittelt[823]. Die Einführung einer auf den Telekommunikationsbereich beschränkten Vorratsspeicherung ist nur dann eine vertretbare Entscheidung des Gesetzgebers, wenn er sich zuvor durch Aufklärung der Sachlage versichert, dass von der telekommunikativen Computerbe-

818 Seite 100.
819 Vgl. schon Seite 100.
820 Seite 101.
821 Seite 42.
822 Seiten 31-32.
823 Seite 104.

nutzung überproportional größere Gefahren ausgehen. Eine entsprechende Aufklärung hat der Gesetzgeber vor dem Beschluss des angegriffenen Artikels 2 jedoch unterlassen.

Auf der Grundlage der bisherigen Kenntnisse kann von größeren Gefahren infolge von telekommunikativer Computerbenutzung – wie gezeigt – nicht ausgegangen werden, so dass derzeit keine Gründe von solcher Art und solchem Gewicht ersichtlich sind, dass sie eine Ungleichbehandlung der telekommunikativen gegenüber der unmittelbaren Computerbenutzung rechtfertigen könnten. Aus diesem Grund ist die Einführung einer Vorratsspeicherung von Telekommunikationsdaten gegenwärtig mit Art. 3 Abs. 1 GG unvereinbar.

b) Ungleichbehandlung der Telekommunikation gegenüber dem Postwesen

aa) Ungleichbehandlung des distanzierten Informationsaustausches per Telekommunikation gegenüber dem distanzierten Austausch verkörperter Informationen

Des Weiteren ist es mit Art. 3 Abs. 1 GG unvereinbar, eine Pflicht zur Vorratsspeicherung von Kommunikationsdaten nur im Telekommunikationsbereich vorzusehen, nicht aber im Postbereich. Zu vergleichen ist die Übermittlung von Informationen mittels Telekommunikation mit der postalischen Übermittlung von Informationen. Gemeinsamer Oberbegriff ist die räumlich distanzierte Übermittlung von Informationen, so dass die Vergleichbarkeit der Sachverhalte gegeben ist. Dies gilt auch im Hinblick auf computerlesbare Daten, weil auch diese auf Datenträgern postalisch versandt werden können. Durch den intensiven Eingriff in verschiedene Freiheitsgrundrechte[824] werden die Telekommunikationsnutzer gegenüber den Nutzern von Postdienstleistungen benachteiligt, weil die näheren Umstände der Informationsübermittlung nur im ersten Fall festgehalten werden. Darin liegt ein Eingriff in das Grundrecht der Telekommunikationsnutzer aus Art. 3 Abs. 1 GG.

Was den Rechtfertigungsmaßstab anbelangt, so gibt es viele Menschen und Berufsgruppen, die typischerweise auf die Möglichkeit des telekommunikativen Informationsaustausches angewiesen sind, ohne zumutbarerweise auf die Post ausweichen zu können. Dies gilt besonders für Arbeitnehmer und Selbstständige, die sich bei ihrer Tätigkeit nach äußeren Zwängen richten müssen. Zu dieser Gruppe gehören auch Journalisten, deren zum Teil vertrauliche Arbeit in unserer freiheitlichen Demokratie besonders wichtig ist. Dasselbe gilt etwa für Menschenrechtsorganisationen. Auch außerhalb des beruflichen Bereichs wird im Zeitalter der Informationsgesellschaft der körperliche Informationsaustausch immer mehr verdrängt. Während es beispielsweise Bürger- und Sorgentelefone gibt, die Bürgern eine fachkundige Beratung in Notlagen bieten, ist die Nutzung solcher Angebote per Post meist nicht möglich. Ähnlich verhält es sich mit dem Internet, dessen reichhaltiges Informationsangebot sich durch keine Bibliothek mit Fernleihemöglichkeit ersetzen lässt. Nimmt man die hohe Eingriffsintensität einer Vorratsspeicherung von Telekommunikationsdaten hinzu, dann wiegt die Ungleichbehandlung gegenüber der Postbenutzung so schwer, dass wiederum[825] eine Verhältnismäßigkeitsprüfung erforderlich ist.

Im Unterschied zum unmittelbaren Informationsaustausch kann auf dem Gebiet der Postdienstleistungen nicht geltend gemacht werden, dass eine Aufzeichnung und Vorhaltung von Kommunikationsdaten nicht realisierbar sei. Auch dass der Absender auf postalischen Sendungen bisher nicht angegeben werden muss, hindert die Aufzeichnung von Kommunikationsdaten nicht, weil eine Identifizierungspflicht eingeführt werden könnte. Im Übrigen ist auch im Telekommunikationsbereich stets nur der Anschlussinhaber, nicht aber der jeweilige Benutzer des Anschlusses identifizierbar. Dass eine Vorratsspeicherung im Postbereich mit höherem Aufwand verbunden sein könnte als im Bereich der Telekommunikation, genügt nach dem oben Gesagten[826] nicht, um die gravierende Ungleichbehandlung zu rechtfertigen, zumal der Aufwand einer Vorratsspeicherung im Postbereich ungleich geringer wäre als im Bereich unmittelbarer Kommunikation.

Als Rechtfertigungsgrund kommt weiterhin in Betracht, dass von dem telekommunikativen Informationsaustausch ein höheres Gefahrenpotenzial ausgehen könnte als von dem Informationsaustausch per Post. Ob dies der Fall ist, ist unbekannt und lässt sich empirisch wohl nur im Wege von repräsentativen Untersuchungen feststellen. Fest steht zwar, dass Telekommunikationsnetze im Vergleich zur Nutzung der Post den Austausch von Informationen allgemein erleichtern und diesen kostengünstig, einfach, schnell, vertraulich und über weite Entfernungen – auch Ländergrenzen – hinweg ermöglichen. Allerdings ist auch dem Postverkehr ein spezifisches Gefährdungspotenzial zueigen. Weil bei dem postalischen Verkehr kein Absender angegeben werden muss oder die Absenderangabe nicht überprüft wird, eröffnet die Post zusätzliche Möglichkeiten des konspirativen Informationsaustausches

824 Seite 100.
825 Vgl. schon Seite 100.
826 Seite 101.

zwischen Straftätern. Ebenso wie im Telekommunikationsbereich lässt sich auch beim postalischen Informationsaustausch jegliche Kontrolle unterbinden, indem man verschlüsselte Informationen versendet. Zudem kann der Inhalt von Postsendungen schon des hohen Aufwandes wegen nicht in nennenswertem Maße auf einschlägige Hinweise kontrolliert werden. Damit kann sich die Post als Ausweichmöglichkeit für Straftäter anbieten, die ihre Kommunikation nicht mehr konspirativ über Telekommunikationsnetze abwickeln können, weil in diesem Bereich eine generelle Kommunikationsdatenspeicherung eingeführt wurde.

Summa summarum lassen die generellen Merkmale von Telekommunikationsnetzen nicht mit hinreichender Sicherheit auf ein höheres Gefahrenpotenzial der Telekommunikation schließen als es der Austausch von Informationen per Post aufweist. Entsprechend der obigen Feststellungen[827] ist der Gesetzgeber auch in Bezug auf die Frage, ob von dem telekommunikativen Informationsaustausch größere Gefahren ausgehen als von dem Informationsaustausch per Post, gemäß Art. 3 Abs. 1 GG zur Aufklärung verpflichtet, bevor er eine Vorratsspeicherung allein von Telekommunikationsdaten beschließen darf. Nach bisherigen Erkenntnissen existieren keine Gründe von solcher Art und solchem Gewicht, dass sie eine Diskriminierung der Telekommunikationsbenutzung gegenüber der Postbenutzung im Wege einer generellen Vorratsspeicherung nur von Telekommunikationsdaten rechtfertigen könnten.

bb) Ungleichbehandlung von Telekommunikationsunternehmen gegenüber Postunternehmen

Statt aus der Nutzerperspektive lässt sich der Vergleich von Telekommunikation und Post auch aus Sicht der befördernden Unternehmen anstellen. Eine Pflicht zur generellen Vorratsspeicherung von Telekommunikationsdaten trifft nur Telekommunikations-, nicht aber Postunternehmen, so dass eine Ungleichbehandlung erfolgt. Beide Arten von Unternehmen unterfallen dem Oberbegriff der beruflichen Übermittler von Informationen, so dass sie vergleichbar sind. Von der Ungleichbehandlung nachteilig betroffen sind die Telekommunikationsunternehmen, so dass eine Speicherungspflicht nur für Telekommunikationsdaten einen Eingriff in das Grundrecht der Telekommunikationsunternehmen aus Art. 3 Abs. 1 GG darstellt.

Was den Rechtfertigungsmaßstab angeht, so knüpft eine generelle Kommunikationsdatenspeicherung eindeutig an Personengruppen – nämlich an den Beruf des Telekommunikationsdienstleisters – und nicht nur an Sachverhalte an. Wie gezeigt, greift die Kommunikationsdatenspeicherungspflicht auch intensiv in das Grundrecht der betroffenen Unternehmen aus Art. 12 Abs. 1 GG ein, wenn keine umfassende Kostenerstattung vorgesehen wird[828]. Es ist daher eine Verhältnismäßigkeitsprüfung vorzunehmen.

Wie gezeigt, gibt es nach derzeitigen Erkenntnissen keine hinreichenden Gründe für die Annahme, dass mit der postalischen Vermittlung von Informationen typischerweise geringere Gefahren verbunden seien als mit der telekommunikativen Informationsübermittlung[829]. Weil damit gegenwärtig nicht ersichtlich ist, dass die mit einer Kommunikationsdatenspeicherungspflicht verbundene Benachteiligung von Telekommunikationsunternehmen gerechtfertigt ist, ist eine solche Maßnahme mit Art. 3 Abs. 1 GG unvereinbar.

c) Ungleichbehandlung der Telekommunikation gegenüber sonstigen Leistungen

aa) Ungleichbehandlung der Inanspruchnahme von Telekommunikation gegenüber der Inanspruchnahme sonstiger Leistungen

Es ist nicht gerechtfertigt, nur im Telekommunikationsbereich eine Vorratsspeicherung zu staatlichen Zwecken vorzusehen, nicht aber für Daten über die Inanspruchnahme sonstiger Leistungen.

Eine generelle Kommunikationsdatenspeicherung führt dazu, dass die Inanspruchnahme von Telekommunikation anders behandelt wird als die Inanspruchnahme sonstiger Leistungen, bei deren Erbringung Daten anfallen oder gespeichert werden können, die für die Gefahrenabwehr oder Strafverfolgung nützlich sein können. Allgemein existiert nämlich keine Pflicht zur Vorhaltung gefahrenabwehr- und strafverfolgungsrelevanter Daten zu staatlichen Zwecken. Gemeinsamer Oberbegriff der genannten Sachverhalte ist die Inanspruchnahme von Leistungen, bei deren Erbringung Daten anfallen oder gespeichert werden können, die für die Gefahrenabwehr oder Strafverfolgung nützlich sein können. Eine generelle Vorratsspeicherung von Telekommunikationsdaten benachteiligt Telekommunika-

827 Seite 104.
828 Seiten 89-90.
829 Seiten 107-108.

tionsbenutzer unter anderem gegenüber Kunden von Banken und Fluggesellschaften, so dass ein Eingriff in das Recht der Telekommunikationsnutzer aus Art. 3 Abs. 1 GG vorliegt.

Bezüglich der Anforderungen an eine verfassungsmäßige Rechtfertigung dieser Ungleichbehandlung ist zunächst festzuhalten, dass sich eine Ungleichbehandlung von Sachverhalten ohne unmittelbaren Personenbezug annehmen ließe. Allerdings gilt auch hier wieder, dass man die Benutzung von Telekommunikationsnetzen heutzutage kaum vermeiden kann und dass bestimmte Personengruppen typischerweise besonders darauf angewiesen sind, insbesondere bestimmte Berufsgruppen[830]. Außerdem ist eine generelle Vorratsspeicherung von Telekommunikationsdaten mit einem schwerwiegenden Eingriff in verschiedene Freiheitsgrundrechte[831] verbunden, so dass eine Verhältnismäßigkeitsprüfung vorzunehmen ist. Prüfungsmaßstab ist daher, ob ein sachlicher Grund von solcher Art und solchem Gewicht existiert, dass er die Ungleichbehandlung rechtfertigt.

Dass eine Vorratsspeicherung der Kundendaten von Banken, Fluggesellschaften und anderen Unternehmen nicht machbar oder finanzierbar sei, lässt sich nicht behaupten. Im Unterschied zu Telekommunikationsdaten wäre in diesen Bereichen vielfach sogar keine zusätzliche Erfassung, sondern nur eine verlängerte Speicherung ohnehin erfasster Daten erforderlich, so dass der Aufwand eher geringer wäre.

Weiterhin ist zu überlegen, ob die Kundendaten von Banken und Fluggesellschaften für die Gefahrenabwehr oder Strafverfolgung typischerweise weniger nützlich sind als Telekommunikationsdaten. Gegen diese Überlegung spricht, dass gerade bei der organisierten Kriminalität vermehrt finanzielle Transaktionen und räumliche Mobilität anzunehmen sind. Angesichts der äußerst geringen Wahrscheinlichkeit, dass ein Telekommunikations-Verkehrsdatum bei der Abwehr einer Gefahr von Nutzen ist[832], liegt es nahe, dass diese Wahrscheinlichkeit bei Daten etwa über finanzielle Transaktionen und Flüge mindestens ebenso hoch liegt[833]. Es ist sogar wahrscheinlich, dass in diesen Bereichen zahlenmäßig erheblich weniger Daten anfallen als Telekommunikationsdaten, was für den höheren Nutzen eines typischen, bei Banken oder Fluggesellschaften anfallenden Datums spricht. Dass Telekommunikationsdaten einen höheren Nutzen für die Gefahrenabwehr- oder die Strafverfolgungsbehörden aufweisen, kann daher nicht ohne Weiteres, das heißt nicht ohne entsprechende empirische Erkenntnisse, unterstellt werden, so dass ein unterschiedlicher Nutzen gegenwärtig als Rechtfertigungsgrund ausscheidet.

Ferner ist daran zu denken, dass Daten über finanzielle Transaktionen und über Flüge von Personen schutzwürdiger sein könnten als Telekommunikationsdaten. Dagegen ist die hohe Sensibilität und Aussagekraft von Telekommunikationsdaten anzuführen[834]. Zwar kann man anhand von Flugdaten grobe Bewegungsprofile erstellen. Eine generelle Vorratsspeicherung von Telekommunikationsdaten und damit auch der Mobiltelefon-Positionsdaten ermöglicht die Erstellung von Bewegungsprofilen aber in viel genauerem Maße. Ebenso mögen, was bei Banken gespeicherte Daten angeht, Daten über das Vermögen von Personen besonders sensibel sein. Daten über die Nutzung von Telefon und Internet sind aber nicht weniger sensibel[835]. Dass Telekommunikationsdaten typischerweise weniger schutzwürdig seien als die anderen genannten Daten, lässt sich daher nicht sagen.

Mithin ist kein sachlicher Grund von solcher Art und solchem Gewicht ersichtlich, dass er die generelle Vorratsspeicherung nur von Telekommunikationsdaten rechtfertigen kann. Die Einführung einer solchen Maßnahme ist daher nach gegenwärtigem Erkenntnisstand mit Art. 3 Abs. 1 GG unvereinbar.

Banken und Fluggesellschaften wurden hier im Übrigen nur beispielhaft heraus gegriffen. Sammlungen personenbezogener Daten existieren auch bei einer Vielzahl anderer Stellen wie etwa Kreditauskunfteien, Direktmarketingfirmen, Anwälten, Steuerberatern, Wirtschaftsprüfern, Krankenhäusern, Hotels, Ärzten, Apotheken und Behörden, ohne dass zugunsten der Eingriffsbehörden Mindestspeicherfristen oder auch nur Zugriffsrechte im Einzelfall vorgesehen sind. Weitergehende Möglichkeiten zur Speicherung potenziell nützlicher Daten sind nahezu unbegrenzt denkbar. So könnte man sämtliche Läden und Geschäfte dazu verpflichten, die Identität ihrer Besucher festzuhalten oder die Videobänder von Überwachungskameras aufzubewahren[836]. Man könnte Bewegungen des Straßenverkehrs registrieren, die Benutzung des öffentlichen Personenverkehrs und die Anwesenheit auf öffentlichen Veranstaltungen. Derartige Pflichten wären jedenfalls für diejenigen Stellen, die Kundendaten ohnehin erfassen und im Fall einer Vorratsspeicherungspflicht nur länger aufbewahren müssten, nicht belasten-

830 Seite 100.
831 Seite 100.
832 Seiten 59-60.
833 Ebenso Schmitz, MMR 2003, 214 (216) für die Benutzung von Flohmärkten, Supermärkten und Autobahnen.
834 Seiten 61-79.
835 Seiten 61-79.
836 APIG, Communications Data, 29.

der als es eine Kommunikationsdatenspeicherungspflicht für Telekommunikationsunternehmen ist. Zudem scheinen solche Maßnahmen zur Strafverfolgung und Gefahrenabwehr mindestens ebenso geeignet zu sein wie eine generelle Vorratsspeicherung von Telekommunikationsdaten. Überhaupt ist zweifelhaft, ob Telekommunikationsdaten nützlicher sind als jegliche sonstige Daten oder Kenntnisse über das Verhalten der Bevölkerung.

bb) Ungleichbehandlung von Telekommunikationsunternehmen gegenüber anderen Unternehmen, z.B. Banken und Fluggesellschaften

Die zuvor diskutierte Ungleichbehandlung lässt sich auch unter dem Blickwinkel derjenigen betrachten, die zur Durchführung einer Vorratsspeicherung von Telekommunikationsdaten verpflichtet wären. Zu vergleichen sind dann Telekommunikationsunternehmen einerseits mit Unternehmen wie Banken und Fluggesellschaften andererseits. Als gemeinsamer Oberbegriff ist die Gruppe der Unternehmen anzusehen, die Leistungen anbieten, bei deren Erbringung Daten anfallen oder gespeichert werden können, welche für die Gefahrenabwehr oder Strafverfolgung nützlich sein können. Die benachteiligende Pflicht zur Vorratsspeicherung knüpft an eine bestimmte Personengruppe an, nämlich an den Beruf des Telekommunikationsdienstleisters, so dass alle der oben genannten Kriterien[837] für eine Verhältnismäßigkeitsprüfung sprechen. Nach dem zuvor Gesagten[838] ist kein sachlicher Grund von solcher Art und solchem Gewicht ersichtlich, dass er die Einführung einer Mindestspeicherungspflicht nur für Telekommunikationsdaten rechtfertigen kann. Die Einführung einer Vorratsspeicherungspflicht ist daher auch wegen ungerechtfertigter Benachteiligung der Telekommunikationsunternehmen gegenüber sonstigen Unternehmen der genannten Art mit Art. 3 Abs. 1 GG unvereinbar.

d) Ungleichbehandlung durch Absehen von der Wahl milderer Mittel

Art. 3 Abs. 1 GG ist auch verletzt, weil der Gesetzgeber ungerechtfertigt von der Wahl milderer Mittel als einer generellen Kommunikationsdatenspeicherung abgesehen hat.

aa) Eingriff in den Schutzbereich des Art. 3 Abs. 1 GG

Fraglich ist zunächst, ob Art. 3 Abs. 1 GG unter dem Aspekt der Verfügbarkeit milderer Mittel betroffen sein kann. Grundsätzlich ist anerkannt, dass der Staat unter mehreren zur Erreichung eines Zwecks geeigneten Mitteln die Wahl hat[839]. Wenn mildere Mittel als das gewählte nicht in jedem Einzelfall die gleiche Wirkung entfalten, verstößt der Staat mit seiner Wahl auch nicht gegen das Gebot der Erforderlichkeit des Eingriffs.

Im Hinblick auf Art. 3 Abs. 1 GG kann der Grundsatz der freien Wahl unter mehreren geeigneten Mitteln aber dann nicht uneingeschränkt gelten, wenn gegenüber einer ergriffenen Maßnahme mildere Mittel zur Verfügung stehen, die zwar nicht in jedem Einzelfall die gleiche Wirkung entfalten mögen, aber doch bezogen auf die Gesamtheit der Fälle. In diesen Fällen verlangt Art. 3 Abs. 1 GG eine sachliche Rechtfertigung für die Wahl des Staates. Eine solche kann beispielsweise darin liegen, dass die Wirksamkeit des Mittels gerade in bestimmten Fällen angestrebt ist. Zur Rechtfertigung kann demgegenüber nicht bereits die Behauptung genügen, weitergehende Maßnahmen würden später ergriffen.

Liegt ein Rechtfertigungsgrund nicht vor, dann gebietet Art. 3 Abs. 1 GG dem Gesetzgeber, von mehreren gleichwertigen Mitteln gleichen Gebrauch zu machen. Stehen also beispielsweise zwei gleich wirksame Mittel zur Verfügung, dann muss der Gesetzgeber wählen, ob er auf beide Mittel verzichtet, nur das mildere Mittel einsetzt oder beide Mittel zugleich einsetzt. Die Wahl nur des stärker eingreifenden Mittels verstößt gegen Art. 3 Abs. 1 GG, wenn sie nicht aus besonderen Gründen gerechtfertigt ist.

Fraglich ist, ob gleich wirksame Alternativen zu einer generellen Vorratsspeicherung von Telekommunikationsdaten zur Verfügung stehen. In der Tat existiert neben einer generellen Kommunikationsdatenspeicherung eine Vielzahl von Mitteln, die als mildere aber gleichermaßen wirksame Alternativen gegenüber einer generellen Vorratsspeicherung aller Telekommunikationsdaten in Betracht kommen. Dabei handelt es sich nicht in erster Linie um rechtspolitische Möglichkeiten. In vielen Bereichen erscheinen tatsächliche Maßnahmen in Bezug auf potenzielle Täter, potenzielle Opfer und die zuständigen Behörden sinnvoller.

Was die allgemeine Kriminalprävention angeht, so zeigen einschlägige Forschungsergebnisse, dass Ansätze zur Bekämpfung der Wurzeln von Kriminalität nicht weniger Erfolg versprechen als repressi-

837 Seiten 99-100.
838 Seiten 109-110.
839 BVerfG, NJW 2004, 146 (149).

ve Maßnahmen[840]. Politische Arbeit etwa in den Bereichen Jugend, Arbeit, Wohnen, Soziales und Bildung kann langfristig die beste Sicherheitspolitik sein[841].

Gerade im Bereich der Netzkriminalität im engeren Sinne sind kriminalpräventive Projekte vielversprechend[842]. Hier sind es nämlich zum größten Teil jugendliche Täter, die ohne kriminelle Energie oder Bereicherungsabsicht große Schäden verursachen[843]. Wenn hier beispielsweise durch Aktionen an Schulen ein entsprechendes Problem- und Unrechtsbewusstsein erzeugt würde, wären reale Erfolge zu erwarten[844].

Auch auf Seiten der Opfer von Netzkriminalität – häufig Wirtschaftsunternehmen – ist es erforderlich, ein Problembewusstsein zu erzeugen[845]. Unternehmen sollten bei jeder Veränderung ihrer Informationsstruktur Sicherheitsfragen bedenken. Es sollte sicher gestellt werden, dass Mitarbeiter bei der Computerbenutzung bestimmte Sicherheitsregeln befolgen. Firmen, die Hard- oder Software produzieren, sollten Sicherheitsbelange bereits bei der Produktentwicklung angemessen berücksichtigen. Für einzelne Industriezweige könnten spezielle Verhaltenskodizes erarbeitet werden. Sicherheits-Know-how sollte regelmäßig ausgetauscht werden. Auch der Informationsfluss zwischen Wirtschaft und den Sicherheitsbehörden sollte erhöht werden.

Ein marktwirtschaftlicher Mechanismus zur Durchsetzung solcher Ziele ist die Einführung eines Datenschutz-Audits, wie es etwa das Datenschutzzentrum Schleswig-Holstein bereits anbietet. Der Anreiz für Unternehmen, sich einer solchen Prüfung zu unterziehen, besteht in der Anerkennung von Kundenseite. Der Staat kann sich zudem auf den Kauf von geprüften Produkten beschränken. Weiterhin ist anzunehmen, dass freiwillige Prüfverfahren Auswirkungen auf die von Unternehmen zu zahlende Prämie für Versicherungen gegen Computerschäden haben, so dass auch auf diese Weise marktkonform Druck ausgeübt werden kann. Daneben könnte der Staat die Durchführung von Audits auch durch Gewährung von Steuervorteilen fördern. Mittelfristig kann sich dies für den Staat lohnen, weil ein verstärkter Selbstschutz auf Seiten der Wirtschaft die Eingriffsbehörden entlastet.

Auch die Einführung einer Pflichtversicherung für gewerblich betriebene, an das Internet angeschlossene Informationssysteme kommt in Betracht, zumal sich die Auswirkungen von Netzkriminalität oft auf Vermögensschäden beschränken[846]. Im Bereich der Arbeitsunfälle hat das deutsche Pflichtversicherungssystem zu einer enormen Steigerung des Sicherheitsbewusstseins geführt, was für die Effektivität einer möglichen Pflichtversicherung auch auf dem Gebiet der Telekommunikationsnetze spricht. Gegen Wirtschaftskriminalität sind bisher nur etwa ein Drittel der deutschen Unternehmen versichert[847].

Im Bereich national wichtiger Informationssysteme ist weiterhin die Einführung einer klassischen verwaltungsrechtlichen Genehmigungspflicht mit anschließender Überwachung der Computersysteme denkbar. Die Überwachung ließe sich turnusmäßig wie im Bereich der Kfz-Überwachung oder stichprobenartig wie bei der Lebensmittelüberwachung gestalten. Die Einhaltung verwaltungsrechtlicher Pflichten ließe sich mit der Androhung von Bußgeldern absichern. Das Recht der Ordnungswidrigkeiten ist vom Opportunitätsprinzip bestimmt und wirft daher die Gleichheitsfragen, die sich bei einer faktisch nur fragmentarischen Strafverfolgung stellen, nicht in gleichem Maße auf. Soweit man nicht in Anbetracht der vielfältigen Möglichkeiten der Eigenvorsorge ganz auf das Strafrecht verzichten möchte, kann man die Verfolgung von Straftaten im Bereich der Netzkriminalität im engeren Sinne wenigstens auf Fälle von besonderem öffentlichen Interesse beschränken und es ansonsten den Betroffenen (etwa gewerblichen Inhabern von Urheberrechten) ermöglichen, zivilrechtliche Verfahren zu betreiben.

840 Travis Hirschi, zitiert bei Kunz, Kriminologie, § 34, Rn. 3; Schneider, Kriminologie, 325; Diekmann, Die Befolgung von Gesetzen, 151.

841 Hassemer, Strafen im Rechtsstaat, 262.

842 Sieber, COMCRIME-Studie (I), 199: „The future information society requires mainly non-criminal measures for the prevention of computer crime“; ders., 202: „In the modern risk society the main efforts to reduce risks must focus on technical, structural and educational measures.“

843 BMI/BMJ, Sicherheitsbericht 2001, 202: „Der bisher im Zusammenhang mit Angriffen auf die Sicherheit, Zuverlässigkeit und Integrität von Daten bekannt gewordene Tätertypus entspricht weitgehend dem Klischee des jugendlichen Hackers, der nicht mit außergewöhnlich hoher krimineller Energie und mit Bereicherungsabsicht agiert“; Hong Kong Inter-departmental Working Group on Computer Related Crime, Report (I), 79 f.

844 Robinson, James K.: Vortrag auf der International Computer Crime Conference „Internet as the Scene of Crime“ in Oslo, Norwegen, 29.-31.05.2000, www.usdoj.gov/criminal/cybercrime/roboslo.htm; Hong Kong Inter-departmental Working Group on Computer Related Crime, Report (I), 79 f.

845 Zum Folgenden vgl. Hong Kong Inter-departmental Working Group on Computer Related Crime, Report (I), 85 f.

846 Seiten 36-43.

847 PricewaterhouseCoopers, Wirtschaftskriminalität 2003 (I).

Auch die Bürger lassen sich aktivieren, um die Einhaltung von Datensicherheitsregeln durch Organisationen sicherzustellen. So könnte den Kunden eines Unternehmens ein Auskunftsanspruch bezüglich der vorhandenen Sicherheitsmechanismen zum Schutz ihrer Daten eingeräumt werden. Weiterhin sind Mitarbeiter von Unternehmen und Behörden eine wichtige Informationsquelle, die sich nutzen lässt, indem man eine Möglichkeit zur anonymen Erteilung von Hinweisen auf Sicherheitslücken bereit stellt. Eine starke Einbindung der Beschäftigten ist auch angesichts der Tatsache sinnvoll, dass ein Großteil der Schäden durch Computerkriminalität auf Mitarbeiter des geschädigten Unternehmens zurückzuführen ist[848]. Gerade Missbräuche innerhalb des eigenen Unternehmens lassen sich durch interne Maßnahmen relativ leicht feststellen und unterbinden[849].

In anderen Staaten geht eine Steuerungsfunktion zudem oft vom Zivilrecht aus. Dies funktioniert allerdings nur, wenn hinreichend hohe Schadenssummen drohen. Die USA kennen beispielsweise das Institut des „Strafschadensersatzes" („punitive damages") und das Instrument der Sammelklage („class action"). In Deutschland hat die Rechtsentwicklung auf dem Gebiet der Produkthaftung zu erheblichen Anstrengungen der Hersteller geführt, die auf dem Gebiet der Hard- und Softwaresicherheit in dieser Form nicht zu beobachten sind. Dies wird darauf zurückzuführen sein, dass die verschuldensunabhängige Haftung nach dem Produkthaftungsgesetz nur im Fall von Körper- und Sachschäden greift (§ 1 Abs. 1 S. 1 ProdHG), Netzkriminalität im engeren Sinne aber regelmäßig zu immateriellen Schäden führt. Schäden dieser Art sind auch von der deliktischen Haftung nach § 823 Abs. 1 BGB nicht erfasst. Insoweit könnte es nützlich sein, wenn Betroffene, denen Schäden wegen einer unsicheren Gestaltung von Computersystemen entstanden sind, gegen den Hersteller vorgehen könnten, ohne diesem ein Verschulden nachweisen zu müssen.

Im Internet sind Maßnahmen des Selbstschutzes von außerordentlich hoher Bedeutung[850]. Eine amerikanische Untersuchung kommt zu dem Ergebnis, dass Sicherheitslücken, welche sich verbreitete Viren zunutze machten, ausnahmslos schon über einen Monat lang bekannt waren, bevor es zu Schäden durch Ausnutzen der Lücken kam[851]. Auch die Angriffe, welche in den vergangenen Jahren kommerzielle Internetpräsenzen zum Ziel hatten, sind unter Ausnutzung alter und lange bekannter Sicherheitslücken ausgeführt worden. Allgemein sind im Bereich der Netzkriminalität im engeren Sinne viele Angriffe nur deswegen möglich, weil die Betroffenen ihre Systeme unzureichend eingerichtet haben oder nicht in Stand halten[852]. Dass Sicherheitslücken schon in der Zeit vor Bereitstellung einer Abhilfemöglichkeit ausgenutzt werden, ist selten, so dass sich Schäden durch Netzkriminalität im engeren Sinne in aller Regel effektiv durch Maßnahmen der Betreiber der Einrichtungen unterbinden lassen. Gerade wenn Computeranlagen kommerziell betrieben werden, sollten sie stets auf dem neuesten Stand gehalten werden. Da die Aufdeckung von Sicherheitslücken nach kurzer Zeit zur Bereitstellung einer kostenlosen Abhilfemöglichkeit durch den Hersteller führt („Updates", „Patches"), ist dies ohne unzumutbaren Aufwand möglich. Naturgemäß setzt die sichere Gestaltung von Informationssystemen ein gewisses technisches Verständnis voraus, welches gerade Privatnutzern verstärkt vermittelt werden sollte.

Das enorme Potenzial technischer Schutzmaßnahmen verdeutlicht die Tatsache, dass 77% der im Rahmen einer Umfrage antwortenden Unternehmen und Organisationen als Reaktion auf Computerkriminalität in den meisten Fällen Sicherheitslücken gestopft haben[853]. Die beste Prävention in solchen Fällen ist daher nicht ein staatliches Ermittlungsverfahren, sondern eine Veränderung der betroffenen Systeme. Solche Maßnahmen anstelle eines Strafverfahrens werden regelmäßig auch ausreichen, wo ausschließlich ein Vermögensschaden bei der betroffenen Firma eingetreten ist, zumal sich solche Schäden problemlos versichern lassen[854]. Nur durch technische Maßnahmen ist ein dauerhafter und effektiver Schutz vor Schäden durch Hacking möglich; staatliche Überwachungsmaßnahmen nützen im Vergleich dazu kaum[855]. Zu Recht wird darauf hingewiesen, dass es wenig weiter hilft, wenn ein Teenager, dessen Computervirus die Verwaltung in Deutschland zwei Tage lang lahm gelegt hat, dafür einige Jahre ins Gefängnis kommt. An dem entstandenen Schaden kann dies nichts ändern[856] und e-

848 Symantec, Symantec Internet Security Threat Report (I), 5 und Seite 42.
849 Symantec, Symantec Internet Security Threat Report (I), 5.
850 Hassemer, Staat, Sicherheit und Information, 225 (244).
851 Symantec, Symantec Internet Security Threat Report (I), 7 und 32.
852 Sieber, COMCRIME-Studie (I), 204.
853 CSI/FBI, 2002 Survey (I), 20.
854 CSI/FBI, 2002 Survey (I), 19.
855 Holznagel, Bernd: Stellungnahme für die öffentliche Anhörung „Von der Industrie- zur Wissensgesellschaft: Wirtschaft, Arbeitswelt und Recht, Privatisierung und Patentierung von Wissen", 08.10.2001, www.bundestag.de/gremien/welt/-weltto/weltto126_stell004.pdf, 22.
856 Bogk, Andreas (Chaos Computer Club) in Bundestag, Öffentliche Anhörung zum Thema Cyber-Crime/TKÜV (I), 55; vgl. auch Hassemer, Strafen im Rechtsstaat, 289.

benso wenig an der fortbestehenden Anfälligkeit der betroffenen Systeme für Computerviren, wenn nicht Vorbeugemaßnahmen ergriffen werden. Durch staatliche Eingriffe im Einzelfall werden sich Angriffe auf Computersysteme kaum einmal abwenden lassen. Dass die präventive Wirkung einer verstärkten Strafverfolgung im Bereich der Netzkriminalität im engeren Sinne besonders niedrig angesetzt werden muss, zeigt auch das Beispiel immer neuer Computerviren, die nicht selten aus Ländern mit einer effektiven Strafverfolgung stammen.

Soweit sich Angriffe auf Computersysteme nicht von vornherein verhindern lassen, ist es sinnvoll, Pläne zur Minimierung der Auswirkungen solcher Angriffe und zur möglichst zügigen Instandsetzung betroffener Anlagen bereit zu halten, insbesondere für den Fall ernsthafter Angriffe auf bedeutende Teile der Telekommunikationsinfrastruktur.

Schäden durch Netzkriminalität im engeren Sinne sind mithin in hohem Maße durch technische und organisatorische Maßnahmen vermeidbar. Aber auch im Bereich der Netzkriminalität im weiteren Sinne, etwa in Fällen von Betrug und anderen Vermögensdelikten im Internet, lässt sich durch Sensibilisierung der Nutzer einiges erreichen. Oft wird nur allzu blauäugig auf Angebote eingegangen, deren Unseriosität erfahrene Nutzern sofort bemerkt hätten. Auch ein leichtsinniger Umgang mit persönlichen Daten wie Kreditkartennummern ist zu beklagen. Ein Entgegensteuern durch entsprechende Information erscheint sinnvoll. Die Anzahl der Fälle von Kreditkartenmissbrauch ließe sich zudem durch die Einführung eines günstigen, sicheren und einfachen bargeldlosen Zahlungssystems im Internet erheblich reduzieren. Auf Seiten der Wirtschaft ist davon auszugehen, dass sich die meisten Betrugsfälle zulasten von Unternehmen mit guten Sicherheits- und Kontrollmechanismen vermeiden lassen[857].

Hier ist nicht der Raum, um ausführlich zu analysieren, welche Maßnahmen im Einzelnen zur Verfügung stehen und welche Potenziale noch ausgeschöpft werden können. Diese Fragen sind unter anderem im Rahmen der G8 bereits behandelt worden[858]. Auf der Hand liegt jedenfalls, dass Ansätze zur Prävention, also insbesondere technische, strukturelle und aufklärende Maßnahmen, von vornherein umfassender angelegt sind als repressive Methoden, schon deshalb, weil sie nicht nur vor Schäden durch Straftaten schützen, sondern auch vor Schäden etwa durch Fahrlässigkeit, menschlichen Irrtum, Inkompetenz und höhere Gewalt[859].

Auch auf Seiten der Eingriffsbehörden bestehen erhebliche Verbesserungsmöglichkeiten. Zu Recht warnen Behördenvertreter, dass es eine Überschätzung der Möglichkeiten der Telekommunikationsüberwachung wäre, diese allein als „Schlüssel zur inneren Sicherheit“ anzusehen[860]. Entsprechende Informationen lassen sich oft auch durch klassische Polizeiarbeit finden[861], die zwar aufwändiger sein mag, dafür aber zielgerichteter erfolgen und infolgedessen effektiver sein kann[862]. Die weitgehendsten Befugnisse sind zudem ohne Wert, wenn es immer noch Polizeistellen gibt, die nicht einmal über einen internetfähigen PC verfügen[863]. Es mehren sich die Stimmen, denen zufolge es in Deutschland nicht an Eingriffsbefugnissen fehlt[864], sondern vor allem an personeller Kompetenz[865]. Die bessere Qualifizierung des eingesetzten Personals in technischer Hinsicht verspricht also großen Erfolg[866],

857 CSI/FBI, 2002 Survey (I), 15; vgl. auch Kubica, Die Kriminalpolizei 9/2001 zu Möglichkeiten der Betrugsprävention.

858 Vgl. die detaillierte Auflistung von Präventionsmöglichkeiten für jeweilige Gefahren bei G8 Workshop, Workshop 3 (I) sowie die Zusammenstellung bei G8 Workshop, Workshop 4 (I).

859 Sieber, COMCRIME-Studie (I), 202 f.

860 Bansberg (Abteilung Grundsatzangelegenheiten des Bundesamtes für Verfassungsschutz), Staatsschutz im Internet, 48 (54).

861 Bansberg (Abteilung Grundsatzangelegenheiten des Bundesamtes für Verfassungsschutz), Staatsschutz im Internet, 48 (54).

862 Weichert, DuD 2001, 694 (694).

863 Gusy, Christoph, zitiert bei Thomas, Volker: Christoph Gusy: „Vollständige Sicherheit darf es nicht geben“, fluter 2/2002, 25 (25), www.fluter.de/look/issues/issue6/pdf/FL2_24_25.pdf; vgl. auch Uhe/Herrmann, Überwachung im Internet (I), 111.

864 Bundesregierung, BT-Drs. 14/4173, 20: „In rechtlicher Hinsicht ist wesentlichen Aspekten der Datennetzkriminalität und der Computerstraftaten bereits mit dem derzeit geltenden materiellen Computerstrafrecht und dem Strafprozessrecht Rechnung getragen.“; Weichert, Bekämpfung von Internet-Kriminalität (I), Punkt 8; Schaar, Sicherheit und Freiheitsrechte (I), 17; Garstka, zum Terrorismusbekämpfungsgesetz (I); Germann, 689; eco, Electronic Commerce Forum e.V., Verband der deutschen Internetwirtschaft: Pressemitteilung vom 31.05.2002 zur Gesetzesinitiative des Bundesrats vom 31.05.2002 (BR-Drs. 275/02), www.eco.de/presse/mitteilungen/2002/02-05-31_de.htm.

865 BMI/BMJ, Sicherheitsbericht 2001, 201; Weichert, Bekämpfung von Internet-Kriminalität (I), Punkt 8; Germann, 689; eco, Electronic Commerce Forum e.V., Verband der deutschen Internetwirtschaft: Pressemitteilung vom 31.05.2002 zur Gesetzesinitiative des Bundesrats vom 31.05.2002 (BR-Drs. 275/02), www.eco.de/presse/mitteilungen/2002/02-05-31_de.htm; Polizeigewerkschaft, zitiert bei Heise Verlag: Thüringens Justizminister fordert stärkere Bekämpfung der Internet-Kriminalität, Meldung vom 29.03.2003, www.heise.de/newsticker/data/anm-29.03.03-000/.

866 Kommission, Sichere Informationsgesellschaft (I), 30; Queen Mary (University of London), Studie über Netzkriminalität (I); EuroISPA, Internet Service Providers' Association (Europe) / US ISPA, Internet Service Providers' Association

gerade bei internetbezogenen Sachverhalten. Ebenso ist an eine Kompetenzbündelung zu denken, etwa durch Einrichtung von „Taskforces“ oder Zentralstellen[867]. Demgegenüber ist zu beachten, dass nach den bislang vorliegenden empirischen Studien weder ein erhöhter Personalbestand bei der Polizei noch eine verbesserte sachliche Ausstattung unmittelbar und signifikant zu einer höheren Aufklärungsquote oder gar zu einer Reduktion von polizeilich registrierter Kriminalität geführt hat – im Gegenteil: Mehrere Studien konnten einen linearen Zusammenhang zwischen mehr Polizei und mehr Kriminalität feststellen[868].

Die Bedeutung technischer und organisatorischer Maßnahmen im Bereich der Eingriffsbehörden gegenüber rechtspolitischen Lösungen wird deutlich, wenn man Erfahrungswerte betrachtet: Dass etwa die Terroranschläge vom 11. September 2001 nicht abgewendet wurden, ist auf mangelnde menschliche Ermittlungsarbeit und nicht auf mangelnde Daten zurückzuführen[869]. Die US-amerikanischen Nachrichtendienste verfügten im Vorfeld über eine Vielzahl relevanter Informationen, denen keine Bedeutung beigemessen wurde.

Insgesamt liegt die Annahme nahe, dass Verbesserungen technischer und organisatorischer Art ergiebiger sind als die Schaffung neuer Überwachungsbefugnisse. Anders als in den USA, wo ernsthafte Anstrengungen in dieser Richtung gemacht werden[870], werden hierzulande die vorhandenen Potenziale bei weitem nicht ausgeschöpft[871]. Alternative Präventivmaßnahmen bleiben auf politischer Ebene nicht selten gänzlich unberücksichtigt[872]. Dies mag daran liegen, dass sich rechtspolitische Maßnahmen auf dem Gebiet der inneren Sicherheit der Öffentlichkeit leichter als tatkräftiges Zupacken der Entscheidungsträger präsentieren lassen. Präventivmaßnahmen kosten den Staat zudem oft Geld[873], so dass rechtspolitische Lösungen meist einfacher durchzusetzen sind. Die indirekten Kosten dieser Lösungen – Einbußen an Freiheit und finanzielle Aufwendungen der Wirtschaft – trägt letztlich der Bürger, oft ohne dass er es merkt. Würde der Staat der Wirtschaft für Aufwendungen im Zusammenhang mit staatlichen Hilfsdiensten einen vollen Kostenerstattungsanspruch einräumen und hätten die Bürger diese Kosten daher deutlich sichtbar in Form von Steuern zu tragen, so würde die politisch leichte Durchsetzbarkeit neuer Überwachungsbefugnisse sofort entfallen. Gerade mit einer generellen Vorratsspeicherung von Telekommunikationsdaten sind immense Kosten verbunden[874]. Schon mit einem Bruchteil dieser Mittel können viele der zuvor genannten Alternativmaßnahmen durchgeführt werden.

Neben den genannten Maßnahmen tatsächlicher Art finden sich auch auf dem Gebiet der Rechtspolitik mildere Mittel gegenüber einer generellen Vorratsspeicherung von Telekommunikationsdaten. Insbesondere kommt in Betracht, Sicherheitsbehörden die Befugnis einzuräumen, im Einzelfall die Aufbewahrung bereits gespeicherter Kommunikationsdaten zu verlangen (vgl. Art. 16, 17 CCC). Darüber hinaus kann den Eingriffsbehörden die Befugnis eingeräumt werden, in Einzelfällen die Aufzeichnung von Kommunikationsdaten anzuordnen (Art. 20 CCC)[875]. Zwar gilt die Cybercrime-Konvention des Europarates nur für den Zugriff auf Telekommunikationsdaten bezüglich computergestützter Kommunikationsvorgänge (Art. 1 Buchst. d CCC) im Rahmen von Strafverfahren (Art. 14 CCC). Dies hindert aber nicht daran, die Einführung der in der Cybercrime-Konvention vorgesehenen Befugnisse auch in den übrigen Bereichen als Alternative zur Einführung einer generellen Vorratsspeicherung zu prüfen.

(U.S.A.): Position on the Impact of Data Retention Laws on the Fight against Cybercrime, 30.09.2002, www.euroispa.org/docs/020930eurousispa_dretent.pdf, 3; Weichert, Bekämpfung von Internet-Kriminalität (I), Punkt 8; Uhe/Herrmann, Überwachung im Internet (I), 111.

867 Kommission, Sichere Informationsgesellschaft (I), 30; Robinson, James K.: Vortrag auf der International Computer Crime Conference „Internet as the Scene of Crime“ in Oslo, Norwegen, 29.-31.05.2000, www.usdoj.gov/criminal/-cybercrime/roboslo.htm.

868 Feltes, Fehlerquellen im Ermittlungsverfahren (I) m.w.N.

869 Cappato, Marco (MdEP), zitiert bei Schulzki-Haddouti, Christiane: EU-Rat auf dem Weg zur Verbindungsdaten-Speicherung, 23.11.2002, Telepolis, Heise-Verlag, www.heise.de/tp/deutsch/inhalt/te/13660/1.html.

870 Vgl. die US-Initiative „National Strategy to Secure Cyberspace”: Heise Verlag: US-Regierung startet Netzwerk-Sicherheitsinitiative, Meldung vom 11.06.2002, www.heise.de/newsticker/data/pmz-11.06.02-000/.

871 Kommission, Sichere Informationsgesellschaft (I), 8: „Die meisten Länder konzentrieren ihre Maßnahmen zur Bekämpfung der Computerkriminalität (und insbesondere ihre strafrechtlichen Maßnahmen) auf die nationale Ebene, ohne alternative Präventivmaßnahmen zu berücksichtigen.“

872 Kommission, Sichere Informationsgesellschaft (I), 8.

873 Kommission, Sichere Informationsgesellschaft (I), 30.

874 Seiten 89-90.

875 Bäumler, Helmut / Leutheusser-Schnarrenberger, Sabine / Tinnefeld, Marie-Theres: Grenzenlose Überwachung des Internets? Steht die freie Internetkommunikation vor dem Aus? Stellungnahme zum Gesetzesentwurf des Bundesrates vom 31. Mai 2002, www.rainer-gerling.de/aktuell/vorrat_stellungnahme.html, Punkt 2.

In vielen Fällen genügen Einzelfallbefugnisse zur Erreichung des angestrebten Zwecks. In den USA etwa funktionieren diese Befugnisse gut[876], so dass man eine generelle Vorratsspeicherung von Telekommunikationsdaten dort nicht für erforderlich hält. In manchen Fällen sind Einzelfallbefugnisse zwar nicht gleichermaßen wirksam, nämlich dann, wenn der Zugriff auf in der Vergangenheit angefallene Telekommunikationsdaten erforderlich wird, die nicht gespeichert wurden oder bereits gelöscht worden sind. Der mögliche Effizienzgewinn durch die Einführung einer Vorratsspeicherung von Telekommunikationsdaten wird allerdings dadurch relativiert, dass auch diese Maßnahme ohne Erfolg bleibt, wenn der Nutzer es darauf anlegt, unentdeckt zu bleiben[877]. Zudem zeigen die praktischen Erfahrungen von Internet-Service-Providern, dass Einzelfallbefugnisse im Zusammenspiel mit klassischer kriminalistischer Arbeit regelmäßig ausreichen, um eine ordnungsgemäße Strafverfolgung sicherzustellen[878]. Gerade bei Wiederholungstätern schadet es nicht, wenn Kommunikationsdaten zunächst nicht verfügbar sind, weil diese Daten im Wiederholungsfall durch eine Einzelfallanordnung erhoben werden können. Handelt es sich nicht um einen Wiederholungstäter, dann geht von diesem keine weitere Gefahr aus, so dass das Strafverfolgungsinteresse gegenüber der Privatsphäre rechtstreuer Bürger zurücktreten muss.

Für schwerste Fälle lässt sich auch daran denken, die Sicherheitsbehörden zur Anordnung der kurzzeitigen Aufbewahrung sämtlicher gespeicherter Kommunikationsdaten zu ermächtigen. In Großbritannien wurden Internet-Service-Provider beispielsweise am 11. September 2001 um Aufbewahrung aller verfügbaren Kommunikationsdaten gebeten, was für die Ermittlungen im Zusammenhang mit dem Anschlag auf das World Trade Center von erheblichem Nutzen gewesen sein soll[879].

Als weitere rechtspolitische Maßnahme kommt in Betracht, ein Verfahren der internationalen Rechtshilfe hinsichtlich des Zugriffs auf Telekommunikationsdaten vorzusehen, um den Zugriff auf ausländische Telekommunikationsdaten zu ermöglichen. Für den Bereich der Strafverfolgung leistet dies die Cybercrime-Konvention, in der unter anderem vorgesehen ist, dass jede Vertragspartei von den anderen Unterzeichnerstaaten die Erhebung und Übermittlung vorhandener oder zukünftig anfallender Kommunikationsdaten verlangen kann (Art. 29 und 33 CCC). Ähnliche Mechanismen könnten auch im Bereich der Gefahrenabwehr geschaffen werden, wobei die eigenständige Bedeutung dieses Gebiets gegenüber den Bereich strafbarer Handlungen eher gering ist[880]. Der Verwendung von Erkenntnissen, die im Rahmen von strafrechtlichen Ermittlungen angefordert wurden, zur Gefahrenabwehr steht die Cybercrime-Konvention zudem regelmäßig nicht entgegen (vgl. Art. 28 Abs. 2 Buchst. b CCC).

Die Erforderlichkeit einer internationalen Zusammenarbeit zeigt sich daran, dass es moderne Informations- und Kommunikationssysteme möglich machen, jederzeit von jedem Ort der Welt aus illegale Handlungen zu begehen[881] und Schäden an den verschiedensten Orten der Welt herbeizuführen[882]. Die neuen Technologien kennen keine Staatsgrenzen, obwohl für die Strafverfolgung nach wie vor die Einzelstaaten zuständig sind[883]. Dies macht die internationale Kooperation bei der Strafverfolgung und ein international hinreichend abgestimmtes materielles Strafrecht so wichtig[884]. Dabei sind internationale Rechtshilfeabkommen so lange ein milderes Mittel gegenüber der Einführung einer generellen Vorratsspeicherung von Telekommunikations-Verbindungsdaten wie sie den internationalen Zugriff auf Telekommunikationsdaten nur in einzelnen Fällen erlauben.

Der potenzielle Nutzen von Verfahren der internationalen Rechtshilfe ist hoch einzuschätzen. Wie an anderer Stelle dargelegt[885], können Benutzer von Telekommunikationsnetzen nämlich in weiten Bereichen ohne größere Schwierigkeiten ausländische Diensteanbieter nutzen, so dass der Zugriff auf ihre Telekommunikationsdaten ausschließlich im Ausland möglich ist. Gerade in Kreisen ernsthafter Kriminalität muss davon ausgegangen werden, dass von derartigen Möglichkeiten Gebrauch gemacht wird. Bekannt ist, dass bis zu 89% der Fälle organisierter Kriminalität einen internationalen Bezug

876 Lack, Bob in APIG, All Party Parliamentary Internet Group (UK): The Home Office, APIG Communications Data Inquiry Oral Evidence, 18.12.2002, www.apig.org.uk/homeoffice_oral_evidence.htm.

877 Seite 52.

878 EuroISPA, Internet Service Providers' Association (Europe) / US ISPA, Internet Service Providers' Association (U.S.A.): Position on the Impact of Data Retention Laws on the Fight against Cybercrime, 30.09.2002, www.euroispa.org/docs/020930eurousispa_dretent.pdf, 2.

879 APIG, Communications Data, 30.

880 Seite 43.

881 Kommission, Sichere Informationsgesellschaft (I), 13.

882 Weichert, Bekämpfung von Internet-Kriminalität (I), Punkt 2.

883 G7, High-Tech Crime Communiqué (I).

884 G7, High-Tech Crime Communiqué (I); Weichert, Bekämpfung von Internet-Kriminalität (I), Punkt 2.

885 Breyer, Vorratsspeicherung, 14 ff.

aufweisen[886]. Um die internationalen Aktivitäten solcher Organisationen zu koordinieren, werden regelmäßig Telekommunikationsnetze zum Einsatz kommen. Auch von den 1.126 im Jahre 1999 von der im Bundeskriminalamt eingerichteten „Zentralstelle für anlassunabhängige Recherchen in Datennetzen“ ermittelten Verdachtsfällen wiesen 81% einen Auslandsbezug auf[887]. Dementsprechend waren in 80% der eingeleiteten strafrechtlichen Ermittlungsverfahren Zugriffe auf im Ausland gespeicherte Kommunikationsdaten erforderlich[888].

In Anbetracht dessen erscheint es um vieles nützlicher, den internationalen Zugriff auf ohnehin erhobene Telekommunikationsdaten zu ermöglichen sowie Mechanismen zur internationalen Erhebung von Kommunikationsdaten im Einzelfall einzuführen als leicht zu umgehende Regelungen zur Vorratsspeicherung im nationalen oder regionalen Alleingang vorzusehen. Gerade in den USA befindet sich eine Vielzahl von Diensteanbietern. Da deutsche Behörden insoweit bislang keinen Zugriff haben, erscheint der mögliche Effizienzgewinn durch die national oder kontinental beschränkte Einführung einer Vorratsspeicherung von Telekommunikationsdaten vergleichsweise gering[889].

Diese Einschätzung bestätigen die Ausführungen der finnischen Delegation zur Multidisciplinary Group on Organised Crime der EU: Als größtes Problem im Zusammenhang mit dem Zugriff auf Kommunikationsdaten beklagt sie nicht, dass Daten mangels obligatorischer Vorratsspeicherung teilweise nicht zur Verfügung stehen. Dies sei nur „gelegentlich“ ein Problem[890]. Das größte Problem bestehe vielmehr in der mangelhaften internationalen Zusammenarbeit, besonders mit Nicht-EU-Staaten[891]. Innerhalb der EU dauere es Monate bis Jahre, bis Daten übermittelt würden. Der Zugriff auf Kommunikationsdaten außerhalb der EU sei nahezu komplett unmöglich[892]. Auch Vertreter der deutschen Sicherheitsbehörden betonen, dass die derzeitigen Möglichkeiten der grenzüberschreitenden Telekommunikationsüberwachung völlig unzureichend seien[893]. Neben der normativen Einführung von Rechtshilfeverfahren ist damit auch ihre praktische Effektivierung dringend erforderlich und für die Arbeit der Eingriffsbehörden von großer Bedeutung.

Zusammenfassend existieren verschiedene Mittel, die gegenüber einer generellen Vorratsspeicherung weniger eingreifend sind und gleichwohl einen mindestens ebenso hohen, wenn nicht sogar weitaus höheren Nutzen versprechen. Art. 3 Abs. 1 GG ist betroffen, weil der Gesetzgeber eine Vorratsspeicherung von Telekommunikationsdaten eingeführt hat, ohne zuvor diese Mittel ausgeschöpft zu haben. Durch ein solches Vorgehen werden sowohl die Telekommunikationsnutzer wie auch die Betreiber von Telekommunikationsnetzen benachteiligt, so dass ein Eingriff in die Rechte dieser Personen aus Art. 3 Abs. 1 GG vorliegt.

bb) Rechtfertigung

Es fragt sich, ob sich die Einführung einer Vorratsspeicherung als im Vergleich zu den genannten Alternativen kostengünstigere Maßnahme rechtfertigen ließe. Bei der Vornahme eines Kostenvergleichs sind richtigerweise nicht nur die unmittelbaren Kosten für den Staatshaushalt zu berücksichtigen, sondern auch mittelbare Kosten einer generellen Kommunikationsdatenspeicherung für den Bürger[894]. Deswegen ist ein Verzicht auf Präventivmaßnahmen nicht schon wegen deren Kosten für den Staatshaushalt gerechtfertigt. Eine generelle Kommunikationsdatenspeicherung in Deutschland würde laufende Kosten in Höhe eines zwei- bis dreistelligen Millionenbetrages pro Jahr verursachen[895], die sich letztlich weitgehend in höheren Preisen für die Inanspruchnahme von Telekommunikationsleistungen niederschlagen würden. Dass man mit Mitteln in dieser Größenordnung substanzielle Präventionsprogramme starten kann, liegt auf der Hand.

Als weiterer Rechtfertigungsgrund kommt in Betracht, dass eine Vorratsspeicherung sofort, Alternativen aber erst mittelfristig Nutzen entfalten könnten. Die Richtigkeit dieser Annahme unterstellt, ist freilich zu beachten, dass sofortige Wirkungen auf dem Gebiet des Zugriffs auf Telekommunikationsdaten nicht dringend erforderlich sind[896]. Hinzu kommt, dass Kriminelle schon nach kurzer Zeit lernen würden, eine Vorratsspeicherung zu umgehen, während die oben genannten Alternativen mittel- und

886 Jeserich, TK-Überwachung, 63 (71).
887 BMI/BMJ, Sicherheitsbericht 2001, 203.
888 BMI/BMJ, Sicherheitsbericht 2001, 203.
889 Bundesregierung, BT-Drs. 14/4173, 43 f.: „vorrangig international verbindliche Lösungen“.
890 Finnland in MDG, EU-Questionnaire (I), 18; ebenso für Deutschland Frank Gehde (LKA Berlin), c’t 19/2002, 127.
891 Finnland in MDG, EU-Questionnaire (I), 19.
892 Finnland in MDG, EU-Questionnaire (I), 19.
893 Jeserich (Leitender Oberstaatsanwalt bei der Generalstaatsanwaltschaft in Celle), TK-Überwachung in Zahlen und Fakten, 63 (71); Kubica (Leitender Kriminaldirektor beim BKA), Die Kriminalpolizei 9/2001.
894 Seite 101.
895 Seiten 89-90.
896 Seite 81.

langfristig einen nachhaltigen Nutzen erwarten lassen. Die Tatsache, dass eine Vorratsspeicherung von Telekommunikationsdaten schneller Wirkungen zeigen könnte, kann ihre Bevorzugung daher ebenfalls nicht rechtfertigen.

cc) Ergebnis

Die Einführung einer generellen Kommunikationsdatenspeicherung ist somit erst dann gerechtfertigt, wenn der Staat alle Mittel, die weniger eingreifend sind, insgesamt einen mindestens ebenso hohen Nutzen versprechen und keine höheren Kosten verursachen, ausgeschöpft hat. Ob und welche Mittel diese Voraussetzung im Einzelnen erfüllen, bedarf näherer Untersuchung. Wegen der Eingriffsintensität einer generellen Kommunikationsdatenspeicherung muss der Gesetzgeber vor ihrer Einführung entsprechende Untersuchungen vornehmen lassen und sodann in vertretbarer Weise entscheiden[897]. Die erforderlichen Untersuchungen setzen die Einführung einer generellen Kommunikationsdatenspeicherung nicht voraus[898]. Es liegt auch keine besondere Dringlichkeitssituation vor, in der die sofortige Einführung einer generellen Kommunikationsdatenspeicherung geboten ist. Somit sind die §§ 110a, 110b TKG mit Art. 3 Abs. 1 GG unvereinbar, weil es der Gesetzgeber versäumt hat, die verfügbaren Alternativen vorab zu untersuchen und gegebenenfalls auszuschöpfen.

e) Gleichbehandlung kleiner Telekommunikationsunternehmen mit anderen Telekommunikationsunternehmen

Die in den §§ 110a, 110b TKG vorgesehene, unterschiedslose Verpflichtung aller Anbieter von Telekommunikationsdiensten der dort genannten Arten zur Vorratsspeicherung von Kommunikationsdaten verstößt weiter gegen den Gleichheitssatz, weil damit „innerhalb der betroffenen Berufsgruppe nicht nur einzelne, aus dem Rahmen fallende Sonderfälle, sondern bestimmte, wenn auch zahlenmäßig begrenzte, Gruppen typischer Fälle ohne zureichende sachliche Gründe wesentlich stärker belastet“ werden[899]. In solchen Fällen liegt eine unzulässige Gleichbehandlung ungleicher Sachverhalte vor[900]. Es handelt sich um eine Ausnahme von dem Grundsatz, dass der Gesetzgeber ungleiche Sachverhalte aus Gründen der Praktikabilität grundsätzlich typisieren und die Mitglieder typischer Gruppen gleich behandeln darf[901].

Im vorliegenden Zusammenhang ist fraglich, ob eine Kommunikationsdatenspeicherungspflicht bestimmte Gruppen von Unternehmen wesentlich stärker belastet als die sonst betroffenen Unternehmen. Im Mobilfunkbereich werden sich ungewöhnlich schwerwiegend betroffene Unternehmen nicht finden lassen, weil der deutsche Mobilfunkmarkt von wenigen großen Netzbetreibern dominiert wird. Auch im Festnetzbereich gibt es nur vergleichsweise wenige Betreiber öffentlicher Telekommunikationsnetze. Es existiert zwar eine Vielzahl zum Teil kleiner Unternehmen, die Kapazitäten dieser Netzbetreiber weiter verkaufen (so genannte „Reseller“). Allerdings wird von diesen Unternehmen zum Zweck der Abrechnung schon bisher eine Aufzeichnung von Kommunikationsdaten durchgeführt, so dass in der Einführung einer Mindestspeicherfrist nur eine quantitative Ausweitung der Speicherung liegen würde. Kleine Reseller wären daher nur entsprechend dem von ihnen verkauften Gesprächsvolumen betroffen, so dass der Eintritt einer im Verhältnis erheblich stärkeren Belastung kleiner Unternehmen nicht zu erwarten ist.

Anders liegt es bei Betreibern privater Firmennetze oder von Telekommunikationseinrichtungen beispielsweise in Hotels oder Krankenhäusern. Eine Aufzeichnung von Kommunikationsdaten wird von diesen Betreibern bisher oft nicht durchgeführt[902].

In diesem Bereich ist allerdings problematisch, ob und inwieweit Unternehmen dieser Art durch eine Kommunikationsdatenspeicherungspflicht gerade in ihrer Berufsausübung beeinträchtigt werden. Selbst wenn die hohen Kosten einer Vorratsspeicherung Unternehmen dazu zwingen, auf das Angebot von Telekommunikation für Dritte zu verzichten, bedeutet dies nicht notwendig eine Beeinträchtigung der Ausübung ihres eigentlichen Berufs, etwa im Fall von Krankenhäusern. Nur in bestimmten Fällen lässt sich das Angebot von Telekommunikation für Dritte als von der beruflichen Tätigkeit eines Unternehmens erfasst sehen, etwa im Fall von Hotels und dem Betrieb von Firmennetzen für Dritte. In diesen Fällen ist es denkbar, dass nur größere Unternehmen dieser Art die mit einer generellen Vorratsspeicherung von Kommunikationsdaten verbundenen Kosten tragen können, während kleinere

897 Vgl. Seiten 31-32.

898 Für Untersuchungen über die Effektivität und Belastungsintensität einer Vorratsspeicherung von Telekommunikationsdaten siehe schon Seiten 33-34.

899 Vgl. BVerfGE 30, 292 (327).

900 BVerfGE 30, 292 (333).

901 J/P6-Jarass, Art. 3, Rn. 30 m.w.N.

902 BITKOM: Stellungnahme zur Gesetzesinitiative des Bundesrates vom 31.05.2002 (BR-Drs. 275/02), 12.08.2002, www.bitkom.org/files/documents/Position_BITKOM_Vorratsdatenspeicherung_u.a._12.08.2002.pdf, 8 f.

Unternehmen das Angebot von Telekommunikation aufgeben müssen. Im Fall von Hotels etwa bedeutet das fehlende Angebot von Telefonen einen gravierenden Wettbewerbsnachteil. Kleinere Betreiber von Firmennetzen für Dritte können sogar zur gänzlichen Aufgabe ihres Gewerbes gezwungen sein.

Im Internetbereich ist nur bezüglich kommerzieller Betreiber internationaler Internet-Backbones anzunehmen, dass diese Tätigkeit ausschließlich durch wenige große Unternehmen versehen wird. Das Vorsehen von Härteklauseln ist in diesem Bereich daher nicht erforderlich. In den übrigen Bereichen finden sich derart hohe Eingangsschwellen nicht, so dass es dort eine Vielzahl kleiner, unabhängiger Unternehmen gibt, die keine Finanzpolster aufweisen und von einer staatlichen Inpflichtnahme folglich empfindlich getroffen werden könnten[903]. Daran ändert die grundsätzliche Möglichkeit der Kostenabwälzung – soweit sie in der Praxis überhaupt besteht[904] – jedenfalls insoweit nichts, als sich etwa erforderliche Anlaufinvestitionen nur allmählich wieder amortisieren können, wenigstens für eine Übergangszeit aber aus eigenen Mitteln vorfinanziert werden müssen. In den Niederlanden sollen einige kleine Internet-Access-Provider an dieser Hürde gescheitert sein, als der Staat Auflagen zur Sicherstellung der Überwachbarkeit von Internetkommunikation machte. Dementsprechend ist auch in Deutschland davon auszugehen, dass eine bedeutende Zahl von kleinen Unternehmen und Organisationen nicht in der Lage ist, die Mittel aufzubringen, die erforderlich sind, um einer Kommunikationsdatenspeicherungspflicht nachzukommen.

Auf die Wettbewerbssituation von Kleinunternehmen wirken sich Kosten steigernde Belastungen von vornherein stärker aus als auf größere Unternehmen, die über eine gewisse Kapitaldecke verfügen und – im Fall von Konzernen – teilweise auch auf die Ressourcen verbundener Unternehmen zurückgreifen können[905]. Weil die großen Unternehmen am Markt das Preisniveau vorgeben, ist kleinen Unternehmen die Abwälzung von Überwachungskosten nur in geringerem Maße möglich als Großunternehmen[906]. Ein Großteil dieser Kosten stellt Fixkosten dar, deren Höhe von der Unternehmensgröße unabhängig ist[907]. Solche Kosten treffen Kleinunternehmen daher – gemessen an ihrem Kundenkreis, ihrer Größe und Kapitalausstattung – ungleich härter. Hinzu kommt, dass größere Unternehmen erforderliche Einrichtungen oder Leistungen in größeren Mengen einkaufen und dadurch niedrigere Preise aushandeln können. Der Größenvorteil von Großunternehmen wirkt sich auch bei den variablen Kosten und bei den Möglichkeiten, staatliche Anforderungen kostensparend umzusetzen, aus[908]. Größere Unternehmen werden den Kunden folglich günstigere Konditionen bieten können, was zu einem weiteren Nachteil der Kleinunternehmen führt, die oft gerade auf günstige Preise angewiesen sind, um im Wettbewerb bestehen zu können. Im Internetbereich stellt Werbung zudem oft die einzige Einnahmequelle von Kleinunternehmen dar. Diese Unternehmen können selbst eine geringe Kostenerhöhung an ihre Nutzer nicht weiter geben, weil die Anziehungskraft ihres Angebots gerade in dessen Unentgeltlichkeit liegt. Nach aktuellen Untersuchungen ist nur eine Minderheit von Internetnutzern zur Zahlung eines Entgelts für Internetdienste bereit. Dies gilt besonders für Dienste, die an anderer Stelle (z.B. im Ausland) kostenfrei abgeboten werden, etwa E-Mail- oder Chatdienste.

Aus diesen Gründen sind seitens der Kleinunternehmen Insolvenzen und ähnliche schwerste Belastungen ernsthaft zu befürchten, wenn die generelle Kommunikationsdatenspeicherungspflicht in Kraft tritt[909]. Da sich die Auswirkungen eines Gesetzes oft nicht sicher prognostizieren lassen und sich zumeist nur feststellen lässt, dass der Eintritt einer unzumutbaren – insbesondere existenzgefährdenden – Belastung typischer Gruppen von Betroffenen nicht auszuschließen ist, hat das Bundesverfassungsgericht entschieden, dass den Betroffenen unter diesen Umständen ein Abwarten bis zu dem möglichen Eintritt irreparabler Schäden unzumutbar ist, so dass eine Verletzung des Gleichheitssatzes schon dann

903 Home Office (UK), Retention (I), 2: „Smaller or niche-market firms might suffer disproportionately from a blanket requirement"; BITKOM: Stellungnahme zur Gesetzesinitiative des Bundesrates vom 31.05.2002 (BR-Drs. 275/02), 12.08.2002, www.bitkom.org/files/documents/Position_BITKOM_Vorratsdatenspeicherung_u.a._12 .08.2002.pdf, 8; G8 Workshop, Potential Consequences for Data Retention; vgl. auch Karpen, ZRP 2002, 443 (444) allgemein für kleine und mittlere Unternehmen.

904 Seite 91.

905 So schon BVerfGE 30, 292 (330 f.).

906 APIG, All Party Parliamentary Internet Group (UK): The Internet Society of England: APIG Response, 06.12.2002, www.apig.org.uk/isoc.pdf, 4.

907 APIG, Communications Data, 26.

908 Vgl. schon BVerfGE 30, 292 (330 f.).

909 APIG, All Party Parliamentary Internet Group (UK): The Internet Society of England: APIG Response, 06.12.2002, www.apig.org.uk/isoc.pdf, 4; ICC/UNICE/EICTA/INTUG, Common Industry Statement on Storage of Traffic Data for Law Enforcement Purposes, 04.06.2003, www.statewatch.org/news/2003/jun/CommonIndustryPositiondataretention.pdf, 8.

vorliegt, wenn ein Gesetz für den Fall des Eintritts unzumutbarer Belastungen keine Abhilfemöglichkeit vorsieht[910].

Dieses Risiko des Eintritts unzumutbarer Belastungen für Unternehmen der genannten Art lässt sich nur dann weitgehend ausschließen, wenn der Gesetzgeber die Kosten einer Kommunikationsdatenspeicherungspflicht für diese Unternehmen gering hält. Dies lässt sich einerseits durch staatliche Sach- oder Geldmittel erreichen oder andererseits dadurch, dass lediglich die Aufbewahrung von Logfiles, die mit bereits vorhandenen Einrichtungen erzeugt werden können, vorgeschrieben wird. Im letztgenannten Fall muss sich außerdem die Anzahl von Anfragen an Kleinunternehmen in engen Grenzen halten, von diesen dürften keine besonderen Antwortzeiten verlangt werden und die Unternehmen müssen von der Haftung freigestellt werden, wenn sie mit gespeicherten Daten nicht ebenso sicher umgehen können wie größere Unternehmen.

Der Nachteil dieser Möglichkeiten liegt im ersten Fall in der Belastung des Staatshaushaltes. Die Aufzeichnung von Kommunikationsdaten kann je nach Geschäftsmodell eines Unternehmens bisher nicht vorgesehen sein[911] und sich daher nur unter hohen Kosten realisieren lassen. Die zweite Option, nämlich Ausnahmen für Kleinunternehmen vorzusehen, führt zu erheblichen Effektivitätseinbußen. Es ist zu erwarten, dass sich gerade die organisierte Kriminalität Ausnahmen zunutze macht, indem sie gezielt Kleinunternehmen nutzt oder sogar selbst betreibt[912].

Wird keiner der vorgenannten Wege eingeschlagen, dann kann es zu unzumutbaren Belastungen betroffener Unternehmen kommen. Im Vergleich zum Ausmaß dieser Schwierigkeiten müssen Kosten- und Effektivitätserwägungen des Staates zurücktreten, zumal Maßnahmen der Telekommunikationsüberwachung in Deutschland nur in jeweils etwa 0,5-1% der Fälle Betreiber privater Telekommunikationsnetze oder Unternehmen im Internet-Bereich betreffen[913].

Art. 3 Abs. 1 GG gebietet es daher, die Belastung kleiner Internet-Access-Provider und Serverbetreiber in erträglichen Grenzen zu halten. Der Gesetzgeber hat einen Spielraum bezüglich der Frage, wie er dies sicherstellt. Unter dem Aspekt des Art. 10 Abs. 1 Var. 3 GG ist allerdings anzumerken, dass Ausnahmeklauseln für Kleinunternehmen, wie sie etwa in der TKÜV vorgesehen sind, empfindliche Effektivitätseinbußen zur Folge haben, welche die Unverhältnismäßigkeit des Eingriffs in Art. 10 Abs. 1 Var. 3 GG durch eine generelle Kommunikationsdatenspeicherung weiter verstärken würden. Diese Möglichkeit hat daher auszuscheiden, so dass eine obligatorische Vorratsspeicherung von Telekommunikationsdaten mit den Art. 3 Abs. 1, 12 Abs. 1 GG nur vereinbar ist, wenn für Kleinunternehmen der oben genannten Art eine weitgehende Kostenerstattung vorgesehen wird. Da das vorliegend angegriffene Gesetz dies nicht gewährleistet, verstößt es auch in dieser Hinsicht gegen Art. 3 Abs. 1 GG.

f) Ungleichbehandlung von Telekommunikationsunternehmen und ihren Kunden gegenüber der Allgemeinheit der Steuerzahler

aa) Eingriff in den Schutzbereich

Geschäftsmäßige Anbieter von Telekommunikationsdiensten und Telekommunikationsnutzer werden außerdem gegenüber sonstigen Personen ungerechtfertigt benachteiligt, weil das angegriffene Gesetz ihnen allein die Kosten einer Vorratsspeicherung von Telekommunikationsdaten aufbürdet[914]. Gemeinsamer Oberbegriff ist hier die Gruppe aller Personen, denen die Lasten staatlicher Aufgabenwahrnehmung aufgebürdet werden können. Durch eine generelle Kommunikationsdatenspeicherung ohne staatliche Kostenerstattung werden Telekommunikationsunternehmen und mittelbar auch ihre Kunden gegenüber sonstigen Personen benachteiligt, weil sie die mit der Speicherungspflicht verbundenen Kosten und sonstige Belastungen im Wesentlichen allein zu tragen haben. Darin liegt ein Eingriff in ihr Recht auf Gleichbehandlung aus Art. 3 Abs. 1 GG.

bb) Rechtfertigung

Was die Frage der Rechtfertigung anbelangt, so wird teilweise die Auffassung vertreten, eine Inpflichtnahme Privater zu öffentlichen Zwecken, die ohne Kostenerstattung erfolge, sei einer Sonderabgabe vergleichbar und daher nur zulässig, wenn die insoweit vom Bundesverfassungsgericht entwi-

910 BVerfGE 30, 292 (333).

911 Kommission, Discussion Paper for Expert's Meeting on Retention of Traffic Data (I); G8, Availability (I), Annex A: „It should be noted that the content of these logs might be subject to relevant business, technical and legal conditions; not all of the following data elements will be available in all logs.".

912 Lenz, Karl-Friedrich: Stellungnahme zur Anhörung der Kommission über die Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität, europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/Comments/kf_lenz.html.

913 Schulzki-Haddouti, Lauscher unter Beschuss, c't 09/2001, 24 ff.

914 Vgl. Friedrich, Verpflichtung, 182 f. m.w.N.

ckelten Kriterien vorlägen[915]. Zur Begründung wird vorgetragen, es mache keinen Unterschied, ob der Gesetzgeber Personen entschädigungslos in Anspruch nehme oder ob er eine Kostenerstattung vorsehe und die erstatteten Kosten im Wege einer Sonderabgabe wiederum von den Verpflichteten erhebe[916].

(1) Kommunikationsdatenspeicherungspflicht als entschädigungslose Inpflichtnahme Privater zu öffentlichen Zwecken

Die Verpflichtung privater Unternehmen zur Aufzeichnung und Vorhaltung von Telekommunikationsdaten für staatliche Behörden stellt eine Inpflichtnahme Privater zu öffentlichen Zwecken dar. Dies gilt unabhängig davon, ob den Unternehmen auch der eigene Zugriff auf die Datenbestände erlaubt ist[917].

Fraglich ist, ob eine Kostenerstattung oder wenigstens eine Entschädigung der betroffenen Unternehmen für die Vorratsspeicherung vorgesehen ist. Bisher kennt das deutsche Recht eine Entschädigungspflicht bei Auskunftanordnungen von Strafverfolgungsbehörden (§ 23 Abs. 1 S. 1 Nr. 2 JVEG) und von Nachrichtendiensten (§ 20 G10). Nach dem JVEG ist zu entschädigen, wer einem Beweiszwecken dienenden Ersuchen einer Strafverfolgungsbehörde um Auskunfterteilung nachkommt (§ 23 Abs. 1 S. 1 Nr. 2 JVEG). Nach den §§ 23 Abs. 2, 22 S. 1 JVEG kann für einen dazu eingesetzten Mitarbeiter Aufwendungsersatz in Höhe des gezahlten Gehalts verlangt werden, maximal aber 17 Euro pro Stunde und Mitarbeiter. Auch sonst erforderliche Aufwendungen werden ersetzt (§ 7 Abs. 1 S. 1 JVEG), allerdings nur, wenn sie ohne das Auskunftsersuchen nicht angefallen wären[918]. Die Entschädigung umfasst daher nicht die vorbeugende Vorhaltung von Personal und Einrichtungen[919] und bleibt infolgedessen regelmäßig erheblich hinter den tatsächlichen Kosten zurück[920]. So wird unter anderem für die Nutzung zusätzlicher Rechnerkapazitäten, etwa zur Durchführung einer Zielwahlsuche, keine Entschädigung gewährt[921].

§ 23 Abs. 1 S. 1 Nr. 4 Buchst. b JVEG sieht zwar eine Entschädigungspflicht für den Fall vor, dass Dritte „auf Grund eines Beweiszwecken dienenden Ersuchens der Strafverfolgungsbehörde [...] durch telekommunikationstechnische Maßnahmen die Ermittlung [...] der von einem Telekommunikationsanschluß hergestellten Verbindungen ermöglichen (Zählvergleichseinrichtung)“. Man wird dieser Regelung aber keinen Kostenerstattungsanspruch für den Fall einer generellen Kommunikationsdatenspeicherungspflicht entnehmen können. Dies würde nicht nur dem historischen Willen des Gesetzgebers, sondern auch dem Wortlaut widersprechen, der darauf abstellt, dass die Ermittlung der Daten erst auf Ersuchen der Strafverfolgungsbehörde, also im Einzelfall, erfolgt und nicht im Wege einer generellen Kommunikationsdatenspeicherung. Im Zeitalter digitaler Kommunikation kann man zudem von einer „Zählvergleichseinrichtung“ schon begrifflich nicht mehr sprechen.

Auch das angegriffene Gesetz sieht keinen Anspruch auf Kostenerstattung vor.

(2) Rechtfertigung als Sonderabgabe nach der Rechtsprechung des Bundesverfassungsgerichts

Geht man von dem Fehlen eines Kostenerstattungsanspruchs aus, dann richtet sich die Verfassungsmäßigkeit einer generellen Kommunikationsdatenspeicherungspflicht der oben dargestellten Meinung zufolge nach den Kriterien für die Zulässigkeit einer Sonderabgabe. Sonderabgaben bedürfen in einem Steuerstaat besonderer sachlicher Rechtfertigung[922]. Als Rechtfertigungsgründe kommen beispielsweise Ausgleichs- oder Lenkungszwecke in Betracht[923]. Wenn allerdings die Inpflichtnahme Privater zur Durchführung einer Kommunikationsdatenspeicherung ohne Kostenerstattung erfolgt, so soll dies weder Vorteile ausgleichen, die der Staat oder die Allgemeinheit Telekommunikationsunternehmen

915 BeckTKG-Ehmer, § 88, Rn. 51 m.w.N.; Welp, Überwachung und Kontrolle, 136 m.w.N.; „prima facie“ auch Schenke, AöR 125 (2000), 1 (39) m.w.N.; a.A. Germann, 576.

916 BeckTKG-Ehmer, § 88, Rn. 51 m.w.N.; Waechter, VerwArch 87 (1996), 68 (96).

917 Breyer, Vorratsspeicherung, 51 f.

918 Höver, Rn. 9.2.1.

919 Höver, Rn. 9.2.1; Pernice, DuD 2002, 207 (210); Germann, 575 f.; Koenig/Koch/Braun, K&R 2002, 289 (294).

920 Graf, Jürgen (Generalbundesanwalt), zitiert bei Neumann, Andreas: Internet Service Provider im Spannungsfeld zwischen Strafverfolgung und Datenschutz, Bericht von der Veranstaltung in Bonn am 26./27.02.2002, www.artikel5.de/-artikel/ecoveranstaltung2002.html; BITKOM: Stellungnahme zur Gesetzesinitiative des Bundesrates vom 31.05.2002 (BR-Drs. 275/02), 12.08.2002, www.bitkom.org/files/documents/-Position_BITKOM_Vorratsdatenspeicherung_u.a._12.08.2002.pdf, 4; BITKOM: Schriftliche Stellungnahme zur öffentlichen Anhörung am 09.02.2004 in Berlin zum Entwurf eines Telekommunikationsgesetzes (TKG), in Ausschussdrucksache 15(9)961, www.bitkom.org/files/documents/StN_BITKOM_TKG_Wirtschaftsausschuss_03.02.04.pdf, 20 (33): die gesetzliche Entschädigung decke durchschnittlich nur 2% der Kosten; ebenso die Deutsche Telekom AG a.a.O., 150 (164); vgl. auch Bundesrat, BR-Drs. 755/03, 35: es sei kein Kostenersatz „in nennenswertem Umfang“ vorgesehen.

921 OLG Stuttgart, NStZ 2001, 158; OLG Köln, NStZ-RR 2001, 31.

922 BVerfG, NVwZ 1996, 469 (471).

923 Zusammenfassend BVerfG, NVwZ 1996, 469 (471).

gewähren (Ausgleichsfunktion) noch soll es die betroffenen Unternehmen zu einem bestimmten Verhalten anhalten (Lenkungsfunktion). Eine Kostenerstattung unterbleibt vielmehr allein, um dem Staatshaushalt Ausgaben zu ersparen und die Finanzierbarkeit einer generellen Kommunikationsdatenspeicherung zu gewährleisten. Damit sind nach der aufgezeigten Meinung die Kriterien für die Zulässigkeit von Sonderabgaben mit Finanzierungsfunktion anzuwenden.

Nach der Rechtsprechung des Bundesverfassungsgerichts ist die Auferlegung von Sonderabgaben mit Finanzierungsfunktion nur dann zulässig, wenn die belastete Gruppe „durch eine gemeinsame, in der Rechtsordnung oder in der gesellschaftlichen Wirklichkeit vorgegebene Interessenlage oder durch besondere gemeinsame Gegebenheiten von der Allgemeinheit und anderen Gruppen abgrenzbar ist“[924], wenn sie dem mit der Abgabenerhebung verfolgten Zweck evident näher steht als jede andere Gruppe oder die Allgemeinheit der Steuerzahler[925], wenn die Aufgabe, die mit Hilfe des Abgabenaufkommens erfüllt werden soll, ganz überwiegend in die Sachverantwortung der belasteten Gruppe fällt und nicht der staatlichen Gesamtverantwortung zuzuordnen ist[926] und wenn die erzielten Mittel entweder gruppennützig verwendet werden oder „die Natur der Sache eine finanzielle Inanspruchnahme der Abgabenpflichtigen zugunsten fremder Begünstigter aus triftigen Gründen eindeutig rechtfertigt“[927].

Die Abgrenzbarkeit der Gruppe der Anbieter von Telekommunikationsdiensten ist zunächst gegeben. Das Kriterium der besonderen Sachnähe dieser Gruppe kann man hingegen nur dann als erfüllt ansehen, wenn die Anbieter von Telekommunikation durch ihr Angebot eine Quelle besonderer Gefahren für bestimmte Rechtsgüter schaffen. Um dies zu begründen, könnte man auf die besonderen Eigenschaften der Telekommunikation verweisen, die sich Kriminelle in vielen Fällen zunutze machen[928]. Daraus ließe sich eine mittelbare Rechtsgutsgefährdung durch das Angebot von Telekommunikation herleiten.

Gegen eine solche Argumentation ist jedoch anzuführen, dass § 9 Abs. 1 TDG deutlich der Gedanke einer prinzipiellen Nichtverantwortlichkeit der Anbieter von Telediensten zugrunde liegt, wenn er bestimmt: „Diensteanbieter sind für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie 1. die Übermittlung nicht veranlasst, 2. den Adressaten der übermittelten Informationen nicht ausgewählt und 3. die übermittelten Informationen nicht ausgewählt oder verändert haben. Satz 1 findet keine Anwendung, wenn der Diensteanbieter absichtlich mit einem der Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen.“ Die Begründung zur ursprünglichen Gesetzesfassung führte dazu aus[929]: „Dem Diensteanbieter, der fremde Inhalte lediglich, ohne auf sie Einfluss nehmen zu können, zu dem abrufenden Nutzer durchleitet, obliegt es nicht, für diese Inhalte einzutreten. Er soll nicht anders behandelt werden als ein Anbieter von Telekommunikationsdienstleistungen. Denn der bloße Zugangsvermittler leistet ebenfalls keinen eigenen Tatbeitrag.“ Die Begründung zur Neufassung stellt fest[930]: „Diese Tätigkeit ist automatischer Art, bei der der Diensteanbieter in der Regel keine Kenntnis über die weitergeleitete oder kurzzeitig zwischengespeicherte Information hat und diese auch nicht kontrolliert. Bei dem automatisiert ablaufenden Prozess trifft der Diensteanbieter im Hinblick auf die Informationen keine eigene Entscheidung. [...] [I]n den Fällen, in denen der Diensteanbieter keine Kontrolle ausübt und keine Kenntnis von der Information haben kann, kann sie ihm auch nicht im Sinne eigener Verantwortlichkeit zugerechnet werden.“ Diese Ausführungen betreffen zwar unmittelbar nur Teledienste. Die Lage stellt sich bei Telekommunikationsdiensten aber ganz genauso dar[931]. Der Auffassung des Gesetzgebers zufolge sind Betreiber von Telekommunikationsdiensten daher grundsätzlich nicht für die Nutzung ihrer Dienste zu rechtswidrigen Zwecken verantwortlich zu machen.

Die Annahme, dass Telekommunikationsnetze eine besondere Rechtsgutsgefahr darstellten oder erhöhten, ist folglich abzulehnen[932]. Die aus Telekommunikationsnetzen resultierenden Gefahren erscheinen nicht höher als die aus anderen neutralen Tätigkeiten wie Alltagsverrichtungen einer Bank, eines Verkehrs- oder eines Versorgungsunternehmen resultierenden Gefahren. Auch die Tätigkeit eines Automobilherstellers ist beispielsweise kausal dafür, dass Autos als Fluchtfahrzeuge missbraucht werden können, ohne dass man Automobilhersteller deswegen besonders in die Pflicht nehmen dürf-

924 BVerfGE 55, 274 (305 f.).
925 BVerfGE 55, 274 (306).
926 BVerfGE 55, 274 (306).
927 BVerfGE 55, 274 (306).
928 Welp, Überwachung und Kontrolle, 137.
929 BT-Drs. 13/7385, 1 (20).
930 BT-Drs. 14/6098, 1 (24).
931 Vgl. BT-Drs. 13/7385, 1 (20).
932 MPI, VATM-Gutachten (I), 20; Germann, 576; Werner, Befugnisse der Sicherheitsbehörden, 51; ähnlich Schenke, AöR 125 (2000), 1 (39); für Betreiber von Telekommunikationsanlagen auch Kube/Schütze, CR 2003, 663 (669).

te[933]. Ebenso wenig ist es gerechtfertigt, Automobilhändlern die Kosten aufzuerlegen, welche dem Staat durch die Verfolgung von Geschwindigkeitsüberschreitungen entstehen[934]. Nicht anders verhält es sich bei dem Missbrauch von Telekommunikationsnetzen. Solche mit Alltagstätigkeiten verbundene Gefahren sind in den Bereich des allgemeinen Lebensrisikos zu verweisen, der keine besondere Verantwortlichkeit begründen kann[935].

Es kann somit keine Rede davon sein, dass die von einer Vorratsspeicherungspflicht belasteten Unternehmen dem mit der Vorratsspeicherung verfolgten Zweck evident näher stünden als die Allgemeinheit der Steuerzahler. Ebenso wenig fällt die Aufgabe der Strafverfolgung und der Gefahrenabwehr ganz überwiegend in die Sachverantwortung der belasteten Unternehmen[936].

Was das Kriterium der Gruppennützigkeit angeht, so kommt ein Sondernutzen durch eine generelle Kommunikationsdatenspeicherung insoweit in Betracht, als sie das Vertrauen der Nutzer stärken und dadurch die Nutzung der Telekommunikationsnetze insgesamt fördern könnte[937]. Dieser Zusammenhang kann allerdings bestenfalls indirekter Art sein, weil er nicht Ziel der Kommunikationsdatenspeicherung ist, sondern allenfalls ein möglicher Nebeneffekt. Es ist nicht nur in hohem Maße unsicher, ob eine generelle Kommunikationsdatenspeicherung tatsächlich zu einem niedrigeren Kriminalitätsniveau führt[938]. Noch unsicherer ist es, ob sich ein objektiv niedrigeres Kriminalitätsniveau auch auf das subjektive Nutzervertrauen und letztlich auf das Maß an Inanspruchnahme der Telekommunikationsnetze durchschlägt. Umgekehrt gibt es Untersuchungen, die auf die Abwesenheit eines solchen Zusammenhangs hindeuten[939]. Die genannte These ist daher mit so vielen Unsicherheitsfaktoren behaftet, dass sie – vorbehaltlich neuer Forschungserkenntnisse – abzulehnen ist[940].

Zu überlegen ist außerdem, ob eine generelle Kommunikationsdatenspeicherung in besonderem Maße Betreiber von an Telekommunikationsnetze angeschlossenen Computersystemen, insbesondere Betreiber von Internet-Servern, schützt. Allein diese Personengruppe ist nämlich von Netzkriminalität im engeren Sinne betroffen. Dieser Zusammenhang rechtfertigt eine Sonderbelastung der Betreiber solcher Systeme allerdings nur dann, wenn diese Systeme störanfälliger und kriminalitätsgefährdeter sind als andere Anlagen. Nur in diesem Fall dürfen die Kosten von Maßnahmen, die über den Schutz der Allgemeinheit hinaus gehen, anteilig auf die Serverbetreiber abgewälzt werden. Soweit Serverbetreiber von Maßnahmen nicht in besonderer Weise profitieren, sind die Kosten dagegen von der Allgemeinheit zu tragen[941]. Letztlich kann die Frage im vorliegenden Zusammenhang offen bleiben, weil von einer generellen Kommunikationsdatenspeicherung keine merkliche Schutzwirkung zugunsten der Betreiber von Servern zu erwarten ist[942]. Einen wirksamen Schutz auf diesem Gebiet erlauben nur technisch-organisatorische Maßnahmen der Betreiber selbst[943].

Für andere Personen oder Unternehmen, die zu einer Vorratsspeicherung verpflichtet wären, ist ein möglicher Sondernutzen von vornherein nicht zu erkennen. Telefongesellschaften und Internet-Provider etwa sind Netzkriminalität im engeren Sinne grundsätzlich nicht ausgesetzt, weil ihre Einrichtungen für Computerangriffe regelmäßig unzugänglich sind. Auch sonst ist ein Sondernutzen für diese Gruppe nicht zu erkennen, so dass eine entschädigungslose Inanspruchnahme der betroffenen Unternehmen zugunsten der Allgemeinheit durchweg ungerechtfertigt ist.

Soweit das Bundesverfassungsgericht Unternehmen auf die Möglichkeit einer Abwälzung von Kosten auf ihre Kunden verweist, ist es denkbar, die Kriterien der besonderen Sachnähe und der Gruppennützigkeit auf die Telekommunikationsnutzer anzuwenden, welche die Kosten einer generellen Kommunikationsdatenspeicherung letztlich zu tragen haben[944]. Tut man dies, so gelangt man zu dem Ergebnis, dass auch auf Seiten der Telekommunikationsnutzer keine spezifische Nähe zu dem Miss-

933 So Mobilkom Austria und Telekom Austria in Österr. Verfassungsgerichtshof, G 37/02-16 u.a. vom 27.02.2003, S. 18 f., www.epic.org/privacy/intl/austrian_ct_dec_022703.html.

934 Mobilkom Austria und Telekom Austria in Österr. Verfassungsgerichtshof, G 37/02-16 u.a. vom 27.02.2003, S. 19, www.epic.org/privacy/intl/austrian_ct_dec_022703.html.

935 Weichert, Terrorismusbekämpfungsgesetze (I), Punkt I.

936 Im Ergebnis auch BITKOM: Stellungnahme zur Gesetzesinitiative des Bundesrates vom 31.05.2002 (BR-Drs. 275/02), 12.08.2002, www.bitkom.org/files/documents/Position_BITKOM_Vorratsdatenspeicherung_u.a._12.08.2002.pdf, 9.

937 Seiten 25-26.

938 Seiten 49-55.

939 Breyer, Vorratsspeicherung, 52.

940 Im Ergebnis auch Schenke, AöR 125 (2000), 1 (39).

941 Vgl. BVerwGE 112, 194 (205).

942 Seite 55.

943 Seiten 112-113.

944 BeckTKG-Ehmer, § 88, Rn. 54 m.w.N.; der Sache nach wohl auch Pernice, Ina (Deutscher Industrie- und Handelskammertag) in Bundestag, Öffentliche Anhörung zum Thema Cyber-Crime/TKÜV (I), 14.

brauch von Telekommunikationseinrichtungen durch einzelne unter ihnen vorliegt[945]. Von einer besonderen Gruppennützigkeit lässt sich ebenso wenig sprechen[946].

Überhaupt sind kaum Menschen denkbar, die sich jeglicher Telekommunikation enthalten, so dass schon fraglich ist, ob man hier von einer bestimmten Gruppe sprechen kann. In seiner Kohlepfennig-Entscheidung hat das Bundesverfassungsgericht argumentiert, das Interesse an einer funktionsfähigen Energieversorgung sei ein Allgemeininteresse, das nicht im Wege einer Sonderabgabe, sondern nur durch Steuermittel befriedigt werden dürfe[947]. Auch in der Feuerwehrabgabenentscheidung heißt es: „Das Feuerwehrwesen ist eine öffentliche Angelegenheit, deren Lasten nur die Allgemeinheit treffen dürfen und die deshalb [...] nur mit von der Allgemeinheit zu erbringenden Mitteln, im Wesentlichen also durch die Gemeinlast Steuer, finanziert werden darf (vgl. BVerfGE 55, 274 [306]; 82, 159 [180]). Wird in einem solchen Fall nur ein abgegrenzter Personenkreis mit der Abgabe belastet, so verstößt dies auch gegen den allgemeinen Gleichheitssatz nach Art. 3 Abs. 1 GG (vgl. auch BVerfGE 9, 291 [301])."[948] Diese Ausführungen gelten grundsätzlich auch für die Inpflichtnahme Privater im Bereich der Telekommunikation[949]. Sinngemäß haben dies der französische Verfassungsgerichtshof im Dezember 2000[950] und der österreichische Verfassungsgerichtshof im Februar 2003[951] bereits entschieden. Auch in Italien und den USA trägt der Staat die Kosten für die Vorhaltung von Überwachungseinrichtungen durch Privatunternehmen[952]. Kommt eine generelle Vorratsspeicherung von Telekommunikationsdaten danach hauptsächlich der Allgemeinheit zugute, dann dürfen ihre Kosten auch nicht allein den betroffenen Unternehmen oder ihren Kunden auferlegt werden.

Gemessen an den Kriterien für die Zulässigkeit einer Sonderabgabe ist es demnach unzulässig, die Telekommunikationsanbieter zur Finanzierung einer generellen Kommunikationsdatenspeicherung heranzuziehen.

(3) Anwendung auf tatsächliche Inpflichtnahmen

Fraglich ist, ob hieraus zwangsläufig auch die Unzulässigkeit ihrer entschädigungslosen Heranziehung zur Mitwirkung bei einer generellen Kommunikationsdatenspeicherung folgt. Das Bundesverfassungsgericht wendet die Kriterien für die Zulässigkeit einer Sonderabgabe nicht auf tatsächliche Inpflichtnahmen Privater zu öffentlichen Zwecken an. In solchen Fällen prüft es nur die Verhältnismäßigkeit der Inpflichtnahme[953]. Für eine enge Auslegung der Rechtsprechung zu Sonderabgaben spricht, dass sich diese auf das Argument stützt, dass das Grundgesetz grundsätzlich abschließend regele, auf welche Weise der Staat Einnahmen erzielen dürfe[954]. Dieser Gesichtspunkt trifft auf die tatsächliche Inpflichtnahme Privater nicht zu, weil der Staat auf diese Weise keine Einnahmen erzielt.

Ein weiteres Argument, welches das Bundesverfassungsgericht in Bezug auf Sonderabgaben heran zieht, ist demgegenüber ohne weiteres auf Inpflichtnahmen Privater übertragbar. Der Grundsatz der Vollständigkeit des Haushaltsplans[955], welcher die Transparenz der Kosten staatlicher Aktivitäten und die Überschaubarkeit und Kontrolle der dem Bürger auferlegten Lasten gewährleisten soll, ist nämlich in beiden Fällen beeinträchtigt[956].

Ein Grund für die Zurückhaltung des Bundesverfassungsgerichts bei der Ausweitung seiner Rechtsprechung zu Sonderabgaben mag darin liegen, dass die staatliche Inpflichtnahme Privater zu öffentlichen Zwecken weit verbreitet ist und eine restriktive verfassungsrechtliche Beurteilung daher weitreichende Konsequenzen hätte[957]. Beispiele solcher Pflichten sind die Inanspruchnahme der Banken zum Abzug der Kapitalertragssteuer, die Heranziehung der Arbeitgeber zum Lohnsteuerabzug und zur Abführung von Sozialversicherungsbeiträgen, die Verpflichtung von Versicherungsunternehmen zur Einbehaltung der Versicherungssteuer und die Auferlegung von Bevorratungspflichten für Ölimpor-

945 BeckTKG-Ehmer, § 88, Rn. 54; Welp, Überwachung und Kontrolle, 137.
946 Welp, Überwachung und Kontrolle, 137.
947 BVerfGE 91, 186 (206); vgl. schon BVerfGE 23, 12 (23); ähnlich für Betreiber elektrischer und elektronischer Geräte BVerwGE 112, 194 (205).
948 BVerfGE 92, 91 (121).
949 BeckTKG-Ehmer, § 88, Rn. 55.
950 Conseil constitutionnel, 2000-441 DC vom 28.12.2000, www.conseil-constitutionnel.fr/decision/2000/2000441/-2000441dc.htm.
951 Österr. Verfassungsgerichtshof, G 37/02-16 u.a. vom 27.02.2003, www.epic.org/privacy/intl/austrian_ct_dec_022703.html.
952 wik-Consult, Studie (I), 41, 50 und 89.
953 Etwa BVerfGE 30, 292 (315).
954 BVerfGE 55, 274 (299 f.) spricht von einer Gefahr der Aushöhlung der Finanzverfassung durch Sonderabgaben.
955 BVerfG, NVwZ 1996, 469 (471).
956 Elicker, NVwZ 2003, 304 (306).
957 Vgl. VG Köln, CR 2000, 747 (750).

teure[958]. Eine besondere Verantwortlichkeit wegen Schaffung einer Gefahrenquelle ließe sich wohl in keinem dieser Fälle begründen.

Für eine Gleichbehandlung beider Fälle kann man geltend machen, dass eine Inanspruchnahme Privater ohne Kostenerstattung einer Inanspruchnahme mit Kostenerstattung, bei der die erstatteten Kosten im Wege einer Sonderabgabe von den Verpflichteten wieder erhoben werden, gleich kommt[959]. Weiter kann man anführen, dass die Inpflichtnahme Privater in Verbindung mit der aus einer Sonderabgabe finanzierten Kostenerstattung den betroffenen Unternehmen eher zumutbar sein kann als eine entschädigungslose Inpflichtnahme ohne Sonderabgabe. Das gilt insbesondere deswegen, weil eine Sonderabgabe Ausnahmen für besonders hart betroffene Unternehmen zulassen kann, ohne zu Effektivitätseinbußen zu führen. So kann man beispielsweise kleine Internet-Access-Provider von einer Sonderabgabe zur Finanzierung einer generellen Kommunikationsdatenspeicherung ausnehmen, während ihre Befreiung von der Speicherungspflicht selbst nicht ohne Effektivitätseinbußen möglich ist. Kann damit aber die Auferlegung einer Sonderabgabe für die Gruppe der Betroffenen insgesamt weniger belastend sein, dann können für die Zulässigkeit einer Sonderabgabe auch keine strengeren Kriterien gelten als für die Zulässigkeit einer entschädigungslosen Inpflichtnahme.

Es ist demnach überzeugender, beide Fälle gleich zu behandeln[960]. Ein durchgreifender sachlicher Grund für eine Unterscheidung ist nicht ersichtlich. Dies gilt gerade für eine Vorratsspeicherungspflicht, deren Schwerpunkt nicht in der Auferlegung von Hilfsdiensten liegt – die Speicherung von Telekommunikationsdaten könnte der Staat auch selbst vornehmen – sondern in der Abwälzung der hohen, damit verbundenen Kosten.

(4) Gemeinsame Rechtfertigungskriterien

Sind Sonderabgaben und entschädigungslose Inpflichtnahmen somit gleich zu behandeln, so bedeutet dies noch nicht, dass die engen Kriterien des Bundesverfassungsgerichts zur Zulässigkeit von Sonderabgaben zu akzeptieren sind. Vielmehr kann die verbreitete Inpflichtnahme Privater umgekehrt Anlass sein, auch die finanzielle Heranziehung Privater im Wege von Sonderabgaben in höherem Maße zuzulassen als es das Bundesverfassungsgericht bisher tut.

Schon die Abgrenzung der „Sonderabgaben“ von den Steuern ist nicht unproblematisch[961]. Wann das Bundesverfassungsgericht eine Geldleistungspflicht als Sonderabgabe ansieht und dementsprechend strenge Kriterien anwendet, lässt sich nicht eindeutig vorhersehen. Nach § 3 AO sind Steuern „Geldleistungen, die nicht eine Gegenleistung für eine besondere Leistung darstellen und von einem öffentlich-rechtlichen Gemeinwesen zur Erzielung von Einnahmen allen auferlegt werden, bei denen der Tatbestand zutrifft, an den das Gesetz die Leistungspflicht knüpft; die Erzielung von Einnahmen kann Nebenzweck sein.“ Worin sich hiervon eine Sonderabgabe unterscheiden soll, ist nicht ersichtlich.

Zwar mag der Kreis der von einer Sonderabgabe Betroffenen klein sein. Das kann aber auch bei besonderen Steuern der Fall sein (z.B. Spielbankenabgabe). Es kann legitime Gründe dafür geben, einem kleinen Personenkreis eine besondere Abgabenlast aufzuerlegen. Im heutigen Zeitalter der Globalisierung kann etwa der Gesichtspunkt maßgeblich sein, dass Rechtssubjekte einer bestimmten Besteuerung nicht durch Ausweichen in das Ausland entgehen können. Ein weiterer Gesichtspunkt kann die besondere Leistungsfähigkeit einzelner Steuersubjekte sein, etwa wenn deren Tätigkeit besonders profitabel ist. Weiterhin kann vorrangig eine Lenkungswirkung angestrebt sein, die es erforderlich macht, gerade bestimmte Personen in Anspruch zu nehmen.

Festzuhalten bleibt, dass es nicht gerechtfertigt ist, die Zulässigkeit der Inanspruchnahme einzelner Personen davon abhängig zu machen, ob diesen Personen aufgrund ihrer spezifischen Sachnähe eine Kostenverantwortung zugeteilt werden kann und ob die Einnahmen gruppennützig verwendet werden. Stattdessen sind die allgemeinen Kriterien über die Zulässigkeit von Steuern anzuwenden, die vornehmlich auf die Verhältnismäßigkeit der Belastung[962] und auf die Gleichmäßigkeit der Besteuerung[963] abstellen. Diese Kriterien sind sowohl in Fällen von Sonderabgaben wie auch in Fällen der tatsächlichen Inpflichtnahme Privater zu öffentlichen Zwecken anzuwenden, da sich diese beiden Fallgruppen – wie oben dargelegt – nicht maßgeblich unterscheiden.

---

958 Beispiele nach BVerfGE 73, 102 (119 f.).

959 Vgl. Nachweise auf Seite 120, Fn. 915.

960 So auch Friedrich, Verpflichtung, 184 m.w.N.; Friauf, FS Jahrreiß, 45 (56 f.); Waechter, VerwArch 87 (1996), 68 (76); Elicker, NVwZ 2003, 304 (306); a.A. VG Köln, CR 2000, 747 (750).

961 BVerfGE 50, 274 (300): „Abgrenzungsprobleme“; BVerfG, NVwZ 1996, 469 (471): „große Ähnlichkeit“.

962 BVerfGE 91, 207 (221).

963 BVerfGE 66, 214 (223): „Gebot der Steuergerechtigkeit“.

(5) Rechtfertigung im Fall einer Vorratsspeicherung

Im vorliegenden Zusammenhang ist daher eine Prüfung des allgemeinen Gleichheitssatzes vorzunehmen[964]. In Bezug auf den Rechtfertigungsmaßstab liegt eine eindeutige Anknüpfung an Personengruppen – nämlich an die Gruppe der Telekommunikationsunternehmen – und nicht nur an Sachverhalte vor. Wie gezeigt, greift eine Pflicht zur Vorratsspeicherung von Telekommunikationsdaten ohne Kostenerstattung auch intensiv in das Grundrecht der Telekommunikationsunternehmen aus Art. 12 Abs. 1 GG ein[965]. Es ist daher eine Verhältnismäßigkeitsprüfung vorzunehmen. Das Gleiche gilt, wenn man auf die Kunden der Telekommunikationsunternehmen abstellt[966].

Die tatsächliche Inpflichtnahme Privater hat das Bundesverfassungsgericht mitunter damit gerechtfertigt, dass die normativ vorgeschriebene Tätigkeit an diejenige Tätigkeit angelehnt sei, die eine Person ohnehin verrichte[967]. In der Tat mag es volkswirtschaftlich gesehen Sinn machen, Telekommunikationsunternehmen zur Durchführung der Telekommunikationsüberwachung zu verpflichten anstatt ein kompliziertes staatliches Einsatzsystem aufzubauen. Dieser Einsparungseffekt ist allerdings auch dann zu erzielen, wenn den betroffenen Unternehmen ihre Kosten erstattet werden, so dass die bloße Tatsache der Berufsnähe keine entschädigungslose Inpflichtnahme rechtfertigt.

Nach dem oben Gesagten[968] ist auch sonst kein Grund ersichtlich, der nach Art und Gewicht die Belastung der beteiligten Unternehmen oder mittelbar ihrer Kunden mit den Kosten einer Kommunikationsdatenspeicherung zu staatlichen Zwecken rechtfertigen kann. Die Abwehr von Gefahren und die Ahndung von Straftaten ist eine Aufgabe der Allgemeinheit, deren Lasten nur die Allgemeinheit treffen dürfen und die deshalb im Wesentlichen nur mit Steuermitteln finanziert werden darf[969]. Die abweichende Regelung des angegriffenen Gesetzes ist mit Art. 3 Abs. 1 GG unvereinbar.

964 Vgl. auch Friedrich, Verpflichtung, 174 für die Vorhaltung von Überwachungseinrichtungen.
965 Seiten 89-90.
966 Seite 100.
967 BVerfGE 30, 292 (324 f.).
968 Seiten 122-123.
969 Friedrich, Verpflichtung, 183 m.w.N.; MPI, VATM-Gutachten (I), 19 ff. und 26; allgemein für Staatsaufgaben BVerfGE 23, 12 (23).

D. EG-Richtlinie 2006/24/EG

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.[970] Die anhängige Nichtigkeitsklage 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 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 Gericht 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 Ausführungen unter Punkt B.II.1 oben verwiesen.[971]

970 Siehe Seite 10 ff.
971 Seite 10

E. Annahmevoraussetzungen

Der Verfassungsbeschwerde kommt grundsätzliche Bedeutung zu, weil sie verfassungsrechtliche Fragen aufwirft, die sich nicht ohne weiteres aus dem Grundgesetz beantworten lassen. Insoweit wird auf die obigen Ausführungen verwiesen. Dass die aufgeworfenen Fragen über den Einzelfall hinaus für alle Nutzer der modernen Kommunikationstechnik dauerhaft von Bedeutung sind, liegt auf der Hand.

Die Annahme der Verfassungsbeschwerde ist auch zur Durchsetzung der verletzten Grundrechte angezeigt. Die Grundrechtsverletzung hat, wie oben ausgeführt, in Anbetracht der hohen Eingriffsintensität besonderes Gewicht. Zudem hat sich der Gesetzgeber bewusst über Warnungen hinsichtlich der Vereinbarkeit mit dem Grundgesetz hinweg gesetzt.

F. Einstweilige Anordnung

I. Offensichtliche Begründetheit

Der Antrag auf Erlass einer einstweiligen Anordnung (§ 32 BVerfGG) ist begründet, weil eine systematische, verdachtslose Speicherung personenbezogener Daten auf Vorrat mit den Grundrechten des Grundgesetzes offensichtlich unvereinbar ist. Dies ergibt sich bereits aus der ständigen Rechtsprechung des Bundesverfassungsgerichts zum strikten Verbot einer Speicherung personenbezogener Daten auf Vorrat.

II. Folgenabwägung

Sollte das Gericht gleichwohl von einem offenem Ausgang des Verfassungsbeschwerdeverfahrens ausgehen, ist der Antrag auf Erlass einer einstweiligen Anordnung ebenfalls begründet. Die Begründetheit hängt in diesem Fall von der Folgenbeurteilung und -abwägung ab. Dabei fällt nicht nur die Schwere des Eingriffs in die Rechtsposition der Beschwerdeführer ins Gewicht. Vielmehr sind auch die für den Anordnungserlaß sprechenden Interessen anderer Grundrechtsträger und der Allgemeinheit zu berücksichtigen. Die im Falle der Ablehnung einer einstweiligen Anordnung zu erwartenden Nachteile müssen schwer im Sinne des § 32 Abs. 1 BVerfGG sein und gegenüber den Nachteilen, die einträten, wenn eine einstweilige Anordnung erlassen würde, die Verfassungsbeschwerde aber keinen Erfolg hätte, überwiegen.[972]

Bliebe Art. 2 des angegriffenen Gesetzes in Kraft und hätte die Verfassungsbeschwerde im Hauptsacheverfahren Erfolg, würden in der Zwischenzeit die Umstände der Telekommunikation der Beschwerdeführer und praktisch aller Bürger der Bundesrepublik Deutschland aufgezeichnet. Dies würde Millionen von Einzelgesprächen und in der Gesamtheit die Telekommunikation der gesamten Bevölkerung betreffen. Daraus ergäben sich – wie oben aufgezeigt – gravierende Nachteile. Aufgrund der Speicherpflichten ist in verschiedenen Fällen mit weiteren Ermittlungsmaßnahmen zu rechnen, die erhebliche Nachteile mit sich bringen können. Die nachteiligen Folgen wären irreversibel, da sie mit der erfolgenden Auswertung und mit deren Befürchtung einträten. Die Befürchtung einer Überwachung mit der Gefahr einer späteren Auswertung, etwaigen Übermittlung und weiterer Verwendung durch andere Behörden kann bei den Grundrechtsträgern schon im Vorfeld zu Kommunikationsstörungen und zu Verhaltensanpassungen führen. Hier sind nicht nur die individuellen Beeinträchtigungen einer Vielzahl einzelner Grundrechtsträger zu berücksichtigen. Vielmehr betrifft die Protokollierung des Fernmeldeverkehrs auch die Kommunikationsfreiheit und das Kommunikationsverhalten der Telekommunikationsteilnehmer insgesamt. Das würde nicht nur die Entfaltungschancen der Einzelnen beeinträchtigen, sondern auch das Gemeinwohl.

Würde der Vollzug der angegriffenen Regelung vorläufig ausgesetzt, erwiese sich die Verfassungsbeschwerde aber später als unbegründet, würden die Umstände der Telekommunikation nicht auf Vorrat gespeichert und könnten dementsprechend teilweise nicht abgerufen werden. Damit entfiele die Möglichkeit, aufgezeichnete Kontakte zu Zwecken der Strafverfolgung auszuwerten und die Informationen zu nutzen. Darüber hinaus wäre die Möglichkeit einer nachträglichen Auswertung versperrt. Gleichwohl bliebe die bestehende Möglichkeit des Zugriffs auf Verkehrsdaten, die zu Abrechnungszwecken gespeichert sind oder auf richterliche Anordnung gespeichert werden (§ 100g StPO), erhalten. Diese Möglichkeit hat in den letzten Jahren eine wirksame Strafrechtspflege gesichert. Im Bereich telekommunikativ begangener Straftaten ist die Aufklärungsquote den einschlägigen Statistiken zufolge nicht niedriger, sondern höher als im Durchschnitt (55%). In den Bereichen Internetbetrug und Softwarepiraterie liegt die Aufklärungsquote sogar bei über 80%.

Wägt man die Folgen ab, wiegen die Nachteile im Falle der Ablehnung der begehrten Anordnung weniger schwer als die Nachteile im Falle ihres Erlasses. Die durch die Erwartung einer Überwachung hervorgerufenen Befürchtungen und damit verbundene Kommunikationsstörungen und Verhaltensanpassungen sind gravierend. Die von der Vorratsspeicherung drohende Störung des Kommunikationsverhaltens wäre besonders groß, weil der Einzelne befürchten müßte, einer Kenntnisnahme und Verwertung seiner privaten oder beruflichen Kontakte ausgesetzt zu sein, ohne entsprechende Verdachtsmomente geliefert zu haben. Würden in einer nicht unbedeutenden Anzahl von Fällen Ermittlungsmaßnahmen und Informations- und Datenverarbeitungsvorgänge aufgrund von Verdachtsanhaltspunkten erfolgen, die sich im Ergebnis als strafrechtlich irrelevant erwiesen, wären Beeinträchtigungen

972 BVerfGE 93, 181 (186 f.).

der Grundrechtsträger zu besorgen, ohne daß dem ein ins Gewicht fallender Nutzen auf seiten der Sicherheitsbelange gegenüberstünde. Insoweit kann ein Überwiegen der Belange der Strafverfolgung nicht angenommen werden. Durch die Einschränkung wird die Strafverfolgung gegenüber dem früheren Rechtszustand nicht zusätzlich erschwert. Hat die Verfassungsbeschwerde keinen Erfolg, so ist die durch den Erlass der einstweiligen Anordnung entstehende Informationslücke schließbar, während die Nachteile für die von der Auswertung und ihren Folgen Betroffenen großenteils nicht mehr reversibel wären.

III. Richtlinie 2006/24/EG

Das Europarecht hindert die einstweilige Aussetzung des deutschen Umsetzungsgesetzes bereits deshalb nicht, weil die Richtlinie 2006/24/EG wegen Inexistenz und Verstoßes gegen das deutsche Zustimmungsgesetz keine Umsetzungspflicht Deutschlands auslöst. Insoweit wird auf die Ausführungen unter Punkt B.II.1 oben Bezug genommen.[973]

Im Übrigen sind auch die Voraussetzungen, unter denen nach Gemeinschaftsrecht einstweiliger Rechtsschutz gewährt werden kann[974], erfüllt: Die Wirksamkeit der Richtlinie 2006/24/EG ist nicht nur sehr zweifelhaft sondern sogar offensichtlich nicht gegeben. Eine Nichtigkeitsklage ist bei dem Europäischen Gerichtshof bereits anhängig. Die einstweilige Aussetzung ist dringlich, weil den Antragstellern und den übrigen Grundrechtsträgern – wie bereits ausgeführt – schwere und irreparable Schäden drohen. Schließlich wird der Richtlinie 2006/24/EG auch nicht jede praktische Wirksamkeit genommen. Vielmehr erfolgt die Aussetzung nur einstweilig für die Dauer des vorliegenden Verfahrens.

Sollte das Gericht wegen fehlender Ausführungen oder wegen mangelnder Substantiierung des Vortrags der Beschwerdeführer eine rechtlich nachteilhafte Entscheidung beabsichtigen, so wird um vorherige Gewährung rechtlichen Gehörs gebeten, also um einen Hinweis und um Einräumung einer Gelegenheit zur Ergänzung der Ausführungen.

973 Seite 10.
974 Schoch/Schmidt-Aßmann/Pietzner, § 80 VwGO, Rn. 269 m.w.N.

Quellenverzeichnis

Achelpöhler, Wilhelm / Niehaus, Holger: Videoüberwachung öffentlicher Plätze, in: DuD 2002, S. 731-735.

AK, Alternativkommentar: Kommentar zum Grundgesetz für die Bundesrepublik Deutschland. Hrsg. von Erhard Denninger u.a. Neuwied u.a., 2001. Stand: 2. Aktualisierungslieferung, August 2002, zitiert: AK-GG-*Bearbeiter*.

Albers, Hans W.: Der Nicht-Störer im bereichsspezifischen Datenschutz, in: ZRP 1990, S. 147-149.

Albrecht, Hans-Jörg / Arnold, Harald / Demko, Daniela / Braun, Elisabeth u.a.: Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen, Freiburg 2003, zitiert: Albrecht/Arnold/Demko/ Braun, Rechtswirklichkeit und Effizienz der Telekommunikationsüberwachung. Im Internet abrufbar unter www.bmj.bund.de/media/archive/136.pdf.

Albrecht, Peter-Alexis: Die vergessene Freiheit, 1. Aufl., Berlin 2003, zitiert: Albrecht, Die vergessene Freiheit.

Allitsch, Rainer: Data Retention on the Internet, in: CRi (Computer und Recht international) 2002, S. 161-168.

APIG, All Party Parliamentary Internet Group (UK): Communications Data, Report of an Inquiry, Januar 2003, www.apig.org.uk/APIGreport.pdf, zitiert: APIG, Communications Data (I).

Artikel-29-Gruppe der EU, Arbeitsgruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten: Anonymität im Internet, Empfehlung 3/97 vom 03.12.1997, europa.eu.int/comm/internal_market/privacy/docs/wpdocs/1997/wp6_de.pdf, zitiert: Artikel-29-Gruppe der EU, Anonymität (I).

Artikel-29-Gruppe der EU, Arbeitsgruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten: Privatsphäre im Internet, 21.11.2000, europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2000/wp37de.pdf, zitiert: Artikel-29-Gruppe der EU, Privatsphäre im Internet (I).

Artikel-29-Gruppe der EU, Arbeitsgruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten: Stellungnahme 5/2002 zur Erklärung der europäischen Datenschutzbeauftragten auf der Internationalen Konferenz in Cardiff (9.-11. September 2002) zur obligatorischen systematischen Aufbewahrung von Verkehrsdaten im Bereich der Telekommunikation vom 11.10.2002, europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp64_de.pdf, zitiert: Artikel-29-Gruppe der EU, Stellungnahme 5/2002 (I).

Artikel-29-Gruppe der EU, Arbeitsgruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten: Empfehlung 2/99 zur Achtung der Privatsphäre bei der Überwachung des Fernmeldeverkehrs der Artikel 29-Gruppe vom 03.05.1999, europa.eu.int/comm/internal_market/privacy/docs/wpdocs/1999/wp18de.pdf, zitiert: Artikel-29-Gruppe der EU, Überwachung (I).

Artikel-29-Gruppe der EU, Arbeitsgruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten: Aufbewahrung von Verkehrsdaten durch Internet-Dienstanbieter für Strafverfolgungszwecke, Empfehlung 3/99 vom 07.09.1999, europa.eu.int/comm/internal_market/privacy/docs/wpdocs/1999/wp25de.pdf, zitiert: Artikel-29-Gruppe der EU, Vorratsspeicherung (I).

Asbrock, Bernd: Der Richtervorbehalt – prozedurale Grundrechtssicherung oder rechtsstaatliches Trostpflaster? In: ZRP 1998, S. 17-19.

Backes, Otto / Gusy, Christoph: Eine empirische Untersuchung von Richtervorbehalten bei Telefonüberwachungen, in: StV 2003, S. 249-252.

Bansberg, Jürgen: Staatsschutz im Internet, S. 48-54 in: Holznagel, Bernd / Nelles, Ursula / Sokol, Bettina (Hrsg.): Die neue TKÜV (Telekommunikations-Überwachungsverordnung), 1. Aufl., München 2002, zitiert: Bansberg, Staatsschutz im Internet.

Bär, Wolfgang: Aktuelle Rechtsfragen bei strafprozessualen Eingriffen in die Telekommunikation, in: MMR 2000, S. 472-480.

Baumeister, Peter: Das Rechtswidrigwerden von Normen, 1. Aufl., Berlin 1996, zitiert: Baumeister, Das Rechtswidrigwerden von Normen.

Bäumler, Helmut / von Mutius, Albert (Hrsg.): Anonymität im Internet, 1. Aufl., Braunschweig u.a. 2003, zitiert: Bäumler/v. Mutius-*Bearbeiter*, Anonymität im Internet.

Bäumler, Helmut: Eine sichere Informationsgesellschaft? In: DuD 2001, S. 348-352.

Bergmann, Lutz / Möhrle, Roland / Herb, Armin: Datenschutzrecht, Stuttgart u.a., Stand: September 2003, zitiert: Bergmann/Möhrle/Herb, Datenschutzrecht.

Berliner Kommentar: Berliner Kommentar zum Grundgesetz, herausgegeben von Karl Heinrich Friauf und Wolfram Höfling, 1. Aufl., Berlin 2000, Stand Juni 2002, zitiert: Berliner Kommentar-*Bearbeiter*.

Berner, Georg / Köhler, Gerd Michael: Polizeiaufgabengesetz. 16. Aufl., München 2000, zitiert: Berner/Köhler, PAG.

Bernsmann, Klaus: Anordnung der Überwachung des Fernmeldeverkehrs – Mitteilung der geographischen Daten des eingeschalteten Mobiltelefons, Anmerkung zu BGH (Ermittlungsrichter) NJW 2001, 1587, in: NStZ 2002, S. 103-104.

Bizer, Johann: Datenschutz verkauft sich – wirklich! In: DuD 2001, S. 250-250.

Bizer, Johann: Forschungsfreiheit und informationelle Selbstbestimmung, 1. Aufl., Baden-Baden 1992, zitiert: Bizer, Forschungsfreiheit.

Bizer, Johann: Grundzüge des TK-Datenschutzes, Stand der TK-Überwachung, 29.01.2003, youthful2.free.fr/Jbz-tkue%2829-01-2003%29.pdf, zitiert: Bizer, Grundzüge des TK-Datenschutzes (I).

Bizer, Johann: Schüler am Netz: Rechtsfragen beim Einsatz von Email, Newsgroups und WWW in Schulen, web.archive.org/web/20030215163608/http://www.jtg-online.de/jahrbuch/band6/Bizer2_Lf.html, zitiert: Bizer, Rechtsfragen beim Einsatz von Email, Newsgroups und WWW in Schulen (I).

Bizer, Johann: Telekommunikation und Innere Sicherheit 2000, in: Jahrbuch Telekommunikation und Gesellschaft 2001, herausgegeben von H. Kubicek u.a., Heidelberg 2001, S. 496-509, zitiert: Bizer, Jahrbuch Telekommunikation und Gesellschaft 2001.

Bizer, Johann: Telekommunikation und Innere Sicherheit 2001, in: Jahrbuch Telekommunikation und Gesellschaft 2002, herausgegeben von H. Kubicek u.a., Heidelberg 2002, S. 1-22, zitiert: Bizer, Jahrbuch Telekommunikation und Gesellschaft 2002. Im Internet abrufbar unter youthful2.free.fr/(Bizer)TKinSich01inJahrbTKuG2002.pdf.

BMI, Bundesministerium des Innern: Polizeiliche Kriminalstatistik 2001, www.bmi.bund.de/downloadde/19721/Download.pdf, zitiert: BMI, PKS 2001 (I).

BMI, Bundesministerium des Innern: Polizeiliche Kriminalstatistik 2002, www.bmi.bund.de/Anlage24353/Polizeiliche_Kriminalstatistik_2002.pdf, zitiert: BMI, PKS 2002 (I).

BMI/BMJ, Bundesministerium des Innern, Bundesministerium der Justiz: Erster Periodischer Sicherheitsbericht, 1. Aufl., Berlin 2001, zitiert: BMI/BMJ, Sicherheitsbericht 2001.

BMI/BMJ, Bundesministerium des Innern, Bundesministerium der Justiz: Erster Periodischer Sicherheitsbericht. Kurzfassung. Berlin, Juli 2001, www.bmi.bund.de/downloadde/11860/Download_Kurzfassung.pdf, zitiert: BMI/BMJ, Sicherheitsbericht 2001, Kurzfassung (I).

BMJ, Bundesministerium der Justiz: Stellungnahme zum Entwurf eines Gesetzes zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz) vom 17. Oktober 2001, www.ccc.de/CRD/20011017BMJ.PDF, zitiert: BMJ, Stellungnahme zum Terrorismusbekämpfungsgesetz (I).

BMWi-Ressortarbeitsgruppe: Eckpunkte zur Anpassung der Regelungen des § 90 TKG, 28.03.2002, www.almeprom.de/fiff/material/Eckpunkte_90_TKG_Prepaid.pdf, zitiert: BMWi-Ressortarbeitsgruppe, Eckpunkte zur Anpassung der Regelungen des § 90 TKG (I).

Bönitz, Dieter: Strafgesetze und Verhaltenssteuerung, 1. Aufl., Göttingen 1991, zitiert: Bönitz, Strafgesetze und Verhaltenssteuerung.

Bottger, Andreas / Pfeiffer, Christian: Der Lauschangriff in den USA und in Deutschland, in: ZRP 1994, S. 7-17.

Brenner, Harald: Die strafprozessuale Überwachung des Fernmeldeverkehrs mit Verteidigern, 1. Aufl., Tübingen 1994, zitiert: Brenner, Die strafprozessuale Überwachung des Fernmeldeverkehrs mit Verteidigern.

Breyer, Patrick: Der staatliche Zugriff auf Telekommunikations-Bestandsdaten aus verfassungsrechtlicher Sicht, in: RDV 2003, S. 218-222.

Breyer, Patrick: Die Cyber-Crime-Konvention des Europarats, in: DuD 2001, S. 592-600.

Breyer, Patrick: Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, Berlin 2005, zitiert: Breyer, Vorratsspeicherung.

Büchner, Wolfgang / Ehmer, Jörg / Geppert, Martin / Kerkhoff, Bärbel / Piepenbrock, Hermann-Josef / Schütz, Raimund / Schuster, Fabian: Beck'scher TKG-Kommentar, 2. Aufl., München 2000, zitiert: BeckTKG-*Bearbeiter*.

Bundesregierung: Begründung v4.0 zur TKÜV, 17.10.2001, www.dud.de/dud/documents/e-tkuev-4-0-b.pdf, zitiert: Bundesregierung, Begründung v4.0 zur TKÜV (I).

Bundestag: Öffentliche Anhörung zum Thema Cyber-Crime/TKÜV des Ausschusses für Kultur und Medien, Unterausschuss „Neue Medien", Protokoll 14/13, 05.07.2001, www.bundestag.de/gremien/a23_ua/Protokoll_13.pdf, zitiert: Bundestag, Öffentliche Anhörung zum Thema Cyber-Crime/TKÜV (I).

Buxel, Holger: Die sieben Kernprobleme des Online-Profilings aus Nutzerperspektive, in: DuD 2001, S. 579-583.

Callies, Christian: Sicherheit im freiheitlichen Rechtsstaat, in: ZRP 2002, S. 1-7.

Calliess, Christian / Matthias Ruffert (Hrsg.): Kommentar des Vertrages über die Europäische Union und des Vertrages zur Gründung der Europäischen Gemeinschaft: EUV/EGV, 2. Aufl., Neuwied u.a. 2002, zitiert: Calliess/Ruffert-*Bearbeiter*.

Chryssogonos, Kostas: Verfassungsgerichtsbarkeit und Gesetzgebung, 1. Aufl., Berlin 1987, zitiert: Chryssogonos, Verfassungsgerichtsbarkeit und Gesetzgebung.

Covington & Burling: Memorandum of laws concerning the legality of data retention with regard to the rights guaranteed by the European Convention on Human Rights, 10.10.2003, www.statewatch.org/news/2003/oct/Data_Retention_Memo.pdf, zitiert: Covington & Burling, Memorandum (I).

CSI / FBI: 2002 CSI/FBI Computer Crime and Security Survey, lcb1.uoregon.edu/ldeck/actg320/FBI2002.pdf, zitiert: CSI/FBI, 2002 Survey (I).

Data Protection Commissioner (UK): Response of the Data Protection Commissioner to the Government's Regulation of investigatory powers Bill, March 2000, www.dataprotection.gov.uk/dpr/dpdoc.nsf/ed1e7ff5aa6def3 0802566360045bf4d/3fddbd098455c3fe802568d90049ac04?OpenDocument, zitiert: Data Protection Commissioner (UK), RIP (I).

Datenschutzbeauftragte von Berlin, Brandenburg, Bremen, Nordrhein-Westfalens und Schleswig-Holstein: 10 Punkte für einen Politikwechsel zum wirksamen Schutz der Privatsphäre, in: DSB 12/1998, S. 4-4.

Deckers, Rüdiger: Geheime Aufklärung durch Einsatz technischer Mittel, Vortrag auf dem Strafverteidigerkolloquium der Arge Strafrecht des DAV am 9./10. 11. 2001, www.ag-strafrecht.de/strafo/aufsatzdeckers.htm, zitiert: Deckers, Geheime Aufklärung (I).

DG Research, Directorate General for Research of the European Commission: Development of Surveillance Technology and Risk of Abuse of Economic Information (An appraisal of technologies of political control), Part 1/4, The perception of economic risks arising from the potenzial vulnerability of electronic commercial media to interception, Survey of opinions of experts, Interim Study, cryptome.org/dst-1.htm, zitiert: DG Research, Economic risks arising from the potenzial vulnerability of electronic commercial media to interception (I).

Diekmann, Andreas: Die Befolgung von Gesetzen, 1. Aufl., Berlin 1980, zitiert: Diekmann, Die Befolgung von Gesetzen.

Dietel, Alfred: „Innere Sicherheit" – Verheißung und reale Möglichkeiten, in: Bull, Hans Peter (Hrsg.): Sicherheit durch Gesetz? 1. Aufl., Baden-Baden 1987, zitiert: Dietel, Innere Sicherheit.

Dijk, P. van / Hoof, G.J.H. van: Theory and Practise of the European Convention on Human Rights, 2. Aufl., Dezember 1990, zitiert: Van Dijk/van Hoof, Theory and Practise of the European Convention on Human Rights.

Dreier, Horst (Hrsg.): Grundgesetz. Kommentar. Band I: Artikel 1-19, 1. Aufl., Tübingen 1996, zitiert: Dreier-*Bearbeiter*.

DSB-Konferenz, Datenschutzbeauftragte des Bundes und der Länder: Entschließung zum Entwurf eines Gesetzes über das Bundeskriminalamt (BKA-Gesetz), Entschließung der 49. Konferenz am 09./10.03.1995 in Bremen, www.datenschutz-berlin.de/jahresbe/95/anlage/an2_1.htm, zitiert: DSB-Konferenz, BKAG (I).

DSB-Konferenz, Datenschutzbeauftragte des Bundes und der Länder: Für eine freie Telekommunikation in einer freien Gesellschaft, Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15.03.2000, www.bfd.bund.de/information/info5/anl/an06.html, zitiert: DSB-Konferenz, Freie Telekommunikation (I).

DSB-Konferenz, Datenschutzbeauftragte des Bundes und der Länder: Konsequenzen aus dem Urteil des Bundesverfassungsgerichtes zu den Abhörmaßnahmen des BND, Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15.03.2000, www.datenschutz-berlin.de/doc/de/konf/59/bndneu.htm, zitiert: DSB-Konferenz, Konsequenzen aus BVerfGE 100, 313 (I).

DSB-Konferenz, Datenschutzbeauftragte des Bundes und der Länder: Anforderungen an Datenschutzregelungen für den Verfassungsschutz, Beschluss der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 13.09.1985, www.datenschutz-berlin.de/doc/de/konf/sonst/85_dsfvs.htm, zitiert: DSB-Konferenz, Verfassungsschutz (I).

DSB-Konferenz, Datenschutzbeauftragte des Bundes und der Länder: Entschließung zur geplanten erweiterten Speicherung von Verbindungsdaten in der Telekommunikation, Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26.03.1999, www.datenschutz-berlin.de/doc/de/konf/57/telekomm.htm, zitiert: DSB-Konferenz, Vorratsspeicherung (I).

DSB-Konferenz, Datenschutzbeauftragte des Bundes und der Länder: Bestandsaufnahme über die Situation des Datenschutzes „Zehn Jahre nach dem Volkszählungsurteil", Beschluss der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 09./10.03.1984, www.datenschutz-berlin.de/jahresbe/94/anlage/an2_1.htm, zitiert: DSB-Konferenz, Zehn Jahre nach dem Volkszählungsurteil (I).

Eckhardt, Jens: Die neue TKÜV - Innere Sicherheit auf Kosten von Netzbürgern und Providern? In: DSB 06/2001, S. 13.

Eckhardt, Jens: Neue Entwicklungen der Telekommunikationsüberwachung, in: CR 2002, S. 770-775.

Eckhardt, Jens: Neue Regelungen der TK-Überwachung, in: DuD 2002, S. 197-201.

Eckhardt, Jens: TKÜV – Ein Überblick, in: CR 2001, S. 670-678.

Eisenberg, Ulrich: Kriminologie, 5. Aufl., München 2000, zitiert: Eisenberg, Kriminologie.

Elicker, Michael: Der Grundsatz der Lastengleichheit als Schranke der Sonderabgaben, Inpflichtnahmen und Dienstleistungspflichten, in: NVwZ 2003, S. 304-307.

Emmert, Frank: Europarecht, 1. Aufl., München 1996, zitiert: Emmert, Europarecht.

Enderle, Bettina: Anmerkung zu OVG Münster, MMR 2002, S. 563-564, in: MMR 2002, S. 565-565.

EP, Europäisches Parlament: Bericht des nichtständigen Ausschusses des Europäischen Parlaments über das Abhörsystem Echelon 2001/2098 (INI) vom 11.07.2001, www.europarl.eu.int/tempcom/echelon/pdf/rapport_echelon_de.pdf, zitiert: EP, Echelon-Bericht (I).

EP, Europäisches Parlament: Entschließung P5-0104/2004 des Europäischen Parlaments vom 09.03.2004 zum Ersten Bericht der Kommission über die Durchführung der Datenschutzrichtlinie (95/46/EG), www2.europarl.eu.int/omk/sipade2?PUBREF=-//EP//TEXT+TA+P5TA-2004-0141+0+DOC+XML+V0//DE&L=DE&LEVEL=3&NAV=S&LSTDOC=Y,zitiert: EP, Entschließung zur Durchführung der Datenschutzrichtlinie (I).

EPIC, Electronic Privacy Information Center, PI, Privacy International: Privacy and Human Rights 2002. Teil I: www.privacyinternational.org/survey/phr2002/phr2002-part1.pdf; Teil II: www.privacyinternational. org/survey/phr2002/phr2002-part2.pdf; Teil III: www.privacyinternational.org/survey/phr2002/phr2002-part3.pdf, zitiert: EPIC/PI, Privacy and Human Rights 2002 (I).

EU-Netzwerk unabhängiger Grundrechtsexperten (CFR-CDF): The balance between freedom and security in the response by the European Union and its Member States to the terrorist threats, 31.03.2003, www.statewatch.org/news/2003/apr/CFR-CDF.ThemComment1.pdf, zitiert: EU-Netzwerk unabhängiger Grundrechtsexperten, The balance between freedom and security (I).

EU-Rat, Rat der Europäischen Union: Answers to questionnaire on traffic data retention, Dokument Nr. 14107/02 LIMITE CRIMORG 100 TELECOM 42 vom 20.11.2002, www.statewatch.org/news/2002/nov/euintercept-2002-11-20.html, zitiert: EU-Rat, Answers to questionnaire on traffic data retention (I).

Europarat, Ministerkommittee: Richtlinien des Ministerkommittees des Europarates über Menschenrechte und die Bekämpfung von Terrorismus, www.coe.int/T/E/Com/Files/Themes/terrorism/CM_Guidelines_20020628.asp, zitiert: Europarats-Richtlinien über Menschenrechte und die Bekämpfung von Terrorismus (I).

Eurostat: Eurostat Jahrbuch 2002, Menschen in Europa, web.archive.org/web/20021113192623/http://europa.eu.int/comm/eurostat/Public/datashop/printproduct/DE?catalogue=Eurostat&product=Freeselect1-DE&mode=download, zitiert: Eurostat Jahrbuch 2002, Menschen in Europa (I).

Eurostat: Statistik über die Informationsgesellschaft - Internet- und Mobiltelefonnutzung in der EU, 14.03.2002, web.archive.org/web/20030121214703/http://europa.eu.int/comm/eurostat/Public/datashop/printproduct/DE?catalogue=Eurostat&product=KS-NP-02-008-__-N-DE&mode=download, zitiert: Eurostat, Internetnutzung (I).

Federrath, Hannes: Schwachstelle Schnittstelle: Angriffspunkt für Datenspione, S. 115-123 in: Holznagel, Bernd / Nelles, Ursula / Sokol, Bettina (Hrsg.): Die neue TKÜV (Telekommunikations-Überwachungsverordnung), 1. Aufl., München 2002, zitiert: Federrath, Schwachstelle Schnittstelle.

Feltes, Thomas: Fehlerquellen im Ermittlungsverfahren – Anmerkungen zur Rolle und Funktion der Polizei, Referat im Rahmen der Arbeitsgruppe „Fehlerquellen im Ermittlungsverfahren“ auf dem 25. Strafverteidigertag vom 09.-11.03.2001 in Berlin, www.thomasfeltes.de/htm/Strafverteidigertag.htm, zitiert: Feltes, Fehlerquellen im Ermittlungsverfahren (I).

Feltes, Thomas: Verhaltenssteuerung durch Prävention, in: MschrKrim 1993, S. 341-354.

Feser, Frank: Anmerkung zu LG Wuppertal, MMR 2002, S. 560, in: MMR 2002, S. 560, 560.

Fischer, Thomas / Maul, Heinrich: Tatprovozierendes Verhalten als polizeiliche Ermittlungsmaßnahme, in: NStZ 1992, S. 7-13.

Fox, Dirk / Bizer, Johann: Namenlos im Netz, in: DuD 1998, S. 616.

Fox, Dirk: Big Brother is listening in, in: DuD 2002, S. 194.

French Delegation of Police Cooperation Working Party: Computer crime – Summary of replies to the questionnaire (Enfopol 38), 24.04.2001, www.statewatch.org/news/2001/may/ENFO38.PDF, zitiert: French Delegation of Police Cooperation Working Party, Enfopol 38 (I).

Friauf, Karl Heinrich: Öffentliche Sonderlasten und Gleichheit der Steuerbürger, S. 45-66 in: Festschrift für Hermann Jahrreiß zum 80. Geburtstag, Institut für Völkerrecht und ausländisches öffentliches Recht der Universität zu Köln (Hrsg.), 1. Aufl., Köln u.a. 1974, zitiert: Friauf, FS Jahrreiß.

Friedrich, Dirk: Die Verpflichtung privater Telekommunikationsunternehmen, die staatliche Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen, 1. Aufl., Aachen 2001, zitiert: Friedrich, Verpflichtung.

Frowein, Jochen / Peukert, Wolfgang: EMRK-Kommentar, 2. Aufl., Kehl 1996, zitiert: Frowein/Peukert-*Bearbeiter*.

G7 Justice and Interior Ministers: Communiqué Annex: Principles and Action Plan To Combat High-Tech Crime, G7 Justice and Interior Ministers' Meeting (Washington DC), 10.12.1997, www.usdoj.gov/criminal/cybercrime/principles.htm, zitiert: G7, High-Tech Crime Principles (I).

G7 Justice and Interior Ministers: Communiqué, G7 Justice and Interior Ministers' Meeting (Washington DC), 10.12.1997, www.usdoj.gov/criminal/cybercrime/communique.htm, zitiert: G7, High-Tech Crime Communiqué (I).

G8 Government-Industry Workshop on Safety and Confidence in Cyberspace: Report of Workshop 1a, Theme 1: Locating and identifying High-Tech Criminals, Workshop A: Data retention and User Authentication, cryptome.org/g8-isp-e-spy.htm, zitiert: G8 Workshop, Workshop A (I).

G8 Government-Industry Workshop on Safety and Security in Cyberspace: Discussion Paper for Workshop 1: Potential Consequences of Data Retention for Various Business Models Characterizing Internet Services, Tokyo, Mai 2001, cryptome.org/g8-isp-e-spy.htm, zitiert: G8 Workshop, Potential Consequences of Data Retention (I).

G8 Government-Industry Workshop on Safety and Security in Cyberspace: Report of Workshop 1: Data Retention, Tokyo, Mai 2001, www.mofa.go.jp/policy/i_crime/high_tec/conf0105-4.html, zitiert: G8 Workshop, Workshop 1 (I).

G8 Government-Industry Workshop on Safety and Security in Cyberspace: Report of Workshop 3: Threat Assessment and Prevention, Tokyo, Mai 2001, www.mofa.go.jp/policy/i_crime/high_tec/conf0105-6.html, zitiert: G8 Workshop, Workshop 3 (I).

G8 Government-Industry Workshop on Safety and Security in Cyberspace: Report of Workshop 4: Protection of E-Commerce and User Authentication, Tokyo, Mai 2001, www.mofa.go.jp/policy/i_crime/high_tec/conf0105-7.html, zitiert: G8 Workshop, Workshop 4 (I).

G8 Justice and Interior Ministers: Principles on the Availability of Data Essential to Protecting Public Safety, G8 Justice and Interior Ministers' Meeting (Canada 2002), canada.justice.gc.ca/en/news/g8/doc3.html, zitiert: G8, Availability (I).

Garstka, Hansjürgen/Dix, Alexander/Walz, Stefan/Sokol, Bettina/Bäumler, Helmut: Für eine Sicherung der freien Telekommunikation in unserer Gesellschaft, Hintergrundpapier vom 25.08.1999, www.datenschutz-berlin.de/doc/de/sonst/tk.htm, zitiert: Garstka/Dix/ Walz/Sokol/Bäumler, Hintergrundpapier (I).

Garstka, Hansjürgen: Stellungnahme zum Terrorismusbekämpfungsgesetz anlässlich der öffentlichen Anhörung zum Terrorismusbekämpfungsgesetz im Innenausschuss des Bundestages am 30.11.2001, www.datenschutz-berlin.de/doc/de/sonst/sgarantt.htm, zitiert: Garstka, zum Terrorismusbekämpfungsgesetz (I).

Geiger, Rudolf: Grundgesetz und Völkerrecht, 3. Aufl., München 2002, zitiert: Geiger, Grundgesetz und Völkerrecht.

Gerling, Rainer W./Tinnefeld, Marie-Theres: Anonymität im Netz, in: DuD 2003, S. 305.

Germann, Michael: Gefahrenabwehr und Strafverfolgung im Internet, 1. Aufl., Berlin 2000, zitiert: Germann.

Glöckner, Arne: „Terrorismus" – Rechtsfragen der äußeren und inneren Sicherheit, in: NJW 2002, S. 2692-2694.

Gola, Peter / Schomerus, Rudolf: Bundesdatenschutzgesetz, 7. Aufl., München 2002, zitiert: Gola/Schomerus, BDSG.

Göppinger, Hans: Kriminologie, 5. Aufl., München 1997, zitiert: Göppinger, Kriminologie.

Grabenwarter, Christoph: Europäische Menschenrechtskonvention, 1. Aufl., München 2003, zitiert: Grabenwarter.

Grabitz, Eberhard / Hilf, Meinhard: Das Recht der Europäischen Union, Stand: 18. ErgL Mai 2001, zitiert: Grabitz/Hilf-*Bearbeiter*.

Gridl, Rudolf: Datenschutz in globalen Telekommunikationssystemen, 1. Aufl., Baden-Baden 1999, zitiert: Gridl, Datenschutz in globalen Telekommunikationssystemen.

Gusy, Christoph: Das Grundgesetz als normative Gesetzgebungslehre, in: ZRP 1985, S. 291-299.

Gusy, Christoph: Das Grundrecht des Post- und Fernmeldegeheimnisses, in: JuS 1986, S. 89-96.

Gusy, Christoph: Informationelle Selbstbestimmung und Datenschutz: Fortführung oder Neuanfang? In: KritV 2000, S. 52-64.

Hamm, Rainer: „Überwachungssicherheit" – wer soll sicher vor wem oder was sein? In: NJW 2001, S. 3100-3101.

Hamm, Rainer: TKÜV – Ein Kompromiss auf dem Boden der Verfassung? S. 81-89 in: Holznagel, Bernd / Nelles, Ursula / Sokol, Bettina (Hrsg.): Die neue TKÜV (Telekommunikations-Überwachungsverordnung), 1. Aufl., München 2002, zitiert: Hamm, TKÜV.

Hänel, Nicole: Oberster Datenschützer kritisiert TKG-Novelle, 19.12.2003, www.politik-digital.de/edemocracy/netzrecht/tkg-novelle.shtml, zitiert: Hänel, Oberster Datenschützer kritisiert TKG-Novelle (I).

Hassemer, Winfried: Freiheitliches Strafrecht, 1. Aufl., Berlin 2001, zitiert: Hassemer, Freiheitliches Strafrecht.

Hassemer, Winfried: Staat, Sicherheit und Information, in: Johann Bizer/Bernd Lutterbeck/Joachim Rieß (Hrsg.): Umbruch von Regelungssystemen in der Informationsgesellschaft, Stuttgart 2002, S. 225-245, zitiert: Hassemer, Staat, Sicherheit und Information. Im Internet abrufbar unter www.alfred-buellesbach.de/PDF/21_Hassemer_Staat.pdf.

Hassemer, Winfried: Strafen im Rechtsstaat, 1. Aufl., Baden-Baden 2000, zitiert: Hassemer, Strafen im Rechtsstaat.

Hoeren, Thomas (Hrsg.): Handbuch Multimedia-Recht, 1. Aufl., München 1999, Stand der Bearbeitung: Dezember 1998, zitiert: HMR-*Bearbeiter*.

Hohmann, Harald (Hrsg.): Freiheitssicherung durch Datenschutz, 1. Aufl., Frankfurt a.M. 1987, zitiert: Hohmann-*Bearbeiter*, Freiheitssicherung durch Datenschutz.

Home Office (UK): Consultation paper under Part 11 of the Anti-terrorism, Crime and Security Act 2001 about the voluntary retention of communications data, www.homeoffice.gov.uk/docs/vol_retention.pdf, zitiert: Home Office (UK), Consultation paper (I).

Home Office (UK): Retention of Communications Data, www.statewatch.org/news/2001/nov/retention_of_communications_data.pdf, zitiert: Home Office (UK), Retention (I).

Hong Kong Inter-departmental Working Group on Computer Related Crime: Report, www.hkispa.org.hk/pdf/ComputerRelatedCrime.pdf, zitiert: Hong Kong Inter-departmental Working Group on Computer Related Crime, Report (I).

Hornung, Gerrit: Zwei runde Geburtstage: Das Recht auf informationelle Selbstbestimmung und das WWW, in: MMR 2004, S. 3-8.

Höver, Albert: Gesetz über die Entschädigung von Zeugen und Sachverständigen. Kommentar. 21. Aufl., Köln u.a. 2000, zitiert: Höver.

Information Commissioner (UK): Comments on the provisions of the Anti-Terrorism, Crime and Security Bill relating to the retention of communications data, 05.12.2001, www.publications.parliament.uk/pa/jt200102/jtselect/jtrights/51/51ap02.htm, zitiert: Information Commissioner (UK), Comments on the provisions of the Anti-Terrorism, Crime and Security Bill relating to the retention of communications data (I).

Innenministerkonferenz, Ständigen Konferenz der Innenminister und -senatoren der Länder: Beschlüsse der 165. Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder am 24.11.2000 in Bonn, www.bremen.de/innensenator/Kap4/PDF/0011.pdf, zitiert: Innenministerkonferenz vom 24.11.2000 (I).

Internationale Konferenz der Datenschutzbeauftragten: Gemeinsame Erklärung auf der 14. Konferenz, 29.10.1992, Sydney, Fernmeldegeheimnis, www.datenschutz-berlin.de/infomat/heft14/b3.htm, zitiert: Internationale Konferenz der Datenschutzbeauftragten, Fernmeldegeheimnis (I).

Internationale Konferenz der Datenschutzbeauftragten: Gemeinsame Erklärung auf der 5. Konferenz, 18.10.1983, Stockholm, Neue Medien, www.datenschutz-berlin.de/infomat/heft14/b1.htm, zitiert: Internationale Konferenz der Datenschutzbeauftragten, Neue Medien (I).

IWGDPT, Internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation: Gemeinsamer Standpunkt zu Datenschutzaspekten des Entwurfs einer Konvention zur Datennetzkriminalität des Europarates vom 13./14.09.2000, angenommen auf der 28. Sitzung der Arbeitsgruppe am 13./14.09.2000 in Berlin, www.datenschutz-berlin.de/doc/int/iwgdpt/cy_en.htm, zitiert: IWGDPT, Cybercrime-Konvention (I).

IWGDPT, Internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation: Gemeinsamer Standpunkt über die öffentliche Verantwortung im Hinblick auf das Abhören privater Kommunikation, angenommen auf der 23. Sitzung in Hong Kong SAR (China) am 15.04.1998, www.datenschutz-berlin.de/doc/int/iwgdpt/inter_de.htm (Übersetzung), zitiert: IWGDPT, Öffentliche Verantwortung bei Abhörmaßnahmen (I).

IWGDPT, Internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation: Gemeinsamer Standpunkt zu Datenschutz und Aufenthaltsinformationen in mobilen Kommunikationsdiensten, angenommen auf der 29. Sitzung der Arbeitsgruppe am 15./16.02.2001 in Bangalore, www.datenschutz-berlin.de/doc/int/iwgdpt/locat_de.htm, zitiert: IWGDPT, Standortdaten.htm (Übersetzung) (I).

IWGDPT, Internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation: Arbeitspapier zur Überwachung der Telekommunikation, angenommen auf der 31. Sitzung der Arbeitsgruppe am 26./27.03.2002 in Auckland (Neuseeland), www.datenschutz-berlin.de/doc/int/iwgdpt/wptel_de.htm (Übersetzung), zitiert: IWGDPT, Terrorismus (I).

Jarass, Hans / Pieroth, Bodo: Grundgesetz für die Bundesrepublik Deutschland. Kommentar, 4. Aufl., München 1997. 5. Aufl., München 2000. 6. Aufl., München 2002, zitiert: J/P^{Auflage}-*Bearbeiter*.

Jeserich, Hans-Dieter: TK-Überwachung in Zahlen und Fakten, S. 63-78 in: Holznagel, Bernd / Nelles, Ursula / Sokol, Bettina (Hrsg.): Die neue TKÜV (Telekommunikations-Überwachungsverordnung), 1. Aufl., München 2002, zitiert: Jeserich, TK-Überwachung.

Kaiser, Günther: Kriminologie, 7. Aufl., Heidelberg 1985, zitiert: Kaiser, Kriminologie.

Karpen, Ulrich: Gesetzesfolgenabschätzung, in: ZRP 2002, S. 443-446.

Kloepfer, Michael: Informationsrecht, 1. Aufl., München 2002, zitiert: Kloepfer, Informationsrecht.

Kloepfer, Michael: Privatsphäre im Fadenkreuz staatlicher Überwachung? S. 91-114 in: Holznagel, Bernd / Nelles, Ursula / Sokol, Bettina (Hrsg.): Die neue TKÜV (Telekommunikations-Überwachungsverordnung), 1. Aufl., München 2002, zitiert: Kloepfer, Privatsphäre.

Klug, Christoph: Zweites BfD-Symposium „Datenschutz in der Telekommunikation" – Bericht, in: RDV 2001, S. 311-312.

Köck, Wolfgang: Gesetzesfolgenabschätzung und Gesetzgebungsrechtslehre, in: VerwArch 93 (2002), S. 1-21.

Koenig, Christian / Koch, Alexander / Braun, Jens-Daniel: Die TKÜV: Neue Belastungen für Internet Service Provider und Mobilfunknetzbetreiber? In: K&R 2002, S. 289-297.

Kommission der Europäischen Gemeinschaften: Discussion Paper for Expert's Meeting on Retention of Traffic Data, 06.11.2001, europa.eu.int/information_society/topics/telecoms/internet/crime/wpapnov/index_en.htm, zitiert: Kommission, Discussion Paper for Expert's Meeting on Retention of Traffic Data (I).

Kommission der Europäischen Gemeinschaften: Mitteilung „Illegale und schädigende Inhalte im Internet", KOM(1996) 487 endg., europa.eu.int/ISPO/legal/de/internet/communic.html, zitiert: Kommission, Illegale Inhalte (I).

Kommission der Europäischen Gemeinschaften: Mitteilung „Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität", KOM(2000) 890 endg., europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeComDE.pdf, zitiert: Kommission, Sichere Informationsgesellschaft (I).

Kommission der Europäischen Gemeinschaften: Mitteilung der Kommission an das Europäische Parlament betreffend den Gemeinsamen Standpunkt des Rates im Hinblick auf den Erlass der Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, SEK(2002) 124 endg., 05.02.2002, youthful2.free.fr/05971d2.pdf, zitiert: Kommission, SEK(2002) 124 endg. (I).

Kommission der Europäischen Gemeinschaften: Public Hearing on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, 07.03.2001, europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/Hearingreport.html, zitiert: Kommission, Cybercrime-Anhörung (I).

Kommission der Europäischen Gemeinschaften: Your Views on Data Protection, Questionnaire on the implementation of the Data Protection Directive (95/46/EC), results of on-line consultation 20.06.2002-15.09.2002, europa.eu.int/comm/internal_market/en/dataprot/lawreport/docs/consultation-citizens_en.pdf, zitiert: Kommission, Your Views on Data Protection (I).

Kopp, Ferdinand / Ramsauer, Ulrich: Verwaltungsverfahrensgesetz. 7. Aufl., München 2000, zitiert: Kopp/Ramsauer.

Krader, Gabriela: Kampf gegen die Internetkriminalität, in: DuD 2001, S. 344-347.

Kube, Hanno/Schütze, Marc: Die Kosten der TK-Überwachung, in: CR 2003, S. 663-671.

Kudlich, Hans: Strafprozessuale Probleme des Internet, in: JA 2000, S. 227-234.

Kugelmann, Dieter: Cyber-Crime Konvention, in: DuD 2001, S. 215-223.

Kugelmann, Dieter: Der Schutz privater Individualkommunikation nach der EMRK, in: EuGRZ 2003, S. 16-25.

Kunz, Karl-Ludwig: Kriminologie. 2. Aufl., Bern u.a. 1998, zitiert: Kunz, Kriminologie.

Kury, Helmut: Das Dunkelfeld der Kriminalität, in: Kriminalistik 2001, S. 74-84.

Kutscha, Martin: Datenschutz durch Zweckbindung – ein Auslaufmodell? In: ZRP 1999, S. 156-160.

Kutscha, Martin: Große Koalition der Inneren Sicherheit? Die gegenwärtige Polizeigesetzgebung der Länder, In: Bürgerrechte & Polizei/CILIP 59 (1/98), S. 57-69. Im Internet abrufbar unter www.cilip.de/ausgabe/59/p-gesetz.htm.

Limbach, Jutta: 25 Jahre Datenschutzgesetz, in: RDV 2002, S. 163-166.

LINX (London Internet Exchange) Content Regulation Committee: LINX Best Current Practice – Traceability, 18.05.1999, www.linx.net/noncore/bcp/traceability-bcp.html, zitiert: LINX, Traceability (I).

LINX (London Internet Exchange): LINX Best Current Practice – User Privacy, 15.05.2001, www.linx.net/noncore/bcp/privacy-bcp.html, zitiert: LINX, User Privacy (I).

Lisken, Hans / Denninger, Erhard (Hrsg.): Handbuch des Polizeirechts. 2. Aufl., München 1996. 3. Aufl., München 2001, zitiert: L/D^{Auflage}-*Bearbeiter*.

Lisken, Hans: Über Aufgaben und Befugnisse der Polizei im Staat des Grundgesetzes, in: ZRP 1990, S. 15-21.

Lisken, Hans: Zur polizeilichen Rasterfahndung, in: NVwZ 2002, S. 513-519.

Lorenz, Frank Lucien: Aktionismus, Populismus? – Symbolismus! In: GA 1997, S. 51-71.

Lücking, Erika: Die strafprozessuale Überwachung des Fernmeldeverkehrs, 1. Aufl., Freiburg 1992, zitiert: Lücking, Die strafprozessuale Überwachung des Fernmeldeverkehrs.

Mangoldt, Hermann v. / Klein, Friedrich / Starck, Christian: Das Bonner Grundgesetz. Kommentar. Band I. 4. Aufl., München 1999, zitiert: vMKS-*Bearbeiter*.

Maunz, Theodor / Dürig, Günter u.a.: Grundgesetz. Kommentar. München, Stand: Juni 2002, zitiert: M/D-*Bearbeiter*.

MDG, Multidisziplinäre Gruppe „Organisierte Kriminalität" (MDG) des EU-Rats: Answers to the questionnaire on retention of traffic data, 16.09.2002, www.bof.nl/docs/data_retention_answers.pdf, zitiert: MDG, EU-Questionnaire (I).

MDG, Multidisziplinäre Gruppe „Organisierte Kriminalität" (MDG) des EU-Rats: Entwurf für Schlussfolgerungen des Rates zur Informationstechnologie und zur Ermittlungsarbeit und Verfolgung im Bereich der organisierten Kriminalität, 17.12.2002, register.consilium.eu.int/pdf/de/02/st15/15763d2.pdf, zitiert: MDG, Entwurf für Schlussfolgerungen des Rates zur Informationstechnologie (I).

MDG, Multidisziplinäre Gruppe „Organisierte Kriminalität" (MDG) des EU-Rats: Entwurf für Schlussfolgerungen des Rates zur Informationstechnologie und zur Ermittlungsarbeit und Verfolgung im Bereich der organisierten Kriminalität, 28.11.2002, register.consilium.eu.int/pdf/de/02/st12/12721-r3d2.pdf, zitiert: MDG, Entwurf für Schlussfolgerungen des Rates zur Informationstechnologie vom 28.11.2002 (I).

Meade, Joe (Datenschutzbeauftragter Irlands): Retention of Communications Traffic Data, 24.02.2003, www.dataprivacy.ie/7nr240203.htm, zitiert: Meade, Retention of Communications Traffic Data (I).

Meyer-Goßner, Lutz: Strafprozessordnung, Gerichtsverfassungsgesetz, 44. Aufl., München 1999, zitiert: Meyer-Goßner, StPO.

Meyer-Ladewig, Jens: EMRK, 1. Aufl., Baden-Baden 2003, zitiert: Meyer-Ladewig.

MPI, Max-Planck-Institut für ausländisches und internationales Strafrecht: Die Neuregelung zur Auslandskopfüberwachung gemäß § 4 TKÜV auf dem verfassungsrechtlichen Prüfstand, Gutachten im Auftrag des VATM vom Juli 2006, http://www.vatm.de/content/sonstige_materialien/-inhalt/08-09-2006.pdf, zitiert: MPI, VATM-Gutachten (I).

Münch, Ingo v. / Kunig, Philip (Hrsg.): Grundgesetz-Kommentar. Band I: Präambel bis Art. 19, 5. Aufl., München 2000. Band II: Art. 20 bis Art. 69, 5. Aufl., München 2001, zitiert: v. Münch/Kunig-*Bearbeiter*.

NCIS, National Criminal Intelligence Service (UK): APIG-Submission, www.apig.org.uk/lea.pdf, zitiert: NCIS, APIG-Submission (I).

NCIS, National Criminal Intelligence Service (UK): Looking to the Future, Clarity on Communications Data Retention Law, 21.08.2000, www.cryptome.org/ncis-carnivore.htm, zitiert: NCIS Submission (I).

Neumann, Andreas / Wolff, Reinmar: Informationsermittlung für Anordnungen nach §§ 100a und 100g StPO im Wege telekommunikationsrechtlicher Auskunftsverfahren, in: TKMR 2003, S. 110-118.

NFO Infratest: Monitoring Informationswirtschaft, 4. Faktenbericht - April 2002, www.tns-infratest-bi.com/bmwa/infrasearchreg/reg2002.asp?dfile=2002_09de_Internet-Nutzung.pdf, zitiert: NFO Infratest, Monitoring Informationswirtschaft (I).

Niggli, M. A.: Kriminologische Überlegungen zur Strafzumessung, 1997, www.unifr.ch/lman/downloads/publikationen/strafzumessung.pdf, zitiert: Niggli, Kriminologische Überlegungen zur Strafzumessung (I).

Omega Foundation: An Appraisal of the Technologies of Political Control, Summary and Options Report for the European Parliament, September 1998, cryptome.org/stoa-atpc-so.htm, zitiert: Omega Foundation, Report (I).

Omega Foundation: An Appraisal of the Technologies of Political Control, Working document, 06.01.1998, cryptome.org/stoa-atpc.htm, zitiert: Omega Foundation, Working document (I).

Opaschowski, Horst: Quo vadis, Datenschutz? In: DuD 2001, S. 678-681.

Ossenbühl, Fritz: Die Erfüllung von Verwaltungsaufgaben durch Private, in: VVDStRL 29, S. 137-210.

Ossenbühl, Fritz: Die Kontrolle von Tatsachenfeststellungen und Prognoseentscheidungen durch das Bundesverfassungsgericht, in: Christian Starck (Hsrg.): Bundesverfassungsgericht und Grundgesetz, 1. Aufl., Tübingen 1976, zitiert: Ossenbühl, Tatsachenfeststellungen und Prognoseentscheidungen.

Ostendorf, Heribert: Jugendstrafrecht in der Diskussion, in: ZRP 2000, S. 103-107.

Ostendorf, Heribert: Organisierte Kriminalität – eine Herausforderung für die Justiz, in: JZ 1991, S. 62-70.

Pernice, Ina: Die Telekommunikations-Überwachungsverordnung (TKÜV), in: DuD 2002, S. 207-211.

Pieroth, Bodo / Schlink, Bernhard: Grundrechte, 17. Aufl., Heidelberg 2001, zitiert: P/S.

PricewaterhouseCoopers: Wirtschaftskriminalität 2003, August 2003, www.pwc.com/de/ger/inssol/publ/Wirtschaftskriminalitaet_2003.pdf, zitiert: PricewaterhouseCoopers, Wirtschaftskriminalität 2003 (I).

Queen Mary (University of London): Study on legal issues relevant to combating criminal activities perpetrated through electronic communications, Oktober 2000, presented the the European Commission by the Computer Related Crime Research Unit, Queen Mary, University of London, europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/Study2000/Report.html, zitiert: Queen Mary (University of London), Studie über Netzkriminalität (I).

Rieß, Joachim: Der Telekommunikationsdatenschutz bleibt eine Baustelle, in: DuD 1996, S. 328-334.

Rieß, Joachim: Vom Fernmeldegeheimnis zum Telekommunikationsgeheimnis, S. 127-160, in: Alfred Büllesbach (Hrsg.): Datenschutz im Telekommunikationsrecht, 1. Aufl., Köln 1997, zitiert: Rieß, Vom Fernmeldegeheimnis zum Telekommunikationsgeheimnis.

Rohe, Peter Maria: Verdeckte Informationsgewinnung mit technischen Hilfsmitteln zur Bekämpfung der Organisierten Kriminalität, 1. Aufl., Frankfurt a.M. u.a. 1998, zitiert: Rohe, Verdeckte Informationsgewinnung mit technischen Hilfsmitteln zur Bekämpfung der Organisierten Kriminalität.

Roßnagel, Alexander (Hrsg.): Handbuch Datenschutzrecht, 1. Aufl., München 2003, zitiert: Roßnagel-*Bearbeiter*, Handbuch Datenschutzrecht.

Roßnagel, Alexander (Hrsg.): Recht der Multimedia-Dienste, 1. Aufl., München 1999, Stand: November 2000, zitiert: Roßnagel-*Bearbeiter*.

Roßnagel, Alexander / Pfitzmann, Andreas / Garstka, Hansjürgen: Modernisierung des Datenschutzrechts, Berlin 2001, zitiert: Roßnagel/Pfitzmann/Garstka, Modernisierung des Datenschutzrechts.

RSF, Reporters sans frontières: The Internet on Probation, 05.09.2002, www.rsf.fr/IMG/doc-1274.pdf, zitiert: RSF, The Internet on Probation.

Ruhmann, Ingo / Schulzki-Haddouti, Christiane: Abhör-Dschungel, www.heise.de/ct/98/05/082/, zitiert: Ruhmann/Schulzki-Haddouti, Abhör-Dschungel (I).

Ruhmann, Ingo: Grundlose Gleichbehandlung oder TK-Überwachung und die Praxis, in: DuD 1999, S. 696-698.

Sachs, Michael (Hrsg.): Grundgesetz. Kommentar. 2. Aufl., München 1999, zitiert: Sachs-*Bearbeiter*.

Sachs, Michael (Hrsg.): Grundgesetz. Kommentar. 3. Aufl., München 2003, zitiert: Sachs³-*Bearbeiter*.

Schaar, Peter: Cybercrime und Bürgerrechte, www.sewecom.de/dokumente/buendnis90-gruene/01-09-Reader-Cybercrime-und-Buergerrechte.pdf, zitiert: Schaar, Cybercrime und Bürgerrechte (I).

Schaar, Peter: Datenschutz im Internet, 1. Aufl., München 2002, zitiert: Schaar, Datenschutz im Internet.

Schaar, Peter: EU Forum on Cybercrime - Expert's Meeting on Retention of Traffic Data, 06.11.2001, www.peter-schaar.de/Traffic_Data_Retention.pdf, zitiert: Schaar, Retention (I).

Schaar, Peter: Forderungen an Politik und Gesetzgebung, 17.06.2002, www.peter-schaar.de/FES-statement.pdf, zitiert: Schaar, Forderungen an Politik und Gesetzgebung (I).

Schaar, Peter: Persönlichkeitsprofile im Internet, in: DuD 2001, S. 383-388.

Schaar, Peter: Sicherheit und Freiheitsrechte im Internet, Folien zum Boppard-Diskurs „Mit IT-Sicherheit gegen Internet-Kriminalität?“, 05./06.12.2001, www.peter-schaar.de/schutzkonzepte.pdf, zitiert: Schaar, Sicherheit und Freiheitsrechte (I).

Schaffland, Hans-Jürgen / Wiltfang, Noeme: Bundesdatenschutzgesetz, Berlin, Stand: Oktober 2003, zitiert: Schaffland/Wiltfang, BDSG.

Schenke, Ralf: Verfassungsrechtliche Probleme einer präventiven Überwachung der Telekommunikation, in: AöR 125 (2000), S. 1-44.

Schenke, Ralf: Verfassungsrechtliche Probleme einer präventiven Überwachung der Telekommunikation, in: AöR 125 (2000), S. 1-44.

Schenke, Wolf-Rüdiger: Die Verwendung der durch strafprozessuale Überwachung der Telekommunikation gewonnenen personenbezogenen Daten zur Gefahrenabwehr, in: JZ 2001, S. 997-1004.

Schenke, Wolf-Rüdiger: Polizei- und Ordnungsrecht, 1. Aufl., Heidelberg 2002, zitiert: Schenke, Polizei- und Ordnungsrecht.

Schieder, Peter (Präsident der parlamentarischen Versammlung des Europarates): Contribution at the colloquium on „Anti-Terrorist Measures and Human Rights“ in Vienna, 30.10.2002, www.coe.int/T/d/Com/Dossiers/Themen/Terrorismus/DiscSchieder_Vienne2002.asp, zitiert: Schieder, Anti-Terrorist Measures and Human Rights (I).

Schild, Hans-Hermann: Verwendung von Daten aus erkennungsdienstlicher Behandlung nach § 81b StPO, in: DuD 2002, S. 679-683.

Schily, Otto: Rede des Bundesinnenministers zu den Terroranschlägen in den USA und den Beschlüssen des Sicherheitsrates der Vereinten Nationen sowie der Nato vor dem Deutschen Bundestag am 19.09.2001, in: documentArchiv.de (Hrsg.), www.documentArchiv.de/brd/2001/rede_schily_0919.html, zitiert: Schily, Terrorismusrede (I).

Schmitz, Peter: Anmerkung zu RegPräs Darmstadt, MMR 2003, 213-214, in: MMR 2003, 214-216.

Schmitz, Peter: TDDSG und das Recht auf informationelle Selbstbestimmung, 1. Aufl., München 2000, zitiert: Schmitz, TDDSG.

Schneider, Hans Joachim: Einführung in die Kriminologie, 3. Aufl., Berlin u.a. 1993, zitiert: Schneider, Kriminologie.

Scholz, Rupert: „Reformismus“ statt wirklicher Reformen, in: ZRP 2002, S. 361-362.

Schulzki-Haddouti, Christiane: Internationale Abhörpolitik, S. 125-130 in: Holznagel, Bernd / Nelles, Ursula / Sokol, Bettina (Hrsg.): Die neue TKÜV (Telekommunikations-Überwachungsverordnung), 1. Aufl., München 2002, zitiert: Schulzki-Haddouti, Internationale Abhörpolitik.

Schütte, Matthias: Befugnis des Bundesgrenzschutzes zu lageabhängigen Personenkontrollen, in: ZRP 2002, S. 393-399.

Schwarze, Jürgen (Hrsg.): EU-Kommentar, 1. Aufl., Baden-Baden 2000, zitiert: Schwarze-*Bearbeiter*.

Schweer, Martin / Thies, Barbara: Kriminalität und Kriminalitätsfurcht, in: Kriminalistik 2000, S. 336-342.

Schweitzer, Michael: 3. Staatsrecht, Völkerrecht, Europarecht. 7. Aufl., Heidelberg 2000, zitiert: Schweitzer.

Schwimmer, Walter (Generalsekretär des Europarates): Elements for a statement at the concluding discussion of the colloquium on „Anti-terrorist measures and Human Rights“ in Vienna, 30/31.10.2002, www.coe.int/T/d/Com/Dossiers/Themen/Terrorismus/Disc_Schwimmer.asp, zitiert: Schwimmer, Anti-terrorist measures and Human Rights (I).

Sherman, Lawrence W. / Gottfredson, Denise / MacKenzie, Doris / Eck, John / Reuter, Peter / Bushway, Shawn: Preventing Crime: What works, what doesn't, what's promising. A report to the United States Congress, www.ncjrs.org/ojjdp/exefiles/docword.exe, zitiert: Sherman u.a.-*Bearbeiter*, Preventing Crime (I).

Sieber, Ulrich: Gutachten im Auftrag des Deutschen Multimedia Verbandes e.V. (dmmv) und des Verbandes Privaten Rundfunks und Telekommunikation e. V. (VPRT) zum Thema Datenpiraterie, 12.09.2002, Technischer Teil, www.dmmv.de/shared/data/zip/2501_006_019_druckversion 020904.zip, zitiert: Sieber, Gutachten zum Thema Datenpiraterie (I).

Sieber, Ulrich: Legal Aspects of Computer-Related Crime in the Information Society, COMCRIME-Studie für die Europäische Kommission, 01.01.1998, europa.eu.int/ISPO/legal/en/comcrime/sieber.doc, zitiert: Sieber, COMCRIME-Studie (I).

Simitis, Spiros (Hrsg.): Kommentar zum Bundesdatenschutzgesetz, 5. Aufl., Baden-Baden 2003, zitiert: Simitis-*Bearbeiter*.

Simitis, Spiros: Daten- oder Tatenschutz – ein Streit ohne Ende? In: NJW 1997, S. 1902-1903.

Simitis, Spiros: Datenschutz – Rückschritt oder Neubeginn? In: NJW 1998, S. 2473-2479.

Simitis, Spiros: Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung, in: NJW 1984, S. 394-405.

Simitis, Spiros: Internet oder der entzauberte Mythos vom „freien Markt der Meinungen“, in: Assmann, Heinz-Dieter u.a. (Hrsg.): Wirtschafts- und Medienrecht in der offenen Demokratie, 1. Aufl., Heidelberg 1997, S. 285-314, zitiert: Simitis, Internet.

Simitis, Spiros: Von der Amtshilfe zur Informationshilfe – Informationsaustausch und Datenschutzanforderungen in der öffentlichen Verwaltung, in: NJW 1986, S. 2795-2805.

Starkgraff, K.H.: Der Richtervorbehalt – prozedurale Grundrechtssicherung oder rechtsstaatliches Trostpflaster? In: ZRP 1998, S. 484.

Steinke, Wolfgang: Telefondatenspeicherung – Neue Perspektiven für die Polizei, in: NStZ 1992, S. 372-373.

Stelkens, Paul / Bonk, Heinz Joachim / Sachs, Michael (Hrsg.): Verwaltungsverfahrensgesetz. Kommentar. 6. Aufl., München 2001, zitiert: Stelkens/Bonk/Sachs-*Bearbeiter*.

Stern, Klaus: Das Staatsrecht der Bundesrepublik Deutschland, Bd. 3 Halbbd. 2: 1. Aufl., München 1994, zitiert: Stern.

Streinz, Rudolf: Europarecht, 4. Aufl., Heidelberg 1999, zitiert: Streinz, Europarecht.

Symatec: Symantec Internet Security Threat Report, Februar 2003, ses.symantec.com/PDF/Threat_Report_Final_4C.pdf, zitiert: Symantec, Symantec Internet Security Threat Report (I).

Tallo, Ivar: Bericht zum Entwurf des Cybercrime-Abkommens, Dokument Nr. 9031, 10.04.2001, assembly.coe.int/Main.asp?link=http%3A%2F%2Fassembly.coe.int%2FDocuments%2FWorkingDocs%2FDoc01%2FEDOC9031.htm, zitiert: Tallo, Bericht zum Entwurf des Cybercrime-Abkommens (I).

Tauss, Jörg / Kelber, Ulrich: Zum Schutz kritischer Infrastrukturen, in: DuD 2001, S. 694-695.

The President's Working Group on Unlawful Conduct on the Internet (USA): The Electronic Frontier, The challenge of unlawful conduct involving the use of the Internet, März 2000, www.usdoj.gov/criminal/cybercrime/unlawful.htm, zitiert: The President's Working Group on Unlawful Conduct on the Internet (USA), The Electronic Frontier (I).

Tuengerthal, Hansjürgen: Zur Umsetzung von EG-Richtlinien und staatengerichteten EG-Entscheidungen in deutsches Recht und Überprüfung der Umsetzung der Fleischhygienegebührenrechtsakte der EG, Frankfurt a.M. 2003, www.richtlinienumsetzung.de/tuenger.pdf, zitiert: Tuengerthal, Zur Umsetzung von EG-Richtlinien (I).

Uhe, Bianca / Herrmann, Jens: Überwachung im Internet – Speicherung von personenbezogenen Daten auf Vorrat durch Internet Service Provider, 18.08.2003, ig.cs.tu-berlin.de/oldstatic/da/2003-08/UheHerrmann-Diplomarbeit-082003.pdf, zitiert: Uhe/Herrmann, Überwachung im Internet (I).

ULD-SH, Unabhängiges Landeszentrum für Datenschutz in Schleswig-Holstein: Bundesratsmehrheit plant Anschlag auf das Recht auf unbeobachtete Kommunikation, Pressemitteilung vom 29.05.2002, www. datenschutzzentrum.de/material/themen/presse/kommunik.htm, zitiert: ULD-SH, Bundesratsmehrheit plant Anschlag auf das Recht auf unbeobachtete Kommunikation (I).

ULD-SH, Unabhängiges Landeszentrum für Datenschutz in Schleswig-Holstein: Verstößt das IMSI-Catcher-Gesetz gegen das Zitiergebot des Art. 19 Abs. 1 S. 2 Grundgesetz?, www.datenschutzzentrum.de/material/themen/divers/imsicat, zitiert: ULD-SH, IMSI (I).

ULD-SH, Unabhängiges Landeszentrum für Datenschutz in Schleswig-Holstein: Kriminalität im Internet offenbar weit geringer als bislang angenommen, Pressemitteilung vom 15.08.2002, www.datenschutzzentrum.de/material/themen/presse/interkrim.htm, zitiert: ULD-SH, Internet-Kriminalität (I).

ULD-SH, Unabhängiges Landeszentrum für Datenschutz in Schleswig-Holstein: Rote Karte für Internetschnüffler, Hintergrundinformationen, www.datenschutzzentrum.de/material/themen/rotekarte/hintergr.htm, zitiert: ULD-SH, Kampagne, Hintergrund (I).

ULD-SH, Unabhängiges Landeszentrum für Datenschutz in Schleswig-Holstein: Sichere Informationsgesellschaft, Bekämpfung der Computerkriminalität und Datenschutz – Stellungnahme zur Mitteilung der Kommission KOM(2000) 890, zugleich Kritik des Entwurfs einer „Convention on Cyber-Crime“ des Europarats (PC-CY (2000) Draft No. 25 Rev.), www.datenschutzzentrum.de/material/themen/cybercri/cyberkon.htm, zitiert: ULD-SH, Sichere Informationsgesellschaft (I).

Waechter, Kay: Bereitstellungspflicht für Fernmeldeanlagenbetreiber, in: VerwArch 87 (1996), S. 68-96.

Waechter, Kay: Die „Schleierfahndung“ als Instrument der indirekten Verhaltenssteuerung durch Abschreckung und Verunsicherung, in: DÖV 1999, S. 138-147.

Weichert, Thilo: Datenschutz zwischen Terror und Informationsgesellschaft, www.datenschutzverein.de/Themen/terrords2.html, zitiert: Weichert, Terror und Informationsgesellschaft (I).

Weichert, Thilo: Datenschutzrechtliche Anforderungen an die Bekämpfung von Internet-Kriminalität, Beitrag zum Symposium „Internet-Kriminalität“ des Landeskriminalamts Mecklenburg-Vorpommern am 01.11.2000, www.datenschutzzentrum.de/material/themen/cybercri/cyber_mv.htm, zitiert: Weichert, Bekämpfung von Internet-Kriminalität (I).

Weichert, Thilo: Terrorismusbekämpfungsgesetze – Auswirkungen für die Wirtschaft, 10.07.2002, www.datenschutzzentrum.de/material/themen/divers/terrwir.htm, zitiert: Weichert, Terrorismusbekämpfungsgesetze (I).

Weichert, Thilo: Überwachungsstaat nicht zulassen, in: DuD 2001, S. 694.

Weinem, Wolfgang: Die moderne Überwachung der Telekommunikation – Möglichkeiten und Grenzen im gesetzlichen Rahmen, S. 451-478 in: Festschrift für Horst Herold zum 75. Geburtstag, 1. Aufl., 1998, zitiert: Weinem, TK-Überwachung.

Welp, Jürgen: Die strafprozessuale Überwachung des Post- und Fernmeldeverkehrs, 1. Aufl., Heidelberg 1974, zitiert: Welp, Die strafprozessuale Überwachung des Post- und Fernmeldeverkehrs.

Welp, Jürgen: Die TKÜV im System staatlicher Abhörbefugnisse, S. 3-14 in: Holznagel, Bernd / Nelles, Ursula / Sokol, Bettina (Hrsg.): Die neue TKÜV (Telekommunikations-Überwachungsverordnung), 1. Aufl., München 2002, zitiert: Welp, TKÜV.

Welp, Jürgen: Strafprozessuale Zugriffe auf Verbindungsdaten des Fernmeldeverkehrs, in: NStZ 1994, S. 209-215.

Welp, Jürgen: Überwachung und Kontrolle, 1. Aufl., Berlin 2000, zitiert: Welp, Überwachung und Kontrolle.

Werner, Ulrich: Befugnisse der Sicherheitsbehörden nach neuem Telekommunikationsrecht, in: Der Hamburgische Datenschutzbeauftragte (Hrsg.), Datenschutz bei Multimedia und Telekommunikation, 1. Aufl., Hamburg 1998, S. 37-54, zitiert: Werner, Befugnisse der Sicherheitsbehörden.

Weßlau, Edda: Gefährdungen des Datenschutzes durch den Einsatz neuer Medien im Strafprozess, in: ZStW 113 (2001), S. 681-708.

wik-Consult: Studie im Auftrag des Bundesministeriums für Wirtschaft und Arbeit über den rechtlichen Rahmen für das Angebot von TK-Diensten und den Betrieb von TK-Anlagen in den G7-Staaten in Bezug auf die Sicherstellung der Überwachbarkeit der Telekommunikation, April 2003, www.bmwi.de/Redaktion/Inhalte/Pdf/Homepage_2Fdownload_2Ftelekommunikation__post_2FTKUE-G7__K.pdf,property=pdf.pdf, zitiert: wik-Consult, Studie (I).

Windthorst, Kay: Verfassungsrecht I. Grundlagen. 1. Aufl., München 1994, zitiert: Windthorst.

Wuermeling, Ulrich / Felixberger, Stefan: Fernmeldegeheimnis und Datenschutz im Telekommunikationsgesetz, in: CR 1997, S. 230-238.

Ziercke, Jörg: Welche Eingriffsbefugnisse benötigt die Polizei? In: DuD 1998, S. 319-323.

Zwingel, Wolfgang: Technische Überwachungsmaßnahmen aus Sicht der Polizei, S. 37-46 in: Holznagel, Bernd / Nelles, Ursula / Sokol, Bettina (Hrsg.): Die neue TKÜV (Telekommunikations-Überwachungsverordnung), 1. Aufl., München 2002, zitiert: Zwingel, Technische Überwachungsmaßnahmen aus Sicht der Polizei.