

An das
Bundesverfassungsgericht
Schlossbezirk 3
76131 Karlsruhe

Verfassungsbeschwerde

von Patrick Breyer, [...anonymisiert...]

wegen

Ausweiszwang für im Voraus bezahlte Mobilfunkanschlüsse

A. Antrag

Ich beantrage festzustellen, dass § 111 Absatz 1 Sätze 3-7 des Telekommunikationsgesetzes vom 22.06.2004 (BGBl. I S. 1190), zuletzt geändert durch Gesetz vom 27.06.2017 (BGBl. I S. 1963), meine Grundrechte aus den Artikeln 2 in Verbindung mit 1 sowie aus Artikel 5 GG verletzen und nichtig sind.

B. Sachverhalt

Ich beschwere mich über die Pflicht zur Identifizierung aller Inhaber im voraus bezahlter Mobilfunkanschlüsse in Deutschland anhand eines Ausweispapiers o.ä., weil sie meine Rechte auf informationelle Selbstbestimmung (Art. 2, 1 GG) sowie auf freie Meinungsäußerung und freien Informationszugang (Art. 5 GG) verletzt.

I. Gesetzeslage

Am 22.06.2004 hat der deutsche Gesetzgeber ein Telekommunikationsgesetz beschlossen, das unter anderem folgende Bestimmung enthielt:

§ 111 Daten für Auskunftersuchen der Sicherheitsbehörden

(1) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt und dabei Rufnummern vergibt oder Telekommunikationsanschlüsse für von anderen vergebene Rufnummern bereitstellt, hat für die Auskunftsverfahren nach den §§ 112 und 113 die Rufnummern, den Namen und die Anschrift des Rufnummerninhabers, das Datum des Vertragsbeginns, bei natürlichen Personen deren Geburtsdatum, sowie bei Festnetzanschlüssen auch die Anschrift des Anschlusses vor der Freischaltung zu erheben und unverzüglich zu speichern, auch soweit diese Daten für betriebliche Zwecke nicht erforderlich sind; das Datum des Vertragsendes ist bei Bekanntwerden ebenfalls zu speichern. Satz 1 gilt auch, soweit die Daten nicht in Teilnehmerverzeichnisse (§ 104) eingetragen werden. Wird dem Verpflichteten nach Satz 1 eine Änderung bekannt, hat er die Daten unverzüglich zu berichtigen; in diesem Zusammenhang hat er bisher noch nicht erfasste Daten nach Satz 1 nachträglich zu erheben und zu speichern, sofern ihm eine Erhebung der Daten ohne besonderen Aufwand möglich ist. Nach Ende des Vertragsverhältnisses sind die Daten mit Ablauf des auf die Beendigung folgenden Kalenderjahres zu löschen. Eine Entschädigung für die Datenerhebung und -speicherung wird nicht gewährt. Für das Auskunftsverfahren nach § 113 ist die Form der Datenspeicherung freigestellt.

(2) Bedient sich der Diensteanbieter nach Absatz 1 Satz 1 eines Vertriebspartners, hat der Vertriebspartner die Daten nach Absatz 1 Satz 1 zu erheben und diese sowie die nach § 95 erhobenen Daten unverzüglich dem Diensteanbieter zu übermitteln; Absatz 1 Satz 2 gilt entsprechend. Satz 1 gilt auch für Daten über Änderungen, soweit sie dem Vertriebspartner im Rahmen der üblichen Geschäftsabwicklung zur Kenntnis gelangen.

(3) Für Vertragsverhältnisse, die am Tage des Inkrafttretens dieser Vorschrift bereits bestehen, müssen Daten im Sinne von Absatz 1 Satz 1 außer in den Fällen des Absatzes 1 Satz 3 nicht nachträglich erhoben werden.

Durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21.12.2007 hat § 111 TKG folgende Fassung erhalten:

§ 111 Daten für Auskunftersuchen der Sicherheitsbehörden

(1) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt und dabei Rufnummern oder andere Anschlusskennungen vergibt oder Telekommunikationsanschlüsse für von anderen vergebene

ne Rufnummern oder andere Anschlusskennungen bereitstellt, hat für die Auskunftsverfahren nach den §§ 112 und 113

1. die Rufnummern und anderen Anschlusskennungen,
2. den Namen und die Anschrift des Anschlussinhabers,
3. bei natürlichen Personen deren Geburtsdatum,
4. bei Festnetzanschlüssen auch die Anschrift des Anschlusses,
5. in Fällen, in denen neben einem Mobilfunkanschluss auch ein Mobilfunkendgerät überlassen wird, die Gerätenummer dieses Gerätes sowie
6. das Datum des Vertragsbeginns

vor der Freischaltung zu erheben und unverzüglich zu speichern, auch soweit diese Daten für betriebliche Zwecke nicht erforderlich sind; das Datum des Vertragsendes ist bei Bekanntwerden ebenfalls zu speichern. Satz 1 gilt auch, soweit die Daten nicht in Teilnehmerverzeichnisse (§ 104) eingetragen werden. Die Verpflichtung zur unverzüglichen Speicherung nach Satz 1 gilt hinsichtlich der Daten nach Satz 1 Nr. 1 und 2 entsprechend für denjenigen, der geschäftsmäßig einen öffentlich zugänglichen Dienst der elektronischen Post erbringt und dabei Daten nach Satz 1 Nr. 1 und 2 erhebt, wobei an die Stelle der Daten nach Satz 1 Nr. 1 die Kennungen der elektronischen Postfächer und an die Stelle des Anschlussinhabers nach Satz 1 Nr. 2 der Inhaber des elektronischen Postfachs tritt. Wird dem Verpflichteten nach Satz 1 oder Satz 3 eine Änderung bekannt, hat er die Daten unverzüglich zu berichtigen; in diesem Zusammenhang hat der nach Satz 1 Verpflichtete bisher noch nicht erhobene Daten zu erheben und zu speichern, sofern ihm eine Erhebung der Daten ohne besonderen Aufwand möglich ist. Für das Auskunftsverfahren nach § 113 ist die Form der Datenspeicherung freigestellt.

(2) Bedient sich der Diensteanbieter nach Absatz 1 Satz 1 oder Satz 3 eines Vertriebspartners, hat der Vertriebspartner die Daten nach Absatz 1 Satz 1 und 3 unter den dort genannten Voraussetzungen zu erheben und diese sowie die nach § 95 erhobenen Daten unverzüglich dem Diensteanbieter zu übermitteln; Absatz 1 Satz 2 gilt entsprechend. Satz 1 gilt auch für Daten über Änderungen, soweit sie dem Vertriebspartner im Rahmen der üblichen Geschäftsabwicklung zur Kenntnis gelangen.

(3) Für Vertragsverhältnisse, die am Tage des Inkrafttretens dieser Vorschrift bereits bestehen, müssen Daten im Sinne von Absatz 1 Satz 1 oder Satz 3 außer in den Fällen des Absatzes 1 Satz 4 nicht nachträglich erhoben werden.

(4) Die Daten sind mit Ablauf des auf die Beendigung des Vertragsverhältnisses folgenden Kalenderjahres zu löschen.

(5) Eine Entschädigung für die Datenerhebung und -speicherung wird nicht gewährt.

Durch das Gesetz zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus vom 26.07.2016 hat § 111 TKG folgende Fassung erhalten:

§ 111 Daten für Auskunftersuchen der Sicherheitsbehörden

(1) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt und dabei Rufnummern oder andere Anschlusskennungen vergibt oder Telekommunikationsanschlüsse für von anderen vergebene Rufnummern oder andere Anschlusskennungen bereitstellt, hat für die Auskunftsverfahren nach den §§ 112 und 113

1. die Rufnummern und anderen Anschlusskennungen,
2. den Namen und die Anschrift des Anschlussinhabers,
3. bei natürlichen Personen deren Geburtsdatum,

4. bei Festnetzanschlüssen auch die Anschrift des Anschlusses,
5. in Fällen, in denen neben einem Mobilfunkanschluss auch ein Mobilfunkendgerät überlassen wird, die Gerätenummer dieses Gerätes sowie
6. das Datum des Vertragsbeginns

vor der Freischaltung zu erheben und unverzüglich zu speichern, auch soweit diese Daten für betriebliche Zwecke nicht erforderlich sind; das Datum des Vertragsendes ist bei Bekanntwerden ebenfalls zu speichern. Satz 1 gilt auch, soweit die Daten nicht in Teilnehmerverzeichnisse (§ 104) eingetragen werden. Bei im Voraus bezahlten Mobilfunkdiensten ist die Richtigkeit der nach Satz 1 erhobenen Daten vor der Freischaltung zu überprüfen durch

1. Vorlage eines Ausweises im Sinne des § 2 Absatz 1 des Personalausweisgesetzes,
2. Vorlage eines Passes im Sinne des § 1 Absatz 2 des Passgesetzes,
3. Vorlage eines sonstigen gültigen amtlichen Ausweises, der ein Lichtbild des Inhabers enthält und mit dem die Pass- und Ausweispflicht im Inland erfüllt wird, wozu insbesondere auch ein nach ausländerrechtlichen Bestimmungen anerkannter oder zugelassener Pass, Personalausweis oder Pass- oder Ausweiser-satz zählt,
4. Vorlage eines Aufenthaltstitels,
5. Vorlage eines Ankunftsnachweises nach § 63a Absatz 1 des Asylgesetzes oder einer Bescheinigung über die Aufenthaltsgestattung nach § 63 Absatz 1 des Asylgesetzes,
6. Vorlage einer Bescheinigung über die Aussetzung der Abschiebung nach § 60a Absatz 4 des Aufenthaltsgesetzes oder
7. Vorlage eines Auszugs aus dem Handels- oder Genossenschaftsregister oder einem vergleichbaren amtlichen Register oder Verzeichnis, der Gründungsdokumente oder gleichwertiger beweiskräftiger Dokumente oder durch Einsichtnahme in diese Register oder Verzeichnisse und Abgleich mit den darin enthaltenen Daten, sofern es sich bei dem Anschlussinhaber um eine juristische Person oder Personengesellschaft handelt,

soweit die Daten in den vorgelegten Dokumenten oder eingesehenen Registern oder Verzeichnissen enthalten sind. Die Überprüfung kann auch durch andere geeignete Verfahren erfolgen; die Bundesnetzagentur legt nach Anhörung der betroffenen Kreise durch Verfügung im Amtsblatt fest, welche anderen Verfahren zur Überprüfung geeignet sind, wobei jeweils zum Zwecke der Identifikation vor Freischaltung der vertraglich vereinbarten Mobilfunkdienstleistung ein Dokument im Sinne des Satzes 3 genutzt werden muss. Bei der Überprüfung ist die Art des eingesetzten Verfahrens zu speichern; bei Überprüfung mittels eines Dokumentes im Sinne des Satzes 3 Nummer 1 bis 6 sind ferner Angaben zu Art, Nummer und ausstellender Stelle zu speichern. Für die Identifizierung anhand eines elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes gilt § 8 Absatz 2 Satz 4 des Geldwäschegesetzes entsprechend. Für das Auskunftsverfahren nach § 113 ist die Form der Datenspeicherung freigestellt.

(2) Die Verpflichtung zur unverzüglichen Speicherung nach Absatz 1 Satz 1 gilt hinsichtlich der Daten nach Absatz 1 Satz 1 Nummer 1 und 2 entsprechend für denjenigen, der geschäftsmäßig einen öffentlich zugänglichen Dienst der elektronischen Post erbringt und dabei Daten nach Absatz 1 Satz 1 Nummer 1 und 2 erhebt, wobei an die Stelle der Daten nach Absatz 1 Satz 1 Nummer 1 die Kennungen der elektronischen Postfächer und an die Stelle des Anschlussinhabers nach Absatz 1 Satz 1 Nummer 2 der Inhaber des elektronischen Postfachs tritt.

(3) Wird dem Verpflichteten nach Absatz 1 Satz 1 oder Absatz 2 eine Änderung bekannt, hat er die Daten unverzüglich zu berichtigen. In diesem Zusammenhang hat der nach Absatz 1 Satz 1 Verpflichtete bisher

noch nicht erhobene Daten zu erheben und zu speichern, sofern ihm eine Erhebung der Daten ohne besonderen Aufwand möglich ist.

(4) Bedient sich ein Diensteanbieter zur Erhebung der Daten nach Absatz 1 Satz 1 und Absatz 2 eines Dritten, bleibt er für die Erfüllung der Pflichten nach Absatz 1 Satz 1 und Absatz 2 verantwortlich. Werden dem Dritten im Rahmen des üblichen Geschäftsablaufes Änderungen der Daten nach Absatz 1 Satz 1 und Absatz 2 bekannt, hat er diese dem Diensteanbieter unverzüglich zu übermitteln.

(5) Die Daten nach den Absätzen 1 und 2 sind mit Ablauf des auf die Beendigung des Vertragsverhältnisses folgenden Kalenderjahres zu löschen.

(6) Eine Entschädigung für die Datenerhebung und -speicherung wird nicht gewährt.

Vor Inkrafttreten der vorbezeichneten Vorschriften konnten Telekommunikationsanschlüsse bei diversen Anbietern unter Angabe einer nicht existierenden Identität (Pseudonym) registriert und benutzt werden, so dass eine anonyme mobile Telekommunikation und Internetnutzung möglich war. Überprüft wurde allenfalls die Existenz der Anschrift, nicht aber, ob dort tatsächlich eine Person des angegebenen Namens gemeldet ist. Künftig ist dies nicht mehr möglich.

II. Betroffenheit des Beschwerdeführers

Der Beschwerdeführer nutzt sein Mobiltelefon zur mobilen Sprachkommunikation. Der Anbieter E-Plus speichert 3-4 Monate lang, von wem über sein Netz Anrufe entgegen genommen wurden und wer wen angerufen hat. Bei jeder ein- oder ausgehenden Verbindung speichert E-Plus zudem den Standort (Funkzelle), die Kartenkennung (IMSI) und die Geräteerkennung (IMEI).¹

Der Beschwerdeführer ist in der Bürgerrechtsorganisation „Arbeitskreis Vorratsdatenspeicherung“ aktiv. Es handelt sich um einen Zusammenschluss von Bürgerrechtlern, Datenschützern und Internet-Nutzern, mithin um eine Bürgerinitiative. Die Aktivitäten des Arbeitskreises werden ausschließlich über das Internet koordiniert. Der Beschwerdeführer hat mehrere Demonstrationen des Arbeitskreises maßgeblich mit organisiert. Zur Vorbereitung der Demonstrationen sind elektronische Kontakte mit den zahlreichen Kooperationspartnern und Unterstützern erforderlich. Bei Vorbereitungstreffen mit der Polizei waren auch Beamte des Landesverfassungsschutzes anwesend, weswegen auch sonst mit einer nachrichtendienstlichen Beobachtung der – vollkommen legalen – Aktivitäten des Arbeitskreises gerechnet werden muss. Der Beschwerdeführer fühlt sich in seinen regierungskritischen Aktivitäten beeinträchtigt, wenn sein gesamtes mobiles Kommunikations-, Bewegungs- und Internetnutzungsverhalten für staatliche Stellen personenbezogen nachvollziehbar ist.

Hinzu kommt, dass der Beschwerdeführer im Internet publizistisch tätig ist, sowohl auf dem Internetportal des Arbeitskreises Vorratsdatenspeicherung als auch auf einem eigenen überwachungskritischen Internetportal.² Der Arbeitskreis Vorratsdatenspeicherung hat in der Vergangenheit immer wieder nicht-öffentliche amtliche Dokumente zum Thema Überwachung der Öffentlichkeit zugänglich gemacht. Seine Mitglieder sind dazu darauf angewiesen, anonym mit Informanten kommunizieren zu können.

Schließlich war der Beschwerdeführer von 2012-2017 Landtagsabgeordneter. Aus dieser Zeit hat er vertrauliche Kontakte zu Informanten, die es ihm ermöglicht haben, Missstände und rechtswidrige Praktiken in der schleswig-holsteinischen Landespolizei aufzudecken (z.B. Affäre um sexistische und rassistische Äußerungen von Polizeischülern, Vorwürfe der Unterdrückung entlastender Aussagen im Landeskriminalamt). In der zuletzt genannten Affäre, welche der Beschwerdeführer aufgedeckt hat und zu welcher voraussichtlich ein Untersuchungsausschuss eingerichtet werden wird, recherchiert und veröffentlicht der Beschwerdeführer aktuell.

¹ Bundesnetzagentur, Erhebung vom Januar bis März 2011, http://wiki.vorratsdatenspeicherung.de/images/BNetzA_Speicherdauer.pdf.

² <http://www.daten-speicherung.de>.

Der Beschwerdeführer besitzt und benutzt eine vorausbezahlte Mobiltelefonkarte des Netzes von Eplus. Diese ist noch auf eine falsche Identität registriert worden. Mit zunehmender Benutzung verliert die Karte allerdings an Anonymität (u.a. aufgrund der angefallenen Verkehrsdaten). Außerdem ist mit einer Sperrung im Fall der Datenprüfung jederzeit zu rechnen. Früher oder später wird er eine neue Mobiltelefonkarte registrieren müssen.

Zum Schutz von Informanten vor Nachteilen durch die Anbahnung und Abwicklung von Kontakten mit dem Beschwerdeführer wäre es nötig, anonyme und wechselnde im voraus bezahlte SIM-Karten zu nutzen. Dies ist dem Beschwerdeführer wegen des verfahrensgegenständlichen Gesetzes nicht mehr möglich. Die mangelnde Anonymität der für den Beschwerdeführer verfügbaren Prepaidkarten kann Bürger und Hinweisgeber davon abhalten, ihn im Fall eines Anrufs über Missstände zu informieren. Über die nach § 111 TKG anzugebenden Daten kann der Anschluss des Beschwerdeführers überwacht werden, wenn er vertrauliche Kontakte mit Bürgern und Hinweisgebern abwickelt.

Insoweit ist der Beschwerdeführer von der Gesetzesänderung selbst, gegenwärtig und unmittelbar betroffen (vgl. auch § 150 Abs. 15 S. 2 TKG).

Die Anbieter speichern die nach § 111 TKG erhobenen Daten zusammen mit den zugewiesenen Rufnummern. Die Daten stehen über ein automatisiertes Such- und Abrufverfahren (§ 112 TKG) einer Vielzahl staatlicher Behörden zum direkten Online-Abruf zur Verfügung. Über 100 Behörden haben zurzeit Zugriff auf die Kundendaten (sog. „Bestandsdaten“) von 116 Telekommunikationsunternehmen.³ Im Jahr 2016 sind über 10 Mio. behördliche Abrufe von bzw. Suchanfragen nach Telekommunikations-Bestandsdaten erfolgt, was über 27.000 Abfragen täglich entspricht.⁴ Der Beschwerdeführer wird nicht in Kenntnis gesetzt, wenn seine Daten ausgelesen werden; er erhält auch auf Nachfrage keine Auskunft über behördliche Zugriffe auf seine Daten.

III. Beschwerdefrist

Das Gesetz zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus vom 26.07.2016, mit dem die Ausweispflicht eingeführt wurde, ist am Tag nach der Verkündung und damit am 30.07.2016 um 0 Uhr in Kraft getreten. Da der 29.07.2017 auf einen Samstag fällt, endet die Beschwerdefrist am Montag, den 31.07.2017 um 24 Uhr.

IV. Relevanz von Telekommunikation

100% der Haushalte in Deutschland verfügten 2014 über mindestens einen eigenen Festnetz- oder Mobilfunkanschluss. In 92% der Haushalte gab es einen Festnetzanschluss, in 91% der Haushalte einen Mobilfunkanschluss, in 76% der Haushalte ein Internetanschluss. 66% der deutschen Haushalte nutzten mindestens eine vorausbezahlte Mobilfunkkarte (Prepaid), 29% der Haushalte nutzen Mobiltelefone ausschließlich mit Prepaidkarten.⁵

78% der Deutschen nutzen das Internet täglich oder praktisch täglich.⁶ Internetnutzer verbringen durchschnittlich mehr als zwei Stunden (137 Minuten) pro Tag im Netz.⁷ 73% der Deutschen schreiben und lesen Textnachrichten über das Internet (E-Mails),⁸ 33% senden Nachrichten über soziale Netzwerke oder Instant Messaging,⁹ 18% tele-

³ Bundesnetzagentur, <http://www.bnetza.de/aav>.

⁴ Bundesnetzagentur, <http://www.bnetza.de/aav>.

⁵ Eurobarometer, E-Communications Household Survey von 2014, http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_414_de.pdf.

⁶ Eurostat, Internetnutzung täglich (I_IDAY).

⁷ Bundesnetzagentur, Jahresbericht 2011,

https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Presse/Berichte/2012/Jahresbericht2011pdf.pdf?__blob=publicationFile, 88.

⁸ Eurostat, Senden/Empfangen von E-Mails (I_IUEM).

⁹ Eurostat, Versenden von Nachrichten an soziale Medien-Webseiten oder "Instant Messaging" (I_IUFORIM).

fonieren über das Internet.¹⁰ 44% nutzen soziale oder berufliche Netzwerke im Internet.¹¹ 70% informieren sich online über Waren und Dienstleistungen.¹² 25% hören im Internet Radio oder sehen fern.¹³ 38% nutzen das Internet für Zwecke der Ausbildung oder Weiterbildung.¹⁴ 18% suchen im Internet nach einer Arbeitsstelle.¹⁵ 35% informieren sich auf staatlichen Internetportalen,¹⁶ 37% kommunizieren über das Internet mit Behörden.¹⁷

52% lesen über das Internet Online-Zeitungen und Nachrichtenmagazine.¹⁸ 58% informieren sich in Online-Lexika wie Wikipedia.¹⁹ 22% veröffentlichen eigene Inhalte im Internet.²⁰ 23% lesen oder verfassen Meinungsbeiträge über Bürgerangelegenheiten oder politische Themen auf Internetseiten.²¹ 11% nehmen sogar an Beratungen oder Abstimmungen im Internet über Bürgerangelegenheiten oder politische Themen oder an Internet-Petitionen teil.²² 54% beschaffen über das Internet gesundheitsrelevante Informationen.²³

2% der deutschen Haushalte verzichten gänzlich auf einen Internetanschluss, weil sie Bedenken hinsichtlich der Wahrung ihrer Privatsphäre oder Sicherheit haben.²⁴

C. Begründung

I. Verletzung des Rechts auf informationelle Selbstbestimmung

Die Änderung des § 111 TKG verletzt mein Recht auf informationelle Selbstbestimmung, soweit sie mich ohne jeden Anlass zur Preisgabe und Verifizierung meiner Identität zwingt, bevor ich über einen eigenen Anschluss mobil telekommunizieren und das Internet nutzen kann.

1. Eingriff in den Schutzbereich

Art. 2, 1 GG gewährleisten das Recht auf informationelle Selbstbestimmung und auf Schutz personenbezogener Daten. Dieses Recht umfasst die Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen seine persönliche Lebenssachverhalte erhoben, gespeichert, verwendet oder weiter gegeben werden. Die Sammlung und Speicherung personenbezogener Daten stellt einen Eingriff in das Privatleben des Einzelnen dar.

¹⁰ Eurostat, Telefonieren oder Videoanrufe (I_IUPH1).

¹¹ Eurostat, Nutzen von sozialen oder professionellen Netzwerken (I_IUNET).

¹² Eurostat, Suche nach Informationen über Waren und Dienstleistungen (I_IUIF).

¹³ Eurostat, Web-Radio/Web-Fernsehen (I_IUWEB).

¹⁴ Eurostat, Personen, die das Internet in den letzten 3 Monaten für Aus- und Weiterbildung verwendet haben (I_IE-DUT).

¹⁵ Eurostat, Arbeitssuche oder zur Übermittlung einer Stellenbewerbung (I_IUJOB).

¹⁶ Eurostat, Informationsbeschaffung auf Websites öffentlicher Stellen (I_IGOVIF).

¹⁷ Eurostat, Interaktion mit staatlichen Behörden (I_IUGOV).

¹⁸ Eurostat, Lektüre/das Herunterladen von Online-Zeitungen/Nachrichtenmagazinen (I_IUNW).

¹⁹ Eurostat, Verwendung von Wikis/Online-Lexika, um sich Wissen jeglichen Themas anzueignen (I_IUWIKI).

²⁰ Eurostat, selbst geschaffenen Inhalt auf eine für andere zugängliche Website hochladen (I_IUUPL).

²¹ Eurostat, Lesen oder Verfassen von Meinungsäußerungen über Bürgerangelegenheiten oder politische Themen auf Internetseiten (I_IUPOL).

²² Eurostat, Teilnahme an Beratungen oder Abstimmungen im Internet über Bürgerangelegenheiten oder politische Themen (I_IUVOTE).

²³ Eurostat, Beschaffung von gesundheitsrelevanten Informationen (I_IHIF).

²⁴ Eurostat, Haushalte ohne häuslichen Internetzugang, da Bedenken hinsichtlich der Privatsphäre oder der Sicherheit bestehen (H_XSEC).

§ 111 Abs. 1 S. 3 ff. TKG greift nach der Rechtsprechung des Bundesverfassungsgerichts in das Recht auf informationelle Selbstbestimmung ein, indem er die Verfügbarkeit von Telekommunikationsanschlüssen von der Offenbarung und Verifizierung der Identität des Vertragspartners abhängig macht, selbst wo dies aufgrund der Vorauszahlung betrieblich nicht erforderlich ist. Die Vorschriften verbieten dadurch die anonyme Überlassung von Telekommunikationsanschlüssen. Wegen § 111 TKG können Kommunikationsteilnehmer nicht mehr frei entscheiden, ob sie ihre Identität zutreffend angeben oder anonym bzw. pseudonym mobil telekommunizieren möchten.

Der Einordnung des § 111 Abs. 1 S. 3 ff. TKG als staatlichen Eingriff in die Rechte des Beschwerdeführers steht nicht entgegen, dass der Staat private Telekommunikationsanbieter zur Datenerhebung und -vorhaltung verpflichtet. Diese Verpflichtung ist dem Staat zuzurechnen, weil die Anbieter bei der Identifizierung im Auftrag des Staates tätig werden und dabei über kein eigenes Ermessen verfügen. Der Staat verfolgt mit der Identifizierungspflicht eigene Zwecke, nämlich die Verfügbarkeit eines Teilnehmerverzeichnisses für öffentliche Zwecke sicherzustellen. Eine staatlich auferlegte Pflicht zur Datenerhebung durch Private ist als staatlicher Grundrechtseingriff anzusehen, weil sich der Staat gleichzeitig Zugriffsrechte auf die erhobenen Daten einräumt (§§ 112, 113 TKG).

Die Anonymität der Inhaber von Telekommunikationsanschlüssen zu schützen sichert auch die Unbefangenheit der Telekommunikation. Gewährleistet ist eine unbefangene Fernkommunikation ohne Furcht vor Nachteilen nur, wenn anonym kommuniziert werden kann und der Einzelne dadurch vor seiner Identifikation als Teilnehmer an Kommunikationsvorgängen geschützt ist. Der Erläuternde Bericht zur Empfehlung des Europarats zum Datenschutz in der Telekommunikation²⁵ führt in Abs. 5 zutreffend aus, dass die technische Entwicklung „nicht nur die Privatsphäre von Teilnehmern und Nutzern allgemein gefährden kann, sondern auch deren Kommunikationsfreiheit behindern kann, weil sie das Maß an Anonymität mindert, der sich Teilnehmer und Nutzer unter Umständen bei der Benutzung des Telefons bedienen wollen, indem sie gezwungen werden, ihre Identitäten offenzulegen oder elektronische Spuren zu hinterlassen, die es ermöglichen, die Benutzung ihres Telefons zu überwachen.“²⁶

Die Empfehlung des Europarats über den Datenschutz in der Telekommunikation²⁷ bestimmt unter Ziff. 22 ausdrücklich: „Anonyme Zugangsmöglichkeiten zu Telekommunikationsnetzen und -diensten sollten bereit gestellt werden.“ Der Erläuternde Bericht führt in Abs. 26 aus, diese Empfehlung diene dem Schutz der Kommunikationsfreiheit. Telefondienste könnten Teilnehmer oder Nutzer davon abschrecken, telefonisch zu kommunizieren, weil sie zur „Untergrabung der Anonymität“ tendierten.

2. Mangelnde Rechtfertigung

Gerechtfertigt ist der mit § 111 Abs. 1 S. 3 ff. TKG verbundene Eingriff in die Rechte der Beschwerdeführer nur, wenn er verhältnismäßig ist.

Diese Rechtfertigungsvoraussetzung fehlt im Fall des § 111 Abs. 1 S. 3 ff. TKG: Die Vorschrift schränkt das Recht auf informationelle Selbstbestimmung unverhältnismäßig weit ein. Das grundrechtlich geschützte Interesse unbescholtener Bürger daran, Informationen über Telekommunikationsnetze ohne Furcht vor Aufdeckung des Informationsverhaltens entgegennehmen und darüber kommunizieren zu können, überwiegt das Interesse des Staates daran, Straftaten in vergleichsweise seltenen Fällen besser aufklären zu wollen.

a) Verletzung des Verhältnismäßigkeitsgebots

aa) Der erhoffte Nutzen des § 111 Abs. 1 S. 3 ff. TKG

(1) Ziel der Vorschrift

§ 112 TKG zufolge dient die in § 111 TKG vorgeschriebene Identifizierung aller Telekommunikationsteilnehmer der Erfüllung der gesetzlichen Aufgaben der Gerichte, der Strafverfolgungsbehörden, des Zollkriminalamts, der Verfas-

²⁵ Empfehlung R (95) 4 vom 07.02.1995.

²⁶ <https://wcd.coe.int/ViewDoc.jsp?id=529277&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75>.

²⁷ Empfehlung R (95) 4 vom 07.02.1995.

sungsschutzbehörden des Bundes und der Länder, des Militärischen Abschirmdienstes, des Bundesnachrichtendienstes, der Notrufabfragestellen, der Bundesanstalt für Finanzdienstleistungsaufsicht sowie der polizeilichen Gefahrenabwehr und der Schwarzarbeitsbekämpfung. In der Tat kann die Identifizierung von Kommunikationsteilnehmern im Einzelfall zur Ermittlung, Feststellung oder Verfolgung von Straftaten erforderlich sein.

Die Bundesrepublik argumentiert, dass die Verbreitung bestimmter Vertragsgestaltungen der Telekommunikationsdiensteanbieter die Verfügbarkeit von Kundendaten zur Erfüllung staatlicher Aufgaben reduziere.²⁸ Erst die Verbreitung der Mobilfunktechnologie in Verbindung mit vorausbezahlten Tarifen habe die Erforderlichkeit einer Kundenidentifikation für Abrechnungszwecke entfallen lassen. § 111 TKG solle lediglich dafür sorgen, dass – wie zu Zeiten der Deutschen Bundespost – wieder alle Telekommunikationsteilnehmer identifizierbar seien.

Zunächst einmal ist daran zu erinnern, dass auch zu Zeiten der Deutschen Bundespost an Telefonzellen oder sonst fremden Apparaten anonym Gespräche geführt oder angenommen werden konnten. Richtig ist, dass 1995 der erste Mobilfunk-Privatkundentarif in Deutschland angeboten wurde und 1997 die ersten Prepaid-Karten des Unternehmens Mannesmann. Richtig ist aber auch, dass bereits im Jahr 2000 55% der Mobilfunkteilnehmer vorausbezahlte Tarife nutzten.²⁹ Dieser Anteil ist bis heute stabil geblieben. Lediglich die Mobilfunknutzung insgesamt hat deutlich zugenommen.

Auch ohne korrekte Kundendaten sind Inhaber vorausbezahlter Mobilfunkkarten oft mithilfe von Aufladungsdaten, Lokalisierungsdaten oder Überwachungsaufzeichnungen in Geschäften identifizierbar. Im Übrigen profitieren Strafverfolger von der zunehmenden Verbreitung der Mobilfunktechnologie, zu der die Verfügbarkeit von Prepaidkarten maßgeblich beiträgt, enorm: Die Mobilfunktechnologie ermöglicht beispielsweise die Erstellung detaillierter Bewegungsprofile. Durch die Verbreitung der Telekommunikation hat der Staat heute einen so tiefgreifenden Einblick in unser Informations- und Kommunikationsverhalten wie noch nie. So steigt die Zahl der Ermittlungsverfahren, in denen Telekommunikation überwacht wird, seit Jahren sprunghaft an – selbst bei der Ermittlung von Straftaten, die nicht mittels Telekommunikation begangen worden sind.

Früher mögen Inhaber von Festnetzanschlüssen identifizierbar gewesen sein. Damals wurde anstelle von SMS und Internet aber noch im persönlichen Kontakt miteinander kommuniziert, korrespondiert und sich informiert, was für den Staat weit weniger nachvollziehbar und überwachbar war. Die Menge der für staatliche Zwecke verfügbaren Verbindungs- und Standortdaten hat sich von Jahr zu Jahr insgesamt drastisch erhöht:

Bis 1990 standen den Strafverfolgungsbehörden noch keinerlei Verkehrsdaten über Telekommunikationsverbindungen zur Verfügung, weil nach Takt abgerechnet wurde. Seit Einführung der digitalen Vermittlungsstellen Anfang der 90er Jahre hat die Verfügbarkeit von Verbindungsdaten beständig zugenommen. So fielen 1997 im Festnetz der Deutschen Telekom AG 54 Mrd. Verbindungsdatensätze an,³⁰ während dasselbe Unternehmen heute – trotz eingebrochenen Marktanteils – 120 Mrd. Verbindungsdatensätze pro Jahr verarbeitet.³¹ Laut Statistischem Bundesamt hat sich auch das gesamte Gesprächsvolumen in Fest- und Mobilfunknetzen von 2000 bis 2006 von Jahr zu Jahr erhöht³² und war 2010 so hoch wie noch nie.³³ Laut Eurostat ist dieser jährliche Anstieg schon seit Beginn der

²⁸ Vgl. BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 217.

²⁹ Bundesnetzagentur, Tätigkeitsbericht 2002/2003, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Presse/Berichte/2003/Taetigkeitsbericht2002_2003Id203pdf.pdf?__blob=publicationFile, 51.

³⁰ Welp, TKÜV, 3 (9).

³¹ AP-Meldung vom 02.06.2008, <http://www.pr-inside.com/de/milliarden-datensaetze-im-jahr-r619791.htm>.

³² Statistisches Bundesamt, Entwicklung der Informationsgesellschaft (2007), <http://www.destatis.de>, 51.

³³ Bundesnetzagentur, Tätigkeitsbericht 2010/2011 vom Dezember 2011, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Presse/Berichte/2011/TaetigkeitsberichtTK20102011pdf.pdf;jsessionid=4DD-D4A685A58781C4A40B234EA965540?__blob=publicationFile, 53.

Statistik im Jahr 1980 zu verzeichnen.³⁴ Einem Gesprächsvolumen von 1980 21 Mrd. Gesprächsminuten³⁵ standen 2008 306 Mrd. Gesprächsminuten³⁶ gegenüber. 3,6 Mrd. versandten Textnachrichten (SMS) im Jahr 1999 stehen 34 Mrd. versandten Textnachrichten im Jahr 2009 gegenüber.³⁷ 2002 korrespondierten 38% der Deutschen per E-Mail, 2010 bereits 73%.³⁸

Hinzu kommt die zunehmende Verlagerung alltäglicher Tätigkeiten in das staatlich überwachbare Internet. Dies gilt für die Kommunikation in sozialen und beruflichen Netzwerken, für den Einkauf, für das Lesen von Zeitungen und Nachrichtenmagazinen. Im Internet hören wir Radio oder sehen fern. Wir informieren uns in Online-Lexika und auf Behördenportalen, bilden uns aus und fort, suchen nach Arbeit, veröffentlichen eigene Inhalte im Internet, lesen oder verfassen Meinungsbeiträge über Bürgerangelegenheiten oder politische Themen auf Internetseiten. 11% der Deutschen nehmen an Beratungen oder Abstimmungen im Internet über Bürgerangelegenheiten oder politische Themen oder an Internet-Petitionen teil.³⁹ 54% beschaffen über das Internet gesundheitsrelevante Informationen.⁴⁰

Das von Kommunikationsdaten gezeichnete Bild unseres Verhaltens, in das der Staat Einblick nehmen kann, ist mithin so genau wie noch nie.

Der Staat nutzt diesen Informationsreichtum auch zunehmend aus. So ist die Zahl der Verkehrsdatenzugriffe durch deutsche Strafverfolgungsbehörden von ca. 5.000 im Jahr 2000⁴¹ auf 26.000 im Jahr 2015⁴² angestiegen. Neben der quantitativen Ausweitung hat die Nutzung von Kommunikationsdaten zu Strafverfolgungszwecken auch qualitativ zugenommen. Seit Einführung der Mobilfunktechnologie kann unschwer die Position von Personen laufend bestimmt werden. Seit dem 01.01.2008 ist schon unter den geringen Voraussetzungen des § 100g StPO eine Echtzeitüberwachung von Personen möglich. Zugleich erteilen immer mehr Telekommunikationsunternehmen die angeforderten Auskünfte in elektronischer Form über eine „Elektronische Behördenschnittstelle (ESB)“. Die Daten können dadurch von Seiten der Behörden in umfassende Analysensysteme („Information Warehouses“) eingespeist werden.

Selbst wenn also Prepaidkarten zu einer Abnahme der gespeicherten Kundendaten geführt hätten, würde dies jedenfalls um ein Vielfaches überkompensiert durch die Zunahme der insgesamt verfügbaren Verkehrsdaten, die zur Strafverfolgung auch ohne Identifizierungszwang zur Verfügung stehen. Ungeachtet der Verfügbarkeit von Kundendaten profitieren die Behörden unter dem Strich deutlich von den neuen Informationsquellen.

Die Bewertung eines Totalverbots anonymer vorausbezahlter Telekommunikationsanschlüsse kann sich im Übrigen nicht an überkommenen Vertragsgestaltungen der Telekommunikationsdiensteanbieter orientieren, sondern nur an dem Vergleich mit nicht elektronisch vermittelter Kommunikation, bei der keinerlei Erfassung menschlicher Kontakte oder Identitäten bei einem Kommunikationsmittler erfolgt.

(2) Rechtsvergleich

Rechtsvergleichend ist festzustellen, dass diverse andere Staaten – darunter unsere Nachbarländer Österreich, die Niederlande und Tschechien – eine allgemeine Identifizierungspflicht für Inhaber von Telekommunikationsan-

³⁴ Eurostat, Inlandsgespräche (T501).

³⁵ Eurostat, Inlandsgespräche (T501).

³⁶ Eurostat, Ausgehender Verkehr aller Netzwerke (T500).

³⁷ Eurostat, Anzahl der SMS (T510).

³⁸ Eurostat, Senden/Empfangen von E-Mails (I_IUEM).

³⁹ Eurostat, Teilnahme an Beratungen oder Abstimmungen im Internet über Bürgerangelegenheiten oder politische Themen (I_IUVOTE).

⁴⁰ Eurostat, Beschaffung von gesundheitsrelevanten Informationen (I_IHIF).

⁴¹ Max-Planck-Institut, BT-Drs. 16/7434, 50.

⁴² Bundesjustizamt, Übersicht Telekommunikationsüberwachung für 2015, https://www.bundesjustizamt.de/DE/SharedDocs/Publikationen/Justizstatistik/Uebersicht_Verkehrsdaten_2015.pdf?__blob=publicationFile&v=2.

schlüssen nicht für erforderlich halten. In diversen EU-Mitgliedsstaaten werden Straftaten also auch ohne allgemeinen Identifizierungszwang verfolgt, obwohl auch dort ein Großteil der Mobiltelefonanschlüsse vorausbezahlt werden (Estland: 61%, Finnland: 10%, Irland: 70%, Niederlande: 39%, Österreich: 32%, Portugal: 73%, Schweden: 38%, Slowenien: 32%, Tschechien: 51%, Vereinigtes Königreich: 59%, Lettland, Litauen, Kroatien).⁴³ Dass Straftaten in diesen Ländern weniger erfolgreich als in Deutschland verfolgt würden, ist nicht ersichtlich. Auch in Deutschland selbst hat der Staat seine Aufgaben bis 2004 ohne Identifizierungspflicht und bis 2017 ohne Ausweispflicht erfüllt.

Dass die Aufgabenerfüllung durch § 111 Abs. 1 S. 3 ff. TKG effektiviert worden wäre, ist nicht belegt oder sonst ersichtlich. Schon die am 26. Juni 2004 in Kraft getretene Grundnorm hat die Zahl aufgeklärter Straftaten in Deutschland nicht erkennbar gesteigert (2002: 3,4 Mio., 2003: 3,5 Mio., 2004: 3,6 Mio., 2005: 3,5 Mio., 2006: 3,5 Mio., 2007: 3,5 Mio., 2008: 3,4 Mio., 2009: 3,4 Mio., 2010: 3,3 Mio., 2011: 3,3 Mio., 2016: 3,6 Mio.).⁴⁴ Auch in anderen Staaten, die eine Identifizierungspflicht eingeführt haben, ist ein Anstieg nicht ersichtlich.

Das Bundesverfassungsgericht argumentiert, wegen der zunehmenden Internetnutzung – auch für Rechtsverletzungen – bestehe ein gesteigertes Interesse an der Möglichkeit, Kommunikationsverbindungen den jeweiligen Akteuren zuordnen zu können. In einem Rechtsstaat dürfe das Internet keinen rechtsfreien Raum bilden.⁴⁵ Dass das Internet auch ohne einen generellen und undifferenzierten Identifizierungszwang weit von einem rechtsfreien Raum entfernt ist, ergibt sich indes bereits daraus, dass diverse EU-Mitgliedsstaaten keinen Identifizierungszwang für Inhaber von Telekommunikations- und Internetanschlüssen kennen und man nicht ernsthaft behaupten kann, dass in diesen Nachbarstaaten das Internet ein rechtsfreier Raum wäre. Gleiches gilt für Deutschland bis vor kurzem. Es ist nicht einmal belegt, dass der Identifizierungszwang überhaupt eine statistisch nachweisbare Auswirkung auf Aufklärungsquote oder gar Kriminalitätsrate hätte.

(3) Umgehungsmöglichkeiten

Die Bundesrepublik meint, die deutsche Identifizierungspflicht führe zur Ermittlung, Feststellung oder Verfolgung von mehr Straftaten als es sonst der Fall wäre. Gegen diese Annahme spricht aber, dass Straftäter eine Identifizierung über die nach § 111 TKG zu erhebenden Daten weiterhin verhindern können.⁴⁶ Zwar können bei der Anmeldung wegen der Ausweispflicht keine Fantasieangaben zu Name, Anschrift und Geburtsdatum mehr gemacht werden. Möglich ist jedoch die Nutzung von Mobiltelefonkarten, die andere Personen registriert haben. Gegen ein „Zubrot“ werden auch unbekannte Strohmänner dazu bereit sein. Die anonyme Weitergabe bereits registrierter SIM-Karten (z.B. gegen Barzahlung) ist möglich, zulässig und verbreitet. Viele Händler bieten vorregistrierte Karten an. Ferner können unschwer ausländische unregistrierte SIM-Karten in Deutschland eingesetzt werden, zumal Roaming-Gebühren in der EU weitgehend abgeschafft sind. Eine weitere Möglichkeit dürfte darin liegen, dass Unternehmen oder Vereine (z.B. Parteien) eine Vielzahl von Prepaidkarten auf ihren Namen registrieren und sie ihren Angehörigen/Mitgliedern zur Nutzung überlassen (vgl. § 111 Abs. 1 S. 3 Nr. 7 TKG).

Die Folge von alledem ist, dass Straftäter auch nach Änderung des § 111 TKG Guthabekarten ohne Weiteres einsetzen können, ohne sich wahrheitsgemäß identifizieren zu müssen. Gerade bei ernsthaften und daher wirklich gefährlichen Kriminellen wäre es naiv, anzunehmen, dass diese durch die Identifizierungspflicht dazu bewegt werden

⁴³ OECD, Communications Outlook 2009, <https://dwmw.files.wordpress.com/2011/06/oecd-commoutlook-2011.pdf>, 164.

⁴⁴ Bundeskriminalamt, Polizeiliche Kriminalstatistik, Grundtabelle.

⁴⁵ BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 260.

⁴⁶ Vgl. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Entschließung vom 24.05.2002, <https://www.sachsen-anhalt.de/index.php?id=20322>; Schwedisches Justizministerium, Stellungnahme vom 16.11.2009, http://ec.europa.eu/dgs/home-affairs/what-is-new/public-consultation/2009/pdf/0008/contributions/member_states/reply_se_en.pdf, 4.

könnten, bei dem Kauf von Karten für ihr „Arbeitshandy“ brav ihre persönlichen Daten anzugeben. Die Identifizierungspflicht läuft damit faktisch leer⁴⁷ bzw. trifft im Wesentlichen nur ehrliche, rechtstreuere Bürger.⁴⁸

Das Bundeswirtschaftsministerium schilderte die Situation schon im Jahr 2002 wie folgt:

„Derzeit werden Prepaid-Karten von Straftätern häufig unter Angabe falscher bzw. fiktiver Personalien oder unter dem Namen der Vertriebspartner (Händler) erworben und registriert, oder es werden nicht existente Anschriften angegeben. [...] Sicherheitsbehörden sind oftmals damit konfrontiert, dass Straftäter bewusst und gezielt in kurzen Zeitabständen neue Prepaid-Karten erwerben, die Karte wechseln oder mehrere Prepaid-Karten parallel nutzen und diese teilweise von Telefonat zu Telefonat wechseln. [...] Gegenwärtig sind lediglich in Frankreich die Anbieter von Prepaid-Karten verpflichtet, Kundendaten zu erheben. Es kommt vor, dass trotz Vorgaben von Regierungsseite völlig unzutreffende Angaben gemacht werden. In den anderen EU-Staaten, aus denen Informationen vorliegen, gibt es keine gesetzlichen Regelungen, die bei dem Verkauf von Prepaid-Karten zu beachten sind. [...] Etwa 50 % der Karten werde innerhalb eines Jahres verschenkt, größtenteils innerhalb der Familie.“⁴⁹

Die Bundesnetzagentur berichtet auch 2011 noch:

„In der Praxis sind immer wieder Fälle zu verzeichnen, in denen der originäre Zuteilungsnehmer nicht in der Lage ist, der Bundesnetzagentur die personenbezogenen Daten von Zuteilungsnehmern zu nennen, die von ihm abgeleitete Rufnummernzuteilungen erhalten haben.

Betroffen sind in diesem Zusammenhang insbesondere nationale Teilnehmerrufnummern, die für VoIP-Dienste im Internet zugeteilt werden, Mobilfunkrufnummern von Prepaid-Kunden und Massenverkehrsrufnummern.

Das Unvermögen hat unterschiedliche Ursachen:

- *Die Daten wurden überhaupt nicht erhoben.*
- *Der abgeleitete Zuteilungsnehmer hat falsche Daten angegeben und die angegebenen Daten wurden vom originären Zuteilungsnehmer nicht in geeigneter Weise geprüft.*
- *Die Daten haben sich geändert und wurden vom originären Zuteilungsnehmer nicht aktuell gehalten.*

Beispielsweise kommt es vor, dass vor der Freischaltung von Mobilfunk-Prepaid-Karten entweder ungeprüfte Daten oder die Daten des Vertriebspartners erhoben und gespeichert werden, um dem Nutzer den direkten Gebrauch der Mobilfunkrufnummer zu Prepaid-Produkten zu ermöglichen.

[...] Darüber hinaus beklagen Sicherheits- und Strafverfolgungsbehörden immer wieder Defizite bei den Teilnehmerdaten, die sie bei Bedarf im automatisierten Verfahren nach § 112 TKG über die Bundesnetzagentur abrufen.“⁵⁰

Im Rahmen einer Studie im Auftrag des Bundesjustizministeriums im Jahr 2011 wurden Strafverfolgungsbeamte befragt und berichteten:

⁴⁷ Rannenberg, Identity management in mobile cellular networks and related applications von 2004, <http://www.web-portal-system.de/wps/wse/dl/down/open/rannenberg/f04fedba1e01ddee795db5ebd780739867943e-d5b5acf594d3434521796aff787032c8635283ab3c3fed7d349270beae/identitymanagementinmobilecell965.pdf>, 83.

⁴⁸ ICRI, Stellungnahme zur Vorratsdatenspeicherung, http://ec.europa.eu/dgs/home-affairs/what-is-new/public-consultation/2009/pdf/0008/contributions/fra/reply_icri_kuleuven_en.pdf, 8.

⁴⁹ BMWi-Ressortarbeitsgruppe, Eckpunkte zur Anpassung der Regelungen des § 90 TKG vom 28.03.2002, www.almeprom.de/fiff/material/Eckpunkte_90_TKG_Prepaid.pdf, 7.

⁵⁰ Bundesnetzagentur, Nummerierungskonzept 2011 vom 09.11.2011, https://www.bundesnetzagentur.de/Shared-Docs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/Nummernverwaltung/Nummerierungskonzept/Nummerierungskonzept2011pdf.pdf?__blob=publicationFile, 24.

„Die beim Kauf bzw. der Aktivierung einer Prepaid-Karte vorgesehene Angabe der Personalien werde oftmals entweder gar nicht verlangt oder die angegebenen Personalien würden nicht überprüft. Oft würden Nutzer Namen erfinden (dies seien häufig sogar leicht erkennbare Phantasienamen, wie sie auch in Internet-Foren verbreitet seien) oder die Namen unbeteiligter Dritter verwenden (Familie, Verwandte, Bekannte, Unbekannte). Einige Gesprächspartner berichten von Fällen, in denen solche Personen dann von weiteren, teilweise einschneidenden Maßnahmen wie Durchsuchungen betroffen waren. Insbesondere die Phantasienamen, zu deren Verwendung in manchen Internet-Foren aktiv aufgerufen werde, bereiteten zunehmend Probleme. Auch bei Prepaid-Karten, die über Tauschbörsen weitergereicht werden, seien die Bestandsdaten dann wertlos. Dasselbe gelte bei der Verwendung ausländischer Karten.“⁵¹

Ermittler der Zentralstelle zur Bekämpfung der Internetkriminalität der Generalstaatsanwaltschaft Frankfurt am Main berichten 2012, dass sie mit Bestandsdatenabfragen „in aller Regel nicht weiter“ kommen, weil Straftäter bei der Registrierung regelmäßig falsche Daten angeben.⁵²

Auch die Generalstaatsanwaltschaft München schreibt in einem internen „Leitfaden zum Datenzugriff“ vom Juni 2011:

„Häufig werden PrePaid-Karten verkauft, ohne Verifizierung der (wahren) Personalien des Erwerbers, da § 95 Abs. 4 TKG nur eine Kann-Vorschrift ist. Eine Bestandsdatenabfrage führt daher hier häufig nicht zum wahren Nutzer.“⁵³

Einer Studie der Bundesnetzagentur zufolge gaben mindestens 10 % aller Prepaid-Nutzer von vornherein falsche Personalien an;⁵⁴ hinzu kommen nachträglich weitergegebene Karten ohne Aktualisierung der Kundendaten. Insgesamt sind nach Angaben von Sicherheits- und Strafverfolgungsbehörden im Jahr 2011 trotz § 111 TKG – je nach Netzbetreiber – bis zu 40% der Mobilfunkrufnummern von Prepaid-Kunden nicht anhand von Kundendaten identifizierbar.⁵⁵ Es liegt auf der Hand, dass Straftäter in aller Regel zur Gruppe der nicht korrekt registrierten Kunden gehören. Selbst wenn § 111 TKG in neuer Fassung die Zahl der korrekt registrierten Karten erhöht, ist nichts dafür ersichtlich, dass dies gerade die Gruppe der Straftäter – und nicht nur der ehrlichen Bürger – betrifft.

(4) Fehlen eines empirischen Wirksamkeitsnachweises

Zwar ist im Ausgangspunkt nicht zu bestreiten, dass die Aufklärung einer Straftat im Einzelfall von der Verfügbarkeit von Bestandsdaten abhängen kann. Auch hat die Bundesregierung einzelne Ermittlungsverfahren angeführt, in denen Bestandsdatenabfragen zur Aufklärung einer Straftat oder Abwehr einer Gefahr geführt haben. Jedoch sagt all dies nichts darüber aus, ob der Identifizierungszwang des § 111 TKG die Zahl der aufgeklärten Straftaten oder abgewehrten Gefahren tatsächlich erhöht oder nicht.

Die Argumentation der Bundesregierung leidet darunter, dass Einzelfallbeispiele, eine „langjährige Praxis“ und eine „bewährte Regelung“ allesamt keine belastbare Grundlage sind, um einen möglichen Zusatznutzen des § 111 TKG festzustellen, soweit sie über die Bereitstellung ohnehin anfallender Bestandsdaten zur Verfolgung schwerer Straftaten hinaus gehen. Zur Rechtfertigung der Identifizierungspflicht des § 111 TKG taugen Fallbeispiele im Übrigen schon deswegen nicht, weil sie keinerlei Bezug zu dieser Regelung aufweisen. Es ist nicht dargelegt, dass Erfolge erst durch die Identifizierungs- und Vorratsspeicherungspflicht des § 111 TKG erzielt werden konnten.

⁵¹ Max-Planck-Institut für ausländisches und internationales Strafrecht, Schutzlücken durch Wegfall der Vorratsdatenspeicherung? vom Juli 2011, <http://www.mpg.de/5000721/vorratsdatenspeicherung.pdf>, 168.

⁵² Arbeitskreis Vorratsdatenspeicherung, Meinungs austausch mit Strafverfolgern zur Vorratsdatenspeicherung vom 22.04.2012, <http://www.vorratsdatenspeicherung.de/content/view/579/55/lang,de/>.

⁵³ Generalstaatsanwaltschaft München vom Juni 2011, <http://cryptome.org/isp-spy/munich-spy-all.pdf>, 19.

⁵⁴ Max-Planck-Institut für ausländisches und internationales Strafrecht, Schutzlücken durch Wegfall der Vorratsdatenspeicherung? vom Juli 2011, <http://www.mpg.de/5000721/vorratsdatenspeicherung.pdf>, 168.

⁵⁵ Bundesnetzagentur vom 09.11.2011, <http://www.webcitation.org/69997Nqk8>, 14.

(5) Alternativen

Für Zwecke der Abrechnung erheben die Anbieter ohnehin meist Daten, welche eine Identifizierung des Inhabers ermöglichen. Die in § 111 Abs. 1 TKG erfassten Daten werden zu einem überwiegenden Teil von den Diensteanbietern zur Abwicklung ihrer Vertragsverhältnisse gemäß § 95 TKG ohnehin gespeichert.⁵⁶ Die meisten Ermittlungserfolge wegen Bestandsdaten beruhen daher nicht spezifisch auf der allgemeinen und unterschiedslosen Identifizierungspflicht des § 111 TKG, sondern wären auch ohne diese erzielt worden.

Wo korrekte Kundendaten nicht verfügbar sind, kann die Aufklärung einer Straftat auf anderem Wege möglich sein. Ein Ermittlungsansatz kann sein, über die Aufladevorgänge der Prepaid-Karten zu ermitteln, wer diese vornimmt.⁵⁷ Die Provider/Netzbetreiber verfügen über Daten, wo bzw. an welchen Terminals die Aufladung erfolgte. Falls eine Bezahlung über EC-Karte erfolgte, können die Bankverbindungen im weiteren Verlauf festgestellt werden. Falls die Aufladung bar bezahlt wurde, können eventuell Ermittlungen über installierte Videokameras (z.B. bei Tankstellen) weiterführen. Im Fall erheblicher Straftaten können Nutzer unregistrierter Anschlüsse auch mithilfe von Funkzellendaten oder eines sogenannten IMSI-Catchers lokalisiert und identifiziert werden (§ 100i StPO).⁵⁸ Eine Identifizierung kann teilweise auch über die Kennung des genutzten Endgeräts (IMEI) erfolgen, wenn dessen Kauf nachvollziehbar ist, oder über die Rufnummern der Gesprächspartner der Zielperson (Kommunikationsprofil).⁵⁹ Schließlich ist in vielen Strafverfahren die Anschlusskennung nur ein Ermittlungsansatz unter vielen und kann der Beschuldigte über Spuren ohne Telekommunikationsbezug identifiziert werden. Nach einer Untersuchung von Verkehrsdatenabfragen durch das Max-Planck-Institut werden ein Drittel der Straftaten, in denen eine Verkehrsdatenabfrage erfolglos blieb, gleichwohl auf anderem Wege aufgeklärt.⁶⁰

Das britische „Mobile Crime Industry Action Forum“ sieht in Anbetracht dieser Identifizierungsmöglichkeiten in dem Angebot unregistrierter Anschlüsse sogar einen taktischen Vorteil für Strafverfolger: Vermeintlich anonyme SIM-Karten wägen Straftäter in Sicherheit, veranlassten diese zum Einsatz unregistrierter Karten und erlaubten dadurch deren Aufgreifen, wo es andernfalls nicht möglich gewesen wäre.⁶¹ Ein europäischer Beamter im Bereich der Terrorismusbekämpfung hat angegeben, eine anonyme Mobiltelefonkarte sei „eines der effektivsten Mittel zur Lokalisierung von Al-Kaida“ gewesen. „Die vermeintliche Anonymität kann sie in einem falschen Gefühl von Sicherheit gewogen haben.“⁶²

Inzwischen ist das Protokoll eines Treffens der EU-Mitgliedsstaaten am 04.05.2010 bekannt geworden,⁶³ demzufolge eine Reihe von Staaten eine Registrierungspflicht ablehnte. Es heißt in dem Protokoll:

Apart from opportunity crime that could be triggered by this registration, police avails of other techniques to establish the ID of anonymous users. It would also lead to public resentment. Besides, it would be easy to bypass any obligation which would annul the positive effect of that legislation. Some conceded that the only useful level of regulation would be at EU level.

⁵⁶ BVerfG, 1 BvR 1299/05 vom 24.1.2012, Abs. 135.

⁵⁷ Generalstaatsanwaltschaft München vom Juni 2011, <http://cryptome.org/isp-spy/munich-spy-all.pdf>, 19.

⁵⁸ Vgl. Europäische Kommission, Room Document, <http://www.vorratsdatenspeicherung.de/images/RoomDocumentEvaluationDirective200624EC.pdf>, 11.

⁵⁹ Schwedisches Justizministerium, Stellungnahme vom 16.11.2009, http://ec.europa.eu/dgs/home-affairs/what-is-new/public-consultation/2009/pdf/0008/contributions/member_states/reply_se_en.pdf, 4.

⁶⁰ Starostik, http://www.vorratsdatenspeicherung.de/images/schriftsatz_2008-03-17.pdf#page=2, 2.

⁶¹ Vgl. Gow, Comments submitted to Australian Communications and Media Authority vom März 2006, http://www.acma.gov.au/webwr/_assets/main/lib100696/dr%20gordon%20gow.pdf, 10.

⁶² Van Natta/Butler, How Tiny Swiss Cellphone Chips Helped Track Global Terror Web, <http://cryptome.org/ch-spy-chip.htm>.

⁶³ http://wiki.vorratsdatenspeicherung.de/images/2010.05.04_report_meeting_w_MS_12_March_2010.pdf.

In ihrem Bewertungsbericht zur Richtlinie über die Vorratsdatenspeicherung vom 18.4.2011⁶⁴ schrieb die EU-Kommission:

Six Member States (Denmark, Spain, Italy, Greece, Slovakia and Bulgaria) have adopted measures requiring the registration of prepaid SIM cards. These and other Member States (Poland, Cyprus, Lithuania) have argued in favour of an EU-wide measure for mandatory registration of the identify of users of prepaid services. No evidence has been provided as to the effectiveness of those national measures. Potential limitations have been highlighted, for example, in cases of identity theft or where a SIM card is purchased by a third party or a user roams with a card purchased in a third country. Overall the Commission is not convinced of the need for action in this area at an EU level at this stage.

Im Übrigen scheitert die Aufklärung einer Straftat oft trotz Verfügbarkeit korrekter Kundendaten. Mithilfe von Kundendaten lässt sich nur feststellen, auf wessen Namen ein Anschluss registriert ist. Wer ihn zu einem konkreten Zeitpunkt jedoch genutzt hat, ergibt sich daraus nicht. Nach einer Untersuchung von Verkehrsdatenabfragen durch das Max-Planck-Institut werden 72% der strafrechtlichen Ermittlungsverfahren, in denen Kommunikationsdatenabfragen erfolgreich waren, gleichwohl letztlich eingestellt.⁶⁵

(6) Zwischenergebnis

Insgesamt ist nicht belegt, dass ein Teil der strafrechtlichen Verurteilungen in Deutschland gerade auf § 111 Abs. 1 S. 3 ff. TKG zurückzuführen sein könnte. Alleine die Verfügbarkeit zusätzlicher Daten lässt auf einen effektiven Mehrwert für Zwecke der Strafverfolgung usw. nicht schließen.⁶⁶ Die Bundesrepublik hat es unterlassen, eine unabhängige wissenschaftliche Untersuchung über die Frage in Auftrag zu geben, ob § 111 Abs. 1 S. 3 ff. TKG den Rechtsgüterschutz fördert, ob also durch die Norm etwa weniger Straftaten begangen oder mehr Straftaten aufgeklärt würden als ohne die Vorschrift. Aufgrund der grundsätzlichen Freiheitsvermutung⁶⁷ gehen daraus resultierende Zweifel zulasten des eingreifenden Staates. Auch die EU-Kommission stellt fest: „Bislang wurden keine Nachweise für die Wirksamkeit der einzelstaatlichen Maßnahmen vorgelegt.“⁶⁸ Wissenschaftler bestätigen das Fehlen empirischer Wirksamkeitsnachweise.⁶⁹

Vor diesem Hintergrund lässt sich nicht vertretbarerweise behaupten, dass die Ausweispflicht einen nennenswerten Zusatzbeitrag zur Bekämpfung ernsthafter Kriminalität leiste. Selbst in Bezug auf Unbedarfte, also im Bereich von Kleinkriminalität und Ordnungswidrigkeiten, ist ein Nutzen nicht belegt.

Wenn die Bundesrepublik die angebliche Bedeutung des § 111 TKG hochstilisiert, vergisst sie zu erwähnen, dass die Behörden bis vor wenigen Jahren stets ohne globale und pauschale Identifizierungspflicht ausgekommen sind und in den allermeisten ausländischen Staaten noch immer auskommen. Die Norm ist für staatliche Zwecke entbehrlich; auch ohne sie war und ist eine effektive Strafverfolgung und sonstige staatliche Aufgabenwahrnehmung möglich. Dementsprechend sieht auch die EU-Kommission keinen Bedarf für einen Identifizierungszwang.⁷⁰

In Sachen S. und Marper ist der Europäische Menschenrechtsgerichtshof zutreffend der Behauptung der britischen Regierung entgegen getreten, die damals angefochtene biometrische Vorratsspeicherung sei „unabdingbar“ zur

⁶⁴ COM(2011) 225 final.

⁶⁵ Starostik, http://www.vorratsdatenspeicherung.de/images/schriftsatz_2008-03-17.pdf#page=2, 2.

⁶⁶ Vgl. EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 116.

⁶⁷ Vgl. BVerfGE 6, 55 (72); BVerfGE 32, 54 (72); BVerfGE 55, 159 (165).

⁶⁸ Europäische Kommission, KOM(2011) 225 vom 18.04.2011, http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_de.pdf, 32.

⁶⁹ Jentzsch, Implications of Mandatory Registration of Mobile Phone Users in Africa von 2012, https://www.diw.de/documents/publikationen/73/diw_01.c.394079.de/dp1192.pdf, 20; Centre for Policy Research on Science and Technology of Simon Fraser University Vancouver, Privacy Rights and Prepaid Communications Services vom März 2006, <https://www.sfu.ca/cprost-old/docs/GowPrivacyRightsPrepaidCommServices.pdf>, 18.

⁷⁰ Europäische Kommission, KOM(2011) 225 vom 18.04.2011, http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_de.pdf, 32.

Verfolgung von Straftaten.⁷¹ Dieser Behauptung hat der Gerichtshof erstens entgegen gehalten, dass England die Maßnahme selbst erst 2001 eingeführt habe.⁷² Zweitens hat er darauf hingewiesen, dass die Strafverfolgungsbehörden anderer Staaten auch ohne eine solche Maßnahme auskommen.⁷³

Nichts anderes gilt auch für das deutsche Anonymitätsverbot. Als § 111 TKG im Jahr 2004 beschlossen wurde, wurden Mobilfunkkarten anonym verkauft. Bis 2017 war eine Registrierung auf Fantasienamen möglich. Die Strafverfolgungsbehörden vieler anderer demokratischer Staaten kommen bis heute ohne eine vergleichbare Maßnahme aus und leisten gleichwohl eine wirksame Strafverfolgung.

bb) Das Gewicht des mit § 111 Abs. 1 S. 3 ff. TKG verbundenen Grundrechtseingriffs

Um die gebotene Abwägung vornehmen zu können, ist dem vermeintlichen öffentlichen Interesse an § 111 Abs. 1 S. 3 ff. TKG das Gewicht des damit verbundenen Grundrechtseingriffs gegenüberzustellen.

Das Gewicht eines Grundrechtseingriffs bemisst sich danach, unter welchen Voraussetzungen Eingriffe zulässig sind, welche und wie viele Grundrechtsträger von ihnen betroffen sind und wie intensiv die Grundrechtsträger beeinträchtigt werden.⁷⁴ Zu berücksichtigen ist auch, ob und in welcher Zahl Personen mitbetroffen werden, die für den Eingriff keinen Anlass gegeben haben.⁷⁵ Die Eingriffsintensität hängt bei Informationseingriffen unter anderem von Art, Umfang und denkbarer Verwendungen der erhobenen Daten sowie von der Gefahr ihres Missbrauchs ab.⁷⁶ 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.⁷⁷ Bei der Gewichtung möglicher Nachteile ist die Nutzbarkeit und Verwendungsmöglichkeit der Daten maßgeblich, und zwar unter besonderer Berücksichtigung der Möglichkeit, dass die Daten mit anderen Daten kombiniert und dadurch weitergehende Kenntnisse gewonnen werden können.⁷⁸

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. Nicht nur die wiederholt vorgenommene Ausweitung des Straftatenkatalogs in § 100a StPO zeigt, dass eine solche Entwicklung auch in anderen Bereichen möglich und nicht unwahrscheinlich ist. Zum anderen ist auch an die Gefahr eines rechtswidrigen Missbrauchs zu denken, gerade dort, wo dieser nur schwer zu bemerken ist. Zwar ist, was den Staat selbst angeht, die bloß abstrakte Möglichkeit eines Missbrauchs, 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“.⁷⁹ Eine reale Missbrauchsgefahr ist im Rahmen der Abwägung demgegenüber durchaus zu berücksichtigen.⁸⁰ Die Menschenrechte schützen den Einzelnen nämlich auch „vor fehlerhafter, missbräuchlicher oder exzessiver Verwertung von Kommunikationsdaten durch [...] staatliche Stellen“.⁸¹ Die „in der Gesprächsbeobachtung liegende Gefahr einer Menschenrechtsverletzung der [...] Gesprächsteilnehmer wie auch die

⁷¹ EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 115.

⁷² EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 115.

⁷³ EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 112.

⁷⁴ Vgl. BVerfGE 109, 279 (353).

⁷⁵ Vgl. BVerfGE 109, 279 (353).

⁷⁶ Vgl. BVerfGE 65, 1 (46).

⁷⁷ Vgl. BVerfGE 100, 313 (376).

⁷⁸ Vgl. BVerfGE 65, 1 (45).

⁷⁹ Vgl. BVerfGE 30, 1 (27).

⁸⁰ Vgl. BVerfGE 65, 1 (45 f.).

⁸¹ Vgl. BVerfGE 85, 386 (397).

Gefahr der Sammlung, Verwertung und Weitergabe der Informationen zu anderen Zwecken“ als den gesetzlich vorgesehenen darf daher nicht aus den Augen verloren werden.⁸² Wenn das Grundgesetz das unbefangene Gebrauchmachen von Freiheiten schützen soll, dann darf außerdem nicht unberücksichtigt bleiben, dass sich Bürger bei ihren Entscheidungen weniger durch die Gesetzesformulierungen leiten lassen als vielmehr durch Eindrücke, Emotionen und Befürchtungen. Dementsprechend kommt es im Rahmen der Abwägung auch nicht nur darauf an, welche Nachteile den Betroffenen konkret aufgrund der Überwachungsmaßnahmen drohen. Ebenso zu berücksichtigen sind entferntere Risiken, deren Eintritt von den Bürgern nicht ohne Grund befürchtet wird.⁸³ 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.

Die Anwendung dieser Grundsätze auf § 111 Abs. 1 S. 3 ff. TKG ergibt: Zur Identifizierung von Kommunikationsteilnehmern und Verifizierung der Angaben werden Anbieter frei von jeder Voraussetzung und Eingriffsschwelle dauerhaft und allgemein – mithin global und pauschal⁸⁴ – verpflichtet. Es erfolgt eine flächendeckende Massenerfassung⁸⁵ der Identität unbescholtener und ungefährlicher Inhaber von Telekommunikationsanschlüssen. Beeinträchtigt sind sämtliche Grundrechtsträger, die einen vorausbezahlten Mobiltelefonanschluss unterhalten, und damit ein Großteil der Bevölkerung. Für den rechtstreuen Normalbürger gibt es praktisch keine Möglichkeit mehr, Ferngespräche anonym anzunehmen bzw. anonym für Anrufe erreichbar zu sein. Auch eine anonyme mobile Internetnutzung über private Anschlüsse wird unmöglich.

Von dem Anonymitätsverbot ist der Bürger selbst dann betroffen, wenn er keinerlei Anlass zur Erfassung seiner Identität gegeben hat. Fast durchgängig betrifft der Eingriff Personen, von denen keine Gefahr ausgeht und die keiner Straftat schuldig sind.⁸⁶ Die Aufzeichnung und Verifikation der Identität Unschuldiger ist aber von vornherein überflüssig. Die Ermächtigung setzt keine Verantwortlichkeit oder wenigstens Gefahrennähe der Betroffenen voraus. Die bloße Unterhaltung eines Telekommunikationsanschlusses soll zur Identifizierung führen. § 111 Abs. 1 TKG macht insoweit den Grundsatz der Privatheit des Telekommunikationsverhältnisses bedeutungslos. Die Vorschrift ist nicht auf eine Erfassung „im Einzelfall“ bei Vorliegen einer konkreten Störung beschränkt, sondern gebietet eine anlasslose, globale, pauschale und vorsorgliche Identifizierung aller Telekommunikationsteilnehmer und Internetnutzer.

Zwar gibt es vielfältige Möglichkeiten einer anonymen Telekommunikation und Internetnutzung, welche die Herstellung eines Personenbezugs erschweren oder verhindern können 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. Eine auf anderen Namen registrierte Mobiltelefonkarte zu nutzen, zieht verschiedene Risiken und Nachteile nach sich, selbst wo Normalbürger dazu bereit sind: Mit der Nutzung eines vorausbezahlten Dienstes schließt man einen Vertrag mit dem Telekommunikationsunternehmen ab, der regelmäßig zur Angabe korrekter Personalien verpflichtet. Stellt der Anbieter fest, dass die angegebenen Daten falsch sind, kann dies dazu führen, dass man infolge einer Deaktivierung plötzlich nicht mehr anrufen und angerufen werden kann. Die unzutreffenden Angaben können auch dazu führen, dass man sich nicht an den Anbieter wenden kann, um Kundendienstleistungen in Anspruch zu nehmen oder Probleme beheben zu lassen.

Die verbleibenden Möglichkeiten anonymer Telekommunikation bewirken wegen der damit verbundenen Probleme für den Normalbürger insgesamt daher nur eine geringfügige Minderung der Eingriffsintensität.

⁸² Vgl. BVerfGE 85, 386 (400).

⁸³ Vgl. BVerfGE 100, 313 (376).

⁸⁴ Vgl. BVerfGE 313, 100 (376 und 383).

⁸⁵ Vgl. dazu BVerfGE 313, 100 (377).

⁸⁶ Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Entschließung vom 24.05.2002, <https://www.sachsen-anhalt.de/index.php?id=20322>.

Das Gewicht des Eingriffs vergrößert sich ferner durch die ausufernden gesetzlichen Zugriffsrechte (§§ 112, 113 TKG), zu denen ein zivilrechtlicher Auskunftsanspruch wegen Urheberrechtsverletzungen hinzu tritt (§ 101 UrhG).

(1) Das gesellschaftliche Interesse an Anonymität

Um die Frage beantworten zu können, ob ein derart weitreichender Eingriff in einer demokratischen Gesellschaft erforderlich sein kann, muss untersucht werden, welche Bedeutung Anonymität in einer demokratischen Gesellschaft zukommt.

Gary Marx unterscheidet 15 Funktionen von Anonymität in unserer Gesellschaft:⁸⁷

1. Erleichterung des Informations- und Kommunikationsflusses über öffentliche Angelegenheiten durch Schutz des Informationsgebers (z.B. Hotlines zur anonymen Anzeige von Problemen oder Verstößen durch Whistle Blower, anonyme Informanten der Presse);
2. Ermöglichung der wissenschaftlichen Erforschung von Sachverhalten, über die nur im Schutz der Anonymität Auskunft gegeben wird (z.B. Telefonstudien über Sexualverhalten, über strafbares Verhalten, über die Gesundheit);
3. Sicherzustellen, dass nicht die Offenlegung des Urhebers einer Nachricht oder Meinung die Wahrnehmung ihres Inhalts verhindert oder beeinflusst (z.B. wegen Vorurteilen gegen den Autor);
4. Förderung des Meldens, Informierens, Kommunizierens, Austauschs und der Selbsthilfe im Hinblick auf Zustände oder Handlungen, die stigmatisieren, nachteilig oder intim sind (z.B. Hilfe für und Austausch der Betroffenen von Drogenmissbrauch, Gewalt in der Familie, abweichender sexueller Identität, psychischer oder physischer Krankheiten, AIDS oder anderer Sexualkrankheiten, Schwangerschaft; Kauf von Verhütungsmitteln, Medikamenten oder bestimmten Magazinen);
5. Ermöglichung von Hilfe trotz Strafbarkeit oder gesellschaftlicher Verachtung (z.B. anonyme Beratung von Drogenabhängigen, anwaltliche Beratung von Beschuldigten);
6. Schutz der Unterstützer unbeliebter Handlungen vor Verpflichtungen, Forderungen, Vorverurteilung, Verwicklungen oder Rache (z.B. Schutz der Identität verdeckter Ermittler oder von Polizist/innen oder von Menschenrechtsorganisationen);
7. Wahrnehmung wirtschaftlicher Interessen durch Einschaltung von Mittelsmännern/-frauen, um zu vermeiden, dass Hintergründe einer geschäftlichen Transaktion bekannt werden (z.B. anonyme Testkäufe, anonyme Versteigerungen);
8. Schutz der eigenen Zeit, des eigenen Raums und der eigenen Person vor unerwünschtem Eindringen (z.B. durch Stalker, Fans oder Werbetreibende);
9. Sicherzustellen, dass Entscheidungen ohne Ansehung der Person getroffen werden (z.B. anonyme Bewerbung);
10. Schutz der eigenen Reputation und Ressourcen vor Identitätsdiebstahl (Handeln anderer unter dem eigenen Namen);
11. Verfolgten Personen die sichere Teilnahme am öffentlichen Leben zu ermöglichen (z.B. sich illegal aufhaltende Flüchtlinge);
12. Durchführung von Ritualen, Spielen und Feiern, welche das Verbergen der eigenen Identität oder das Annehmen einer fremden Identität zum Gegenstand haben und denen eine förderliche Wirkung auf die Persönlichkeitsentwicklung und psychische Gesundheit zugeschrieben wird (z.B. Rollenspiele);
13. Förderung des Experimentierens und Eingehens von Risiken ohne Furcht vor Konsequenzen, Scheitern oder Gesichtverlust (z.B. Auftreten unter dem anderen Geschlecht in einem Chatroom);
14. Schutz der eigenen Persönlichkeit, weil die eigene Identität andere schlichtweg nichts angeht;

⁸⁷ Marx, What's in a Name? Some Reflections on the Sociology of Anonymity (1999), <http://web.mit.edu/gtmarx/www/anon.html>.

15. Erfüllung traditioneller Erwartungen (z.B. die traditionelle Möglichkeit, anonym Briefe schreiben zu können).

Es zeigt sich, dass in vielen Bereichen unserer Gesellschaft ein legitimes oder sogar dringendes Interesse daran besteht, anonym handeln zu können. Anonymität ist vielfach Freiheitsvoraussetzung. In vielen Situationen sind Menschen nur im Schutz der Anonymität bereit, von ihren grundrechtlich geschützten Freiheiten Gebrauch zu machen. Informationen und Meinungen werden oftmals nur im Schutz der Anonymität ausgetauscht oder veröffentlicht. An Demonstrationen und politischen Aktionen nehmen Menschen vielfach nur teil, wenn Anonymität sie vor drohenden oder befürchteten Nachteilen schützt. Wer damit rechnet, dass seine Teilnahme an einer Versammlung oder einer Bürgerinitiative namentlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte verzichten. Wer damit rechnen muss, dass „abweichende“ oder „ungewöhnliche“ Verhaltensweisen Nachteile nach sich ziehen können, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Dies beeinträchtigt nicht nur die individuellen Entfaltungschancen des Einzelnen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.⁸⁸

(2) Das gesellschaftliche Interesse an anonymen Telekommunikations- und Internetanschlüssen

Die Möglichkeit, sich über anonyme Telekommunikations- und Internetanschlüsse informieren und darüber kommunizieren zu können, ist für viele Menschen äußerst wichtig:

- Menschen halten ihre Privatnummern geheim, um sich vor unerwünschten Anrufen oder Nachrichten zu schützen (z.B. Werbung, Stalking, Bedrohung, sexuelle Belästigung), aber auch vor unerwünschten Besuchen, denn aus der Vorwahl von Festnetzanschlüssen kann man auf den privaten Wohnort schließen. Prominente haben ein besonderes Interesse an der Geheimhaltung ihrer Privatnummern.
- Menschen halten ihre Privatnummer geheim, um sich vor Abhören ihrer Kommunikation zu schützen, beispielsweise durch Geheimdienste, aber auch durch unbefugte Privatpersonen (z.B. „phone hacking“ durch Journalisten).
- Menschen halten ihre Privatnummer geheim, um sich vor Identitätsdiebstahl zu schützen. Es ist möglich, eine Fernkommunikation als von einer fremden Kennung ausgehend erscheinen zu lassen (z.B. gefälschte SMS-Absendernummer, gefälschte E-Mail-Absenderadresse, IP-Spoofing) und sich dadurch als eine andere Person auszugeben. Der Betroffene muss sich für die Handlung dann zunächst einmal verantworten.
- Menschen in besonderen Situationen (z.B. Notlagen, Krankheiten, Sucht) sind aus Furcht vor Stigmatisierung oder sonstigen Nachteilen oft nur in vollständiger Anonymität bereit, Informationen und Hilfe zu suchen, sich untereinander auszutauschen und sich beraten zu lassen (z.B. Chatrooms für Opfer sexuellen Missbrauchs).
- Unternehmen telekommunizieren anonym, um Wirtschaftsspionage im Zusammenhang mit Vertragsverhandlungen zu verhindern, aber auch um sich selbst bei Wettbewerbern zu informieren, ohne ihre Identität preisgeben zu müssen.
- Regierungsbehörden (z.B. Nachrichtendienste) kommunizieren anonym, um im Internet recherchieren zu können, ohne als Regierungsbehörde identifizierbar zu sein. Zugleich sind sie darauf angewiesen, dass Menschen Straftaten anonym anzeigen können, die andernfalls nicht gemeldet würden und unaufgeklärt blieben. Dies gilt für die anonyme Offenlegung verschiedenster Missstände wie Steuerhinterziehung oder Korruption (sogenanntes „Whistleblowing“).
- Nur anonyme Telekommunikation erlaubt es der Bevölkerung autoritärer Staaten, sich über politische Nachrichten zu informieren, die in ihrem eigenen Land durch Zensurmaßnahmen gesperrt sind.
- Journalisten, die in autoritären Staaten arbeiten, sind auf anonyme Fernkommunikation angewiesen, um Informationen sicher empfangen und nach Deutschland übermitteln zu können, ohne dass der Aufenthaltsstaat dies zum Anlass für Maßnahmen gegen sie nehmen kann. Auch im Inland sind Informanten zunehmend nur noch im Schutz der

⁸⁸ BVerfGE 65, 1 (43).

Anonymität bereit, Auskunft zu geben. Im Wege anonymer Kommunikation gelingt es dann nicht selten, gravierende Missstände an das Licht der Öffentlichkeit zu bringen.

- Menschenrechtsgruppen brauchen anonyme Kommunikationstechnik für ihre Arbeit mit autoritären ausländischen Staaten, sei es, um von diesen Staaten aus unerkannt mit ihrem Heimatbüro zu kommunizieren, sei es, um unerkannt mit oppositionellen Gruppen in den entsprechenden Staaten in Verbindung zu treten. Eine offene Kommunikation ist hier regelmäßig mit einem nicht zu verantwortenden Sicherheitsrisiko für die Beteiligten verbunden.
- Regierungskritiker, Blogger, Journalisten und Oppositionelle in autoritären ausländischen Staaten (z.B. Iran, Burma, Tibet), die sich für demokratische Reformen in ihrem Land einsetzen, können nur mithilfe anonymer Netze untereinander kommunizieren und die Öffentlichkeit auf die Situation in ihrem Land aufmerksam machen. Ohne den Schutz der Anonymität sind sie Verhaftungen, Gefängnisstrafen und Folter ausgesetzt; anonyme Fernkommunikation schützt also Leben und Freiheit dieser Personen. Beispielsweise in Burma ist die demokratische Opposition auf die anonyme Kommunikation per Internet angewiesen gewesen.

In all diesen Situationen kann eine freie, unbefangene und im allem vertrauliche Kommunikation nur im Schutz der Anonymität erfolgen.

Anonyme Fernkommunikation ist heutzutage vielfach Freiheitsvoraussetzung. In vielen Situationen sind Menschen nur im Schutz anonymer Kommunikationskanäle bereit, von ihren grundrechtlich geschützten Freiheiten Gebrauch zu machen. Wer eine politische Demonstration vorbereitet oder gegenüber der Presse vertraulich Missstände aufdecken will, hat ein berechtigtes Interesse an der Nutzung einer anonymen Mobiltelefonkarte. Die Meinungs- und Versammlungsfreiheit ist gefährdet, wo Organisatoren staatskritischer Demonstrationen (z.B. gegen die Globalisierung, gegen Atomkraft oder gegen soziale Probleme) aus Furcht vor staatlichen Repressalien auf die Benutzung von Telekommunikation zur Koordinierung ihrer Aktivitäten verzichten. Die Pressefreiheit ist gefährdet, wo Informanten aus Furcht vor staatlicher Strafverfolgung nicht mehr zur Aufdeckung staatlicher Missstände per Telekommunikation bereit sind. Die Möglichkeit vertraulicher Kommunikation – und zwar auch gegenüber dem Staat vertraulicher Kommunikation – ist in vielen Bereichen konstitutiv für unsere demokratische Gesellschaft.

Der generelle Identifizierungs- und Verifizierungszwang des § 111 TKG führt dazu, dass eine anonyme Kommunikation kaum noch möglich ist und man sich stets der Nachvollziehbarkeit von Telekommunikation bewusst sein muss. Hierzu genügt es, dass die eigene Rufnummer, E-Mail-Adresse oder IP-Adresse bekannt oder gespeichert wird. Durch diese Nachvollziehbarkeit sinkt die Bereitschaft zur Nutzung der Telekommunikation in bestimmten Situationen erheblich. Wer etwa kritische Meinungsäußerungen gegenüber dem Staat oder die Übermittlung staatsbezogener Informationen an die Presse plant, kann sich heute im Grunde nicht mehr seines Telefons oder Mobiltelefons bedienen, ohne Konsequenzen befürchten zu müssen. Will man das Risiko von (auch unberechtigten) Ermittlungsmaßnahmen vermeiden, muss man auf die Post oder den unmittelbaren Kontakt ausweichen oder auf die Kommunikation überhaupt verzichten. Regierungskritische Organisationen sowie der Presse setzen das Medium der Telekommunikation in solchen Situationen teilweise tatsächlich nicht mehr ein.

Wo die Telekommunikation als Medium anonymer Kommunikation ausfällt, stehen allerdings oft keine praktikablen Alternativen zur Verfügung mit der Folge, dass auf den Informationsaustausch insgesamt verzichtet wird. Dies fügt nicht nur den Betroffenen, sondern auch unserem Gemeinwesen insgesamt schweren Schaden zu. 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.

Auch auf die Internetnutzung sind viele Menschen und Berufsgruppen angewiesen, ohne zumutbarerweise auf andere Informations- und Kommunikationskanäle ausweichen zu können. Das Internet ermöglicht gerade 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.

Für Menschen mit bestimmten Behinderungen kann das Internet überhaupt die einzige Kommunikations- und Informationsmöglichkeit nach außen darstellen. So schrieb eine Person dem Arbeitskreis Vorratsdatenspeicherung nach Inkrafttreten des entsprechenden Gesetzes:

„sitze im rolli und kann nur die rechte hand bewegen. sprechen kann ich auch nicht. internet und sms sind die einzigen möglichkeiten zur kommunikation, die ich habe. die vorstellung, daß jedes wort von mir gespeichert wird, wirkt sowas von abschreckend und... frustrierend auf mich. kein mensch, keine sache, hat durch mich irgendeinen schaden zu befürchten... ich möchte nur in ruhe und unbeobachtet mein ohnehin sehr eingeschränktes leben leben...“

(a) Aussagekraft von Teilnehmerregistern

Die nach § 111 TKG zu erhebenden und staatlichen Stellen zum automatisierten Abruf zur Verfügung zu stellenden (§ 112 TKG) Personendaten sind schon bei isolierter Betrachtung sensibel: In Anbetracht des Verbreitungsgrads von Telekommunikations- und Internetanschlüssen bewirkt § 111 TKG die Erstellung eines recht vollständigen Einwohnerverzeichnisses. Die in § 112 TKG vorgesehenen Suchfunktionen erlauben es Behörden, eine Liste aller Anschlussinhaber in einer Straße oder einem Wohnhaus anzeigen zu lassen. Name und Wohnanschrift einer Person können Rückschlüsse auf ihre Identität zulassen (z.B. auf Geschlecht, Abstammung, Heimat und Herkunft, Glauben), das Geburtsdatum lässt auf das Alter schließen. Abhängig von dem Suchraster der Behörden können bereits Personendaten den Ausschlag für die Einleitung von Ermittlungen gegen eine Person geben, wobei Ermittlungsverfahren meist nicht zur Feststellung einer Schuld des Beschuldigten führen und sich folglich meist gegen (vermutlich) Unschuldige richten. Nach einer Untersuchung von Verkehrsdatenabfragen durch das Max-Planck-Institut werden 72% der strafrechtlichen Ermittlungsverfahren, in denen Kommunikationsdatenabfragen erfolgreich waren, letztlich eingestellt.⁸⁹

Die eigentliche Aussagekraft der nach § 111 TKG zu erhebenden Daten liegt aber in ihrer mittelbaren Nutzbarkeit und Verwendbarkeit. In Kombination mit anderen Informationen kann die Identifizierung eines Anschlussinhabers die Aufdeckung privater und geschäftlicher Kontakte und Beziehungen, die Überwachung oder Rekonstruktion von Kommunikationsinhalten (z.B. Internetnutzung), die Ermittlung persönlicher Interessen und Vorlieben sowie die Erstellung von Bewegungsprofilen erlauben.

Identifizieren beispielsweise die Eingriffsbehörden einen Anschlussinhaber, weil seine Rufnummer in einem Notizbuch oder einem Mobiltelefon oder einem Verbindungsprotokoll oder weil seine IP-Adresse in einer E-Mail oder einem Internet-Surfprotokoll („access log“) verzeichnet ist, so lässt sich mit einiger Wahrscheinlichkeit auf einen Kontakt zwischen zwei Personen, auf die Identität des Absenders der E-Mail oder des Lesers oder Verfassers einer Internetsnachricht schließen. Umgekehrt können die Eingriffsbehörden mithilfe der einer Person zugewiesenen Rufnummer oder Internet-Anschlusskennung Kommunikationsdaten, Nachrichten und zukünftig anfallende Kommunikation des Betroffenen nachverfolgen.

Wer Inhaber welcher Kennung ist oder war, ist der Schlüssel zur Aufhebung der Vertraulichkeit des über den Anschluss abgewickelten Informations- und Kommunikationsverhaltens. Die Anonymität von Anschlussinhabern ist die Garantie der Vertraulichkeit des über den Anschluss abgewickelten Informations- und Kommunikationsverhaltens. § 111 TKG eliminiert diese Garantie ohne jeden Anlass.

⁸⁹ Starostik, http://www.vorratsdatenspeicherung.de/images/schriftsatz_2008-03-17.pdf#page=2, 2.

(b) Besondere Schutzbedürftigkeit der Fernkommunikation

In vielen Grundrechtskatalogen und Gesetzen ist die Vertraulichkeit der Fernkommunikation besonders geschützt. Grund dafür ist die im Vergleich zur unmittelbaren Kommunikation erhöhte Verletzlichkeit.

Diese Verletzlichkeit ergibt sich erstens aus dem Übertragungsweg, während dessen Überquerung sich die Kommunizierenden ihrer Nachricht entäußern müssen, ohne den Zugriff darauf noch kontrollieren zu können.

Zweitens ergibt sich eine besondere Verletzlichkeit aus der notwendigen Einschaltung eines Kommunikationsmittlers (z.B. Telekommunikationsanbieter), der die Möglichkeit hat, Nachrichten unbemerkt zur Kenntnis zu nehmen, abhören zu lassen oder zu protokollieren.

Dritter Grund der besonderen Verletzlichkeit von Fernkommunikation ist die technisch bedingte Notwendigkeit einer Adressierung. Damit Fernkommunikation ihr Ziel erreicht, muss der Adressat bezeichnet werden und ist damit identifizierbar. Damit eine Rückantwort möglich ist, muss der Absender bezeichnet werden und ist damit identifizierbar. Während der Übertragung der Nachricht muss oder kann der Kommunikationsmittler die Adresse der Kommunikationspartner zur Kenntnis nehmen, was eine anonyme Kommunikation weitgehend unmöglich macht. Ein unmittelbares Gespräch ist jederzeit möglich, ohne dass die Gesprächspartner ihre Identität offenbaren müssen. Eine gänzlich anonyme Fernkommunikation ist wegen der Notwendigkeit der Adressierung dagegen nicht möglich.

Vierter Grund der besonderen Verletzlichkeit von Fernkommunikation ist die Notwendigkeit der Bezahlung des Kommunikationsmittlers. Ist die Vermittlung nicht kostenfrei oder vorausbezahlt, müssen zur Abrechnung Zahlungsdaten erhoben werden, die eine Identifizierung des Teilnehmers zulassen. Im Fall unmittelbarer Kommunikation ist dies dagegen nicht erforderlich.

Das Bundesverfassungsgericht argumentiert bisher, hinsichtlich Telekommunikation existiere mangels öffentlicher Wahrnehmbarkeit kein gesellschaftliches Gedächtnis, das es wie in anderen Bereichen erlaubte, zurückliegende Vorgänge auf der Grundlage zufälliger Erinnerung zu rekonstruieren.⁹⁰ Die Bundesregierung hat angeführt, unmittelbare Kommunikation sei nicht anonym möglich, weil die Gesprächspartner einander wahrnehmen. Der Staat könne die Identität eines unmittelbaren Gesprächspartners etwa durch Vernehmung des anderen Gesprächsteilnehmers als Zeuge in Erfahrung bringen.

Zur Würdigung dieser Argumentation ist danach zu unterscheiden, ob der dem Staat bekannte Gesprächsteilnehmer die Identität des (dem Staat unbekannt) Gesprächspartners kennt oder nicht. Kennt der Gesprächsteilnehmer die Identität seines Gesprächspartners, so kann der Staat sie durch Zeugenvernehmung in Erfahrung bringen. Dies gilt dann unabhängig davon, ob der Kontakt in körperlicher Gegenwart oder vermittelt Telekommunikation erfolgt ist.

Kennt der Gesprächsteilnehmer die Identität seines Gesprächspartners nicht, so ist die Wahrscheinlichkeit einer Identifikation im Fall eines telekommunikativen Kontakts eher höher als im Fall eines unmittelbaren Kontakts: Auch ohne staatliche Identifizierungspflicht sind Inhaber von Telekommunikations- und Internetanschlüssen regelmäßig über betrieblich anfallende Daten identifizierbar, sei es über Kundendaten, über Zahlungsdaten oder über Lokalisierungsdaten. Bei unmittelbarer Kommunikation fallen solche Ermittlungsansätze nicht an.

Eine Identifizierung unbekannter Gesprächspartner, die ihre Identität nicht freiwillig offen gelegt haben, wird der andere Teil im Fall eines unmittelbaren Kontakts regelmäßig weder vornehmen noch ermöglichen können. Wenn man seine Identität nicht offen legt, wird ein Gespräch auf einem Marktplatz, in einer Kneipe, auf einem Bahnhof usw. in aller Regel nicht zur nachträglichen Identifizierbarkeit führen. Es kann allenfalls der Gesprächspartner beschrieben werden. Solche Fahndungen bleiben oftmals erfolglos, gerade bei Betrugs- oder Äußerungsdelikten, wie sie bei der Aufklärung von Fernkommunikation im Vordergrund stehen. Bei öffentlichen Veranstaltungen und sonst in der Öffentlichkeit bleibt man regelmäßig in der Menschenmenge anonym. Man behält weitgehend die Kontrolle darüber, ob und gegenüber wem man seine Identität offen legt. Bei der Fernkommunikation kann eine Identifizierung mithilfe des Gesprächspartners sogar leichter möglich sein, etwa wenn die Stimme auf seinem Anrufbeantworter aufge-

⁹⁰ BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 217.

nommen wurde oder eine E-Mail vorliegt, die man auf technische Daten des verwendeten Computers, typische Schreibweisen usw. analysieren kann.

Weitgehend anonym ist auch die unmittelbare verkörperte Kommunikation. Wer einen Brief ohne Absenderangabe in einen Briefkasten einwirft, bleibt unerkannt. Wer hingegen denselben Text per SMS verschickt, gibt dem Empfänger eine persönliche Absenderkennung preis, die eine Identifizierung jederzeit ermöglicht.

Die Nutzung von Fernkommunikationsmitteln begründet auch dann eine erhöhte Gefahr für die Vertraulichkeit eines Kontakts, wenn die Gesprächspartner einander kennen. Einer Ausforschung der persönlichen Kontakte eines Beschuldigten wird meist schon entgegen stehen, dass die Ermittlungsbehörden nicht wissen, mit wem ein Beschuldigter in Kontakt gestanden hat, so dass eine Zeugenvernehmung oder andere Ermittlungsmaßnahme von vornherein ausscheidet. Wurde ein Kommunikationsmittler genutzt, sind die Kommunikationspartner demgegenüber leicht mithilfe der zentral gespeicherten Verbindungsdaten herauszufinden.

Zudem ist der Staat zur Ausforschung unmittelbarer Kommunikation auf die Kooperation des Kommunikationspartners angewiesen, der aber – etwa wenn er selbst Beschuldigter ist – von einem Aussageverweigerungsrecht Gebrauch machen oder als Zeuge lügen oder sich nicht mehr erinnern kann. Im Fall der Fernkommunikation verfügt der Staat demgegenüber über einen stets erreichbaren, stets kooperationswilligen und über objektive Aufzeichnungen verfügenden Dritten, der ihm jederzeit kostengünstig Auskunft erteilen kann.

Die Einschaltung eines Mittlers macht die Fernkommunikation folglich ausforschungsanfälliger als wenn nur der Gesprächspartner als Informationsquelle zur Verfügung steht. Der Mittler kann ohne Vorkenntnisse von Kontakten angegangen werden und die gesamten Fernkommunikationsbeziehungen einer Person anhand seiner eigenen technischen Aufzeichnungen aufdecken.

Im Übrigen trifft das Argument, entsprechende Informationen ließen sich auch auf andere Weise gewinnen, gleichermaßen auf Kommunikationsinhalte und Verbindungsdaten zu. Ebenso wie die Identität von Gesprächspartnern lassen sich auch Gesprächsinhalte und sonstige Gesprächsumstände im Einzelfall durch Zeugenaussagen oder anders rekonstruieren. Gleichwohl würde niemand daraus folgern, ein besonderer Schutz der Fernkommunikation sei überflüssig. Denn die Fernkommunikation ermöglicht Dritten einen heimlichen, zentralen, beweiskräftigen, kooperationsbereiten und kostengünstigen Zugriff auf Kommunikationsbeziehungen, wie ihn andere Ermittlungsmethoden niemals möglich machen können.

Das Argument, die Identifizierung gegenüber dem Kommunikationsmittler gemäß § 111 TKG trete nur an die Stelle der Identifizierung gegenüber dem Gesprächspartner bei unmittelbarer Kommunikation, erweist sich mithin als nicht tragfähig – zumal sich Gesprächspartner kaum einmal einen Ausweis vorlegen lassen werden. Die Behauptung, der Staat könne Telekommunikation schwerer nachvollziehen als unmittelbare Kommunikation, ist in der Praxis nicht haltbar. Richtig ist im Gegenteil, dass der Staat Telekommunikation und die daran Beteiligten technisch bedingt leichter nachvollziehen kann als unmittelbare oder verkörperte Kommunikation. Mit dem Risiko aber, dass aus den eigenen Kontakten jederzeit (nachteilige) Folgen erwachsen können, steht und fällt die Möglichkeit zu freier und unbefangener, in allem vertraulicher Kommunikation.

Ziel des Fernkommunikationsgeheimnisses ist es gerade, eine freie und unbefangene Kommunikation auch über die Ferne zu gewährleisten.⁹¹ Das Recht soll die Bedingungen einer freien Fernkommunikation aufrechterhalten.⁹² Es soll verhindern, dass der Meinungs- und Informationsaustausch mittels Telekommunikationsanlagen deswegen unterbleibt oder nach Form und Inhalt verändert verläuft, weil die Beteiligten damit rechnen müssen, dass staatliche Stellen sich in die Kommunikation einschalten und Kenntnisse über die Kommunikationsbeziehungen oder Kommunikationsinhalte gewinnen.⁹³

⁹¹ Vgl. BVerfG, Beschluss vom 27.7.2005, Az. 1 BvR 668/04, Abs. 81.

⁹² Vgl. BVerfG, Beschluss vom 12.3.2003, Az. 1 BvR 330/96, Abs. 47; Urteil vom 14.07.1999, Az. 1 BvR 2226/94, Abs. 162.

⁹³ Vgl. BVerfGE 100, 313 (359); BVerfG, Beschluss vom 12.3.2003, Az. 1 BvR 330/96, Abs. 47.

An diesem Ziel gemessen muss die Identität Fernkommunizierender vertraulich bleiben. Die fehlende Anonymität der Fernkommunikation wegen der Vorhaltung von Vertragsdaten bei einem Mittelsmann beeinträchtigt die Bereitschaft zur vertraulichen Kommunikation auf elektronischem Wege schwerwiegend, weil man gegebenenfalls Nachteile infolge der eigenen Verbindungen, Aussagen, Bewegungen oder Interessen befürchten muss.

Der Erläuternde Bericht zur Empfehlung des Europarats zum Datenschutz in der Telekommunikation⁹⁴ führt in Abs. 5 aus, dass die technische Entwicklung „nicht nur die Privatsphäre von Teilnehmern und Nutzern allgemein gefährden kann, sondern auch deren Kommunikationsfreiheit behindern kann, weil sie das Maß an Anonymität mindert, der sich Teilnehmer und Nutzer unter Umständen bei der Benutzung des Telefons bedienen wollen, indem sie gezwungen werden, ihre Identitäten offenzulegen oder elektronische Spuren zu hinterlassen, die es ermöglichen, die Benutzung ihres Telefons zu überwachen.“⁹⁵

Das Kommunikationsgeheimnis soll eine in allem vertrauliche Fernkommunikation ermöglichen.⁹⁶ Eine in allem vertrauliche Fernkommunikation ist aber nur im Schutz der Anonymität möglich. Die Grundrechte müssen dazu gewährleisten, dass die Fernkommunikation im Alltag anonym erfolgen kann. Wegen der besonderen Verletzlichkeit der Anonymität im Fall der Fernkommunikation bedarf Fernkommunikation nicht nur hinsichtlich ihres Inhalts, sondern auch hinsichtlich der Identität der Kommunikationspartner eines besonderen Schutzes. Vertraulich bleiben müssen nicht nur die Adressen, Rufnummern oder Kennungen, zwischen denen eine Kommunikation stattgefunden hat, sondern auch die Identität der Inhaber dieser Adressen, Rufnummern oder Kennungen.

(c) Schutzwürdigkeit der Teilnehmeridentität im Vergleich zu anderen Kommunikationsdaten

Die Information, wer über welche Kennung welches Anbieters telekommuniziert, beschreibt die im Rahmen dieses Vertragsverhältnisses abgewickelten einzelnen Kommunikationsvorgänge inhaltlich näher. Nur mithilfe der Teilnehmeridentität lässt sich rekonstruieren, wer (Name, Anschrift, Geburtsdatum) eine bestimmte Verbindung über welchen Anbieter und unter Verwendung welchen Anschlusses (Anschrift und Lage des Anschlusses, Art des Anschlusses, Gerätenummer des Mobiltelefons) hergestellt oder entgegen genommen hat.

Dem lässt sich nicht entgegen halten, die Identität eines Gesprächsteilnehmers lasse sich auch auf andere Weise (z.B. Zeugenaussagen, Beschlagnahme eines Adressbuchs) aufdecken. Denn auch Kommunikationsinhalte und -umstände können sich auf andere Weise aufdecken lassen. Nichtsdestotrotz schützt das Fernkommunikationsgeheimnis davor, dass diese Informationen gerade durch Zugriff auf den Kommunikationsmittler erhoben werden, wovon sich die an einer Fernkommunikation Beteiligten nicht schützen können und was besonders unbemerkt und kostengünstig möglich ist.

Das Bundesverfassungsgericht hat es bisher abgelehnt, der Identität von Anschlussinhabern den gleichen Schutz zukommen zu lassen wie sonstigen Umständen und Inhalten von Fernkommunikation. Zur Begründung hat es angeführt, die Identität eines Anschlussinhabers lasse für sich genommen noch keinen Rückschluss auf Inhalt und Umstände von Fernkommunikation zu.

Diese Betrachtungsweise verkennt, dass auch eine Rufnummer, eine Uhrzeit oder ein Text für sich genommen noch keinen Rückschluss auf Inhalt und Umstände einer Fernkommunikation zulassen. Dieser Rückschluss wird erst mit dem Zusatzwissen möglich, dass über eine bestimmte Rufnummer eines bestimmten Inhabers zu einer bestimmten Uhrzeit eine bestimmte SMS-Nachricht versandt worden ist. Tatsächlich ist die Kenntnis der Identität eines Kommunikationsteilnehmers in der Regel sogar sehr viel aussagekräftiger als der (genaue) Inhalt oder einzelne Umstände (z.B. Verbindungsdauer, Datenvolumen) einer Kommunikation, mit denen sich meist wenig anfangen lässt.

⁹⁴ Empfehlung R (95) 4 vom 07.02.1995.

⁹⁵ [https://wcd.coe.int/ViewDoc.jsp?](https://wcd.coe.int/ViewDoc.jsp?id=529277&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75)

[id=529277&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75](https://wcd.coe.int/ViewDoc.jsp?id=529277&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75).

⁹⁶ Vgl. Zu Art. 10 GG BVerfGE 100, 313 (359); BVerfGE 107, 299, Abs. 50; BVerfGK 5, 74, Abs. 23; BVerfGK 8, 219, Abs. 4.

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

Das Landgericht Frankenthal führt zur Identität eines Internet-Anschlussinhabers zutreffend aus:

„Die von dem überwachenden Unternehmen ausgespähete IP-Adresse ermöglicht schon aus logischen Gründen keine unverwechselbare Individualisierung desjenigen Anschlussinhabers, der diese Adresse zum Tatzeitpunkt benutzt hat, weil erst die Verknüpfung mit den Daten des jeweiligen Providers die Zuordnung zu einem bestimmter Anschlussinhaber erlaubt. Erst die begehrte Auskunft führt somit zur Individualisierung. Ohne diese Auskunft sind die von dem ausspähenden Unternehmen zusammengetragenen Daten ein technisches und rechtliches Nullum, mit dem niemand etwas anfangen kann. [...]

Es ist jedoch nach Auffassung der Kammer weder interessen- noch sachgerecht und letztlich nicht nachvollziehbar, weshalb sich der Grundrechtsschutz des betroffenen Telekommunikationsteilnehmers an einer rechtlich umstrittenen Einstufung bestimmter Daten als Verkehrs- oder Bestandsdaten orientieren soll. Maßgeblich erscheint vielmehr, dass es in Fällen wie dem vorliegenden durch die Offenlegung privater Telekommunikationsdaten zu einer Deanonymisierung kommt, die es ermöglicht, nicht für Dritte bestimmte, dem Fernmeldegeheimnis unterliegende Daten bestimmten Personen zuzuordnen.“⁹⁷

Das Bundesverfassungsgericht meint bisher, der Informationsgehalt der nach § 111 TKG zu erhebenden Daten reiche „nicht sehr weit“.⁹⁸ Der Erkenntniswert von Bestandsdatenauskünften bleibe punktuell und systematische Ausforschungen über einen längeren Zeitraum oder die Erstellung von Persönlichkeits- und Bewegungsprofilen ließen sich allein auf Grundlage solcher Auskünfte nicht verwirklichen.⁹⁹

Bei dieser Betrachtungsweise gerät jedoch die Funktion von Identitätsdaten als Schlüssel zu weiteren Kommunikationsdaten aus dem Blick: Bei den Diensten Telefonie, E-Mail und Internet können Kommunikationspartner weithin das Kommunikations- und Internetnutzungsverhalten des Grundrechtsträgers anhand dessen Anschlusskennung, E-Mail-Adresse oder IP-Adresse aufzeichnen und nachvollziehen. Werden solche Aufzeichnungen (z.B. Liste eingehender Anrufe, eingegangene E-Mails, Internetnutzungs-Logfiles) dem Staat zur Verfügung gestellt, so bleibt der Erkenntniswert einer Auskunft des Kommunikationsmittlers über die Identität des Anschlussinhabers keineswegs punktuell, sondern ermöglicht erst die personenbezogene, systematische Ausforschung des Kommunikations- und Informationsverhaltens eines Menschen über einen längeren Zeitraum oder die Erstellung von Persönlichkeits- und Bewegungsprofilen. Wenn die Bundesrepublik Kommunikationsmittler zur Identifikation ihrer Kunden zwingen will, so tut sie dies gerade, um unsere Telekommunikation und Internetnutzung ausforschen zu können.

Besonders schutzwürdig ist die Anonymität von Internetnutzern. Wenn wir Zeitungen, Magazine oder Bücher lesen, wenn wir im Radio Musik hören oder fernsehen, brauchen wir nicht zu befürchten, dass uns jemand über die Schulter schauen oder mitschreiben könnte. Lesen wir hingegen Zeitungen, Magazine oder Bücher im Internet, hören wir dort Musik oder betrachten wir Videos im Internet (z.B. eine Ministerrede auf der Ministeriumsseite), muss der Anbieter für die Dauer der Übertragung aus technischen Gründen unsere IP-Adresse kennen. Anhand dieser Adresse oder anderer Nutzerkennungen kann jede Eingabe und jeder Mausklick beim Lesen, Schreiben und Diskutieren im Internet erfasst, aufgezeichnet, ausgewertet, weiter gemeldet und offen gelegt werden. Eine Erfassung unseres Internet-Nutzungsverhaltens ist nicht nur einer Filmaufzeichnung unseres Zeitungslesens oder Fernsehens vergleich-

⁹⁷ LG Frankenthal, Beschluss vom 21.05.2008, Az. 6 O 156/08.

⁹⁸ BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 136.

⁹⁹ BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 256.

bar. Vielmehr können Internet-Nutzungsdaten – anders als Videoaufzeichnungen – maschinell zugeordnet und ausgewertet werden und weisen daher eine besonders „hohe Sensitivität“ auf.¹⁰⁰ Was wir im Internet lesen, suchen und schreiben, spiegelt unsere Persönlichkeit, unsere Vorlieben und Schwächen in einmaliger Deutlichkeit wider.

Die nach § 111 TKG gespeicherte Teilnehmeridentität macht in Verbindung mit Nutzungsprotokollen der Anbieter (die dem Staat zugänglich sind) potenziell dessen gesamte Internetnutzung nachvollziehbar, also die Inhalte, für die er sich im Netz interessiert (gelesene Internetseiten, eingegebene Suchbegriffe), die er veröffentlicht oder per E-Mail versandt hat. Eine Identifizierung aller Inhaber von Internetanschlüssen hebt damit die Anonymität der Internetnutzung auf,¹⁰¹ die in vielen Situationen Voraussetzung für die Kommunikationsbereitschaft der Beteiligten ist (z.B. anonyme Information von Journalisten per E-Mail, anonyme Meinungsäußerung im Internet, vertraulicher Austausch von Geschäftsgeheimnissen, vertrauliche Koordinierung politischer Proteste, psychologische, medizinische und juristische Beratung oder Selbsthilfegruppen von Menschen in besonderen Situationen wie Notlagen und Krankheiten). Ist Anonymität in diesen Situationen nicht vorhanden, kann Kommunikation anders verlaufen oder ganz unterbleiben, was schwerwiegende Nachteile für Grundrechtsträger und die Gesellschaft insgesamt nach sich ziehen kann.

Die nach § 111 TKG gespeicherte Teilnehmeridentität ermöglicht in Verbindung mit Nutzungsprotokollen der Anbieter überdies die ungefähre Rekonstruktion des Aufenthaltsorts eines Nutzers anhand der genutzten IP-Adresse, nach neuen Forschungsergebnissen sogar mit hoher Treffsicherheit, ob sich der Nutzer zu Hause, in der Arbeit oder unterwegs aufgehalten hat.¹⁰² Die nach § 111 TKG gespeicherten Daten können also auch die Erstellung von Bewegungsprofilen von Internetnutzern ermöglichen.

Welchen Aufschluss Standortdaten über unser Privatleben geben, zeigt ein Versuch des US-amerikanischen Forschungszentrums MIT, bei dem Telekommunikations-Verbindungsdaten und auf 10m genaue Standortdaten von 100 Versuchspersonen erhoben wurden. Mithilfe dieser Daten gelang es mit einer 90%igen Genauigkeit, die Arbeitskollegen, Bekannten und Freunde jedes Versuchsteilnehmers zu identifizieren.¹⁰³ Ferner waren umfangreiche Vorhersagen möglich. Anhand der Bewegungsdaten einer Person während eines Monats konnte mit einer 95%igen Genauigkeit vorhergesagt werden, wann sich die Person am Arbeitsplatz, zu Hause oder an einem anderen Ort aufhalten würde.¹⁰⁴ Weiter konnte mit einer 90%igen Genauigkeit vorhergesagt werden, ob sich zwei Personen innerhalb der nächsten Stunde begegnen würden.¹⁰⁵ Anhand der Aktivitäten einer Person während der ersten 12 Stunden eines Tages konnten die Aktivitäten während der verbleibenden 12 Stunden mit etwa 80% Genauigkeit vorhergesagt werden.¹⁰⁶ Auch die Zufriedenheit am Arbeitsplatz konnte anhand der Daten vorhergesagt werden.¹⁰⁷ Die weitere Forschung arbeitet daran, das Verhalten großer Organisationen und Gruppen anhand von Kommunikations- und Standortdaten vorherzusagen.¹⁰⁸

Prof. Dieter Fox von der Seattle University hat auf dem Gebiet der „Informationsfusion“ eine Software entwickelt, die anhand der über einige Tage hinweg gesammelten Positionsdaten einer Person mithilfe öffentlich zugänglichen Kartenmaterials und Telefonbüchern in Sekundenschnelle Wohnort, Arbeitsstelle, bevorzugte Verkehrsmittel und

¹⁰⁰ Bundesregierung, Begründung zum TDDSG, BT-Drs. 13/7385, 25.

¹⁰¹ Vgl. BVerfG MMR 2010, 356.

¹⁰² Pitsillidis/Xie/Yu/Abadi/Voelker/Savage, How to Tell an Airport from a Home, 2010, <http://research.microsoft.com/pubs/139079/hotnets10.pdf>.

¹⁰³ MIT, Relationship Inference, <http://reality.media.mit.edu/dyads.php>.

¹⁰⁴ MIT, User Behavior Modeling and Prediction, <http://reality.media.mit.edu/user.php>.

¹⁰⁵ MIT, Relationship Inference, <http://reality.media.mit.edu/dyads.php>.

¹⁰⁶ MIT, Eigenbehaviors, <http://reality.media.mit.edu/eigenbehaviors.php>.

¹⁰⁷ Eagle/Pentland/Lazer, Inferring Social Network Structure using Mobile Phone Data, 2007, http://reality.media.mit.edu/pdfs/network_structure.pdf.

¹⁰⁸ MIT, Machine Perception and Learning of Complex Social Systems, <http://reality.media.mit.edu/>.

die Adressen häufig besuchter Bekannter der Zielperson ermittelt.¹⁰⁹ Angezeigt wird auch, wie lange die Person schläft, wann sie frühstückt, ob sie mit dem Auto oder dem Bus zur Arbeit fährt und in welchem Restaurant sie danach war. Abweichungen vom „normalen“ Bewegungsverhalten der Person lassen sich sofort auffinden und analysieren. Mithilfe mathematischer Algorithmen und Zusatzinformationen wie Stadtplänen und Busrouten lassen sich auch Ungenauigkeiten bei der Positionsbestimmung bereinigen.

Die Aussagekraft einer Information kann nie allein aus ihr selbst heraus beurteilt werden, sondern nur unter Berücksichtigung ihres Verwendungszusammenhangs.¹¹⁰ Entscheidend sind Nutzbarkeit und Verwendungsmöglichkeit der Information.¹¹¹ Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den bestehenden Verarbeitungsmöglichkeiten und Verknüpfungsmöglichkeiten ab.¹¹²

Die Teilnehmeridentität gibt in Kombination mit weiteren Informationen Aufschluss darüber, wer an bestimmten Telekommunikationsvorgängen beteiligt war, und ermöglicht die Erhebung von Kommunikationsinhalten (durch nachfolgende Überwachung des Teilnehmeranschlusses oder durch Abhören von Mailboxen). Die Identität des Kommunikationsteilnehmers ist dabei in der Regel sehr viel bedeutsamer als der (genaue) Inhalt oder einzelne Umstände (z.B. Verbindungsdauer, Datenvolumen) einer Fernkommunikation. Solange der Kommunikationsteilnehmer anonym bleibt, hat er keine Nachteile durch die staatliche Kenntnisnahme seiner Kommunikation zu befürchten. Die Teilnehmeridentität stellt den Schlüssel zur Durchbrechung der Vertraulichkeit der Telekommunikation dar.

Wird der Inhaber einer Kommunikationskennung identifiziert, um seine Fernkommunikation auszuforschen oder zuzuordnen, so wird in die Vertraulichkeit seiner Fernkommunikation eingegriffen. Dasselbe gilt, wenn der Staat alle Inhaber von Kennungen auf Vorrat identifizieren lässt, um im Bedarfsfall ihre Fernkommunikation auszuforschen oder zuzuordnen zu können. Denn dieses Verfahren hebt die Anonymität der Fernkommunikation der Betroffenen auf und ermöglicht staatlichen Stellen jederzeit die Ausforschung deren Kommunikation.

Das Bedürfnis nach anonymer Kommunikation erhöht sich weiter in Anbetracht der Tatsache, dass inzwischen selbst eine flächendeckende Vorratsspeicherung von Verkehrsdaten (Verbindungsdaten, Standortdaten, Internet-Nutzungskennung) gesetzlich vorgesehen ist. Unabhängig von der Frage der Vereinbarkeit dieses Instruments mit den Grundrechten ist festzustellen, dass sämtliche Kommunikations-, Bewegungs- und Internetzugangsdaten wochenlang für staatliche Zwecke vorgehalten werden. Wo solche Gesetze gelten, kann der Kunde mit dem Anbieter nicht die umgehende Löschung seiner Daten mit Verbindungsende vereinbaren (z.B. Flatrate-Tarif).

Im Fall einer Vorratsspeicherung von Verkehrsdaten ist die anonyme Nutzung von Mobiltelefon oder E-Mail das einzige verbleibende Mittel, das die systematisch aufgezeichneten Kommunikationsbeziehungen und Standortdaten noch einigermaßen vor einer Kenntnisnahme und Zuordnung durch den Staat oder Dritte (z.B. Urheberrechtinhaber) schützen kann. Die EU-Richtlinie zur Vorratsdatenspeicherung schränkte die Zulässigkeit anonymer Kommunikationsdienste nicht ein, sondern setzte sie voraus (vgl. Art. 5 Abs. 1 Buchst. e Ziff. 2 vi: „vorbezahlte anonyme Dienste“).

Gerade wo eine totale Verkehrsdatenaufbewahrung in Kraft ist, müssen die schädlichen Auswirkungen einer allgemeinen Verkehrsdatenspeicherung auf die freie und unbefangene Kommunikation begrenzt werden, indem anonyme Telekommunikationsnutzung ermöglicht wird. Eine allgemeine Verkehrsdatenspeicherung wäre gänzlich unerträglich, wenn den betroffenen, oftmals auf nicht rückverfolgbare Kommunikation angewiesenen Personen auch noch die Möglichkeit genommen würde, sich durch Verwendung anonymer Kommunikationsanschlüsse zu schützen.

Das Bundesverfassungsgericht ist bisher der Auffassung, staatliche Bestandsdatenzugriffe hätten ein erheblich weniger belastendes Gewicht als die nahezu vollständige Speicherung der Daten sämtlicher Telekommunikationsver-

¹⁰⁹ Deutschlandradio vom 02.07.2008, <http://www.dradio.de/dlf/sendungen/forschak/810455/>.

¹¹⁰ BVerfGE 65, 1 (45).

¹¹¹ BVerfGE 65, 1 (45).

¹¹² BVerfGE 65, 1 (45).

bindungen auf Vorrat.¹¹³ Dies trifft dies jedenfalls auf einen allgemeinen Identifizierungszwang nicht zu. Solange eine anonyme Telekommunikation möglich ist, ist eine Verkehrsdatenspeicherung weitaus weniger belastend, weil man eine – eventuell missbräuchliche – Zuordnung und personenbezogene Auswertung gespeicherter Verkehrsdaten wenigstens noch mithilfe anonymer Kommunikation einigermaßen vermeiden kann.

Das Bundesverfassungsgericht wendet gleichwohl eine rein formale Betrachtungsweise an, derzufolge nur die veränderlichen Umstände (Verkehrsdaten) und Inhalte der Fernkommunikation nach Art. 10 GG besonders zu schützen seien, nicht aber ihre gleich bleibenden Umstände (über wessen Anschluss wurde kommuniziert?). Die Identität des Anschlussinhabers verdiene nur dann besonderen Schutz, wenn zu ihrer Offenlegung Verkehrsdaten verarbeitet werden müssten, namentlich im Fall veränderlicher Kommunikationskennungen (dynamisch zugewiesener IP-Adressen).

Dieses rein formale Abgrenzungskriterium zieht Wertungswidersprüche nach sich und ist logisch nicht begründbar: So ist nach ihm die Identität des Nutzers einer dynamischen IP-Adresse im Internet besser geschützt als die Identität des Nutzers einer festen IP-Adresse, obwohl die technische Art des Internetzugangs zufällig und ohne Bedeutung für die Schutzwürdigkeit der Identität des Internetnutzers ist. Außerdem verarbeitet der Staat, wenn er die Identität des Inhabers einer festen Kennung zwecks Ausforschung einer Kommunikationsverbindung erhebt, durchaus Verkehrsdaten. Er verknüpft dann nämlich die ihm bekannten Umstände der Kommunikationsverbindung (Verkehrsdaten) mit der Identität der Person, über deren Anschluss die Verbindung hergestellt wurde.

Das deutsche Recht ordnet die nach § 111 TKG zu speichernde Kommunikationskennung selbst als Verkehrsdatum ein. Sie wird nicht als Bestandsdatum von dem Teilnehmer erhoben (§ 3 Nr. 3 TKG), sondern von dem Anbieter – als Bestandteil seines Kommunikationsdienstes – zugeteilt (§ 3 Nr. 30 TKG).¹¹⁴ § 96 Abs. 1 Nr. 1 TKG bezeichnet „die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung“ ausdrücklich als „Verkehrsdaten“. Die Kommunikationskennung betrifft nicht die Person des Teilnehmers, sondern ermöglicht ein- und ausgehende Verbindungen. § 3 Nr. 30 TKG definiert „Verkehrsdaten“ als „Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden“. Auch Art. 2 Buchst. b RiL 2002/58/EG definiert „Verkehrsdaten“ als „Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden“. Die Zuweisung einer Kommunikationskennung und die Vorhaltung eines Anschlusses durch den Anbieter ist notwendiger Bestandteil jedes Fernkommunikationsdienstes. Die Kommunikationskennung wird daher bei der Erbringung des Telekommunikationsdienstes zum Zweck der Vermittlung von Fernkommunikation gespeichert und ist Verkehrsdatum.

Dass die Teilnehmeridentität eine vergleichbare Sensibilität aufweist wie andere Verbindungsdaten, hat der deutsche Gesetzgeber inzwischen mit der Regelung zur Meldepflicht von Datenpannen in § 93 Abs. 3 TKG anerkannt. Der Verlust von Bestands- und Verkehrsdaten begründet danach gleichermaßen eine Informationspflicht. Die Begründung des Gesetzentwurfs zu § 93 Abs. 3 TKG führt dazu aus, die Meldepflicht beziehe sich „auf besonders sensible personenbezogene Daten“¹¹⁵, wozu der Gesetzgeber Bestands- und Verkehrsdaten gleichermaßen zählt.

In anderen Vertragsstaaten genießt die Zuordnung von Anschlusskennungen folgerichtig denselben Schutz wie andere bei der Fernkommunikation anfallende Daten. Das britische Recht definiert etwa sämtliche bei Kommunikationsmittlern vorhandene Daten – Verbindungs-, Bestands- und sonstige Kundendaten – einheitlich als „Kommunikationsdaten“ („communications data“, § 21 Abs. 4 Regulation of Investigatory Powers Act 2000) und regelt auch den staatlichen Zugriff darauf grundsätzlich einheitlich.

Gleiches liegt der Empfehlung Nr. R (95)4 des Europarates zum Schutz persönlicher Daten im Bereich der Telekommunikationsdienste vom 7. Februar 1995 zugrunde.¹¹⁶ Diese regelt die „Sammlung und Verarbeitung personenbezogener Daten im Bereich von Telekommunikationsdiensten“ einheitlich (Grundsatz 3). Als Oberbegriff wird

¹¹³ BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 257.

¹¹⁴ Riechert, Neue Online-Dienste und Datenschutz (2006), 168 ff.; Bizer, DuD 2007, 602 (602).

¹¹⁵ Bundesregierung, BT-Drs. 16/12011, 34.

¹¹⁶ http://www.giodo.gov.pl/plik/id_p/31/j/en/.

„Servicedaten“ verwendet, womit Inhaltsdaten, Verkehrsdaten, Bestandsdaten und sonstige personenbezogene Daten gleichermaßen gemeint sind.¹¹⁷ Auch die Weitergabe personenbezogener Daten wird einheitlich geregelt (Grundsatz 4). In Abs. 53 des Erläuternden Berichts heißt es, „die Verfasser dieser Empfehlung wollten Servicedaten innerhalb des Grundsatzes des Brief- und Kommunikationsgeheimnisses ansiedeln, wie er in Artikel 8 des Europäischen Menschenrechtskonvention niedergelegt ist“. Auch die Verfasser der Empfehlung des Europarats gehen also davon aus, dass Bestandsdaten dem besonderen Schutz des Fernkommunikationsgeheimnis unterliegen.

Die Bundesrepublik argumentiert, § 111 TKG diene nur zu einem Teil der Zuordnung konkreter Fernkommunikationsvorgänge. Häufig würden Teilnehmer auch ohne Bezug zu einem konkreten Kommunikationsvorgang identifiziert, etwa wenn an einem Tatort ein Notizbuch mit Rufnummern vorgefunden werde.

Diesem Einwand ist erstens entgegen zu halten, dass mit der Identifizierung des Inhabers einer Nummer aus einem Notizbuch durchaus abgeschlossene oder beabsichtigte Fernkommunikation aufgedeckt wird. Ist eine Rufnummer in einem Notizbuch notiert, so ist ein Kontakt des Verfassers mit dem Inhaber der Rufnummer zu vermuten. Gerade deshalb nimmt der Staat ja die Identifizierung vor. Das Fernkommunikationsgeheimnis schützt vor einer Aufdeckung der Information, wer mit wem fernkommuniziert hat, auch ohne Kenntnis der näheren Umstände der Kommunikation.

Zweitens erfordert der Zweck des Fernkommunikationsgeheimnisses die umfassende Einbeziehung der Inhaberschaft von Kommunikationskennungen, um den gleichen Vertraulichkeitsschutz wie bei unmittelbarer Kommunikation zu gewährleisten. Kommunizieren Menschen unmittelbar miteinander, entstehen keine Telefonbücher mit eindeutigen Kennungen der Gesprächspartner. Bei unmittelbarer Kommunikation sind die Kommunizierenden nicht auf die Verwendung und Offenbarung eines Adressierungsmerkmals angewiesen, das einen eindeutigen Rückschluss auf ihre Person zulässt. Wer fernkommuniziert, muss dagegen über eine eindeutige Fernmeldekennung des Kommunikationspartners verfügen (z.B. Rufnummer, E-Mail-Adresse, IP-Adresse). Diese Kennung wird auch bei ausgehender Kommunikation oft unfreiwillig offenbart (z.B. E-Mail-Adresse, IP-Adresse). Wo im direkten Kontakt unfreiwillig nur das (anonyme) Gesicht offenbart wird, wird im Fernkontakt eine eindeutige, personenbezogene Kennung offengelegt, die gespeichert und ausgewertet werden kann und die sich jederzeit eindeutig der Person des Anschlussinhabers zuordnen lässt. Das technische Erfordernis einer eindeutigen Kommunikationskennung begründet daher eine spezifische Gefährdung der Anonymität der Fernkommunikation, die zu Schützen Zweck des Kommunikationsgeheimnisses ist. Dass Telekommunikation regelmäßig das Aufschreiben oder Abspeichern der Anschlusskennung der Gegenseite voraussetzt, bekräftigt die technikbedingt erhöhte Verletzlichkeit distanzierter Kommunikation und die entsprechend erhöhte Schutzwürdigkeit der Identität von Anschlussinhabern.

Drittens hat es der Staat mit der Identifikation eines Anschlussinhabers in der Hand, zukünftig bekannt werdende Fernkommunikation der Person des Kommunikationspartners zuzuordnen oder dessen künftige Kommunikation zu überwachen. Auch wenn der Staat das Pseudonym einer Kommunikationskennung also zunächst nicht zur Ausforschung eines konkreten Kommunikationsvorgangs aufhebt, kann er die erhobene Information doch fortan jederzeit genau zu diesem Zweck nutzen. Bei dem Staat eingehende oder ihm zugetragene Kommunikationen können nun ohne Mitwirkung des Kommunikationsmittlers der Person des Anschlussinhabers zugeordnet werden. Die Anonymität der Kommunikationskennung ist aufgehoben. Eine freie, unbefangene in allem vertrauliche Fernkommunikation, die in bestimmten menschlichen Situationen auch anonym möglich sein muss, ist nicht mehr möglich. Eine jederzeit identifizierbare Kommunikation droht nach Art und Inhalt verändert zu verlaufen oder zu unterbleiben. Genau davor schützt das Fernkommunikationsgeheimnis.¹¹⁸

In seiner Entscheidung zur Computerdurchsuchung hat das Bundesverfassungsgericht anerkannt, dass Schutzlücken entstünden, würden die Grundrechte erst vor dem Zugriff auf und nicht schon vor der vorgelagerten Infiltration eines informationstechnischen Systems schützen.¹¹⁹ Es hat einen Eingriff in das Persönlichkeitsrecht bereits

¹¹⁷ Abs. 25 des Erläuternden Berichts, <https://wcd.coe.int/ViewDoc.jsp?id=529277&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75>.

¹¹⁸ Vgl. BVerfGE 100, 313 (359); BVerfG, Beschluss vom 12.3.2003, Az. 1 BvR 330/96, Abs. 47.

¹¹⁹ BVerfG, Urteil vom 27.2.2008, Az. 1 BvR 370/07, Abs. 181.

dann angenommen, wenn „die entscheidende technische Hürde für eine Ausspähung [...] des Systems genommen“ ist.¹²⁰ Was für die Ausspähung eines informationstechnischen Systems gilt, muss auch für die Ausspähung einer fernkommunizierenden Person gelten: Mit Aufdeckung der Zuordnung einer Kommunikationskennung zu ihrer Person ist „die entscheidende technische Hürde für eine Ausspähung“ der Fernkommunikation dieses Nutzers genommen. Mithilfe dieser Zuordnungsfunktion kann der Staat nämlich Verbindungen des Nutzers, der seine Kennung technisch bedingt gegenüber seinen Kommunikationspartnern offen legen muss (z.B. E-Mail-Adresse, IP-Adresse, eingeschränkt auch Rufnummer), identifizieren und diesem zuordnen.

Die Identifizierung des Inhabers einer Rufnummer ist vergleichbar mit der Anfertigung eines Nachschlüssels zu einer Wohnung durch den Staat. Verfügt der Staat über den Schlüssel, kann er fortan jederzeit unbemerkt in die Privatsphäre des Betroffenen eindringen.

Zuletzt lässt sich im Fall einer staatlichen Teilnehmeridentifikation nicht zuverlässig abgrenzen, ob sie zur Fernkommunikationsausforschung vorgenommen wird oder nicht. Da Kommunikationsmittler nicht erkennen können, welchem Zweck ein Auskunftsuchen dient, muss Art. 10 GG im Sinne der Effektivität in stets gleichem Maße die Information schützen, wer über welche Kennung kommuniziert. Eine Unterscheidung nach dem Zweck eines Eingriffs wäre zwar möglich, schaffte aber freiheitsgefährdende Abgrenzungsprobleme und Umgehungsgefahren. Zudem wäre die Möglichkeit einer nachträglichen Zweckänderung der einmal erhobenen Daten in Betracht zu ziehen und zu regeln. Insgesamt ist es einfacher und schützt die Grundrechtsträger wirksamer, die Identität eines Anschlussinhabers stets gleich zu schützen. Der wirksame Schutz des Fernkommunikationsgeheimnisses erfordert einen umfassenden Schutz der Anonymität des Inhabers einer Kommunikationskennung.

(d) Schutzwürdigkeit der TK-Teilnehmeridentität im Vergleich zu sonstigen Kundendaten

Fehl geht das Argument, vergleichbare Kundendaten fielen auch bei anderen Unternehmen an.

Eines besonderen Schutzes bedarf die dem Kommunikationsmittler offenbarte Teilnehmeridentität nicht, weil sie aus sich heraus besonders persönlichkeitsrelevant wäre. Name, Anschrift und Geburtsdatum von Personen werden in der Tat auch in anderem Zusammenhang erhoben und gespeichert.

Eines besonderen Schutzes bedarf die dem Kommunikationsmittler anvertraute Teilnehmeridentität deshalb, weil ihre Geheimhaltung Voraussetzung einer freien und unbefangenen Fernkommunikation über den Anschluss ohne Furcht vor nachteiligen Konsequenzen ist. Nur, wenn die Anmeldung und Unterhaltung eines Telekommunikationsanschlusses oder -kontos anonym möglich ist, kann darüber auch frei und unbefangen ohne Furcht vor nachteiligen Konsequenzen kommuniziert werden. Wegen der hohen Bedeutung freier Fernkommunikation für den Menschen und sein Zusammenleben einerseits und der besonders leichten Ausforschbarkeit von Fernkommunikation andererseits bedürfen ihre Voraussetzungen eines besonderen Schutzes.

Kommunikationsmittler sind keine beliebigen Unternehmen wie andere auch, sondern haben eine besondere Funktion in unserer Gesellschaft, die einen besonderen Schutz der Kommunikationsmittlern anvertrauten Informationen verlangt. Niemand würde von einem Rechtsanwalt oder Steuerberater die Auskunft verlangen, welches Geburtsdatum ein Mandant hat. Diese Daten könnten zwar bei jedem beliebigen Unternehmen vorliegen, sie unterliegen in besonderen Vertrauensverhältnissen aber aus gutem Grund einem besonderen Schutz, weil sonst die unbefangene Inanspruchnahme unentbehrlicher Leistungen nicht mehr gewährleistet wäre.

Es besteht noch ein weiterer Unterschied zu den Kundendaten anderer Unternehmen: Auf Fernkommunikation ist der Mensch heutzutage zwingend angewiesen. Er muss seine persönlichen Daten einem Kommunikationsmittler anvertrauen. Bei anderen Unternehmen hat er hingegen die Wahl, ob er seine Daten preisgibt, zumal Geschäfte des täglichen Lebens auch anonym in Läden und Supermärkten erledigt werden können. Teilweise schreibt der Staat die Nutzung von Fernkommunikation sogar vor, etwa im Fall von Gewerbesteuer-Voranmeldungen über das Internet.

Im Übrigen: Wo Personendaten tatsächlich auch bei jeder anderen Firma erhoben werden könnten, soll sie der Staat doch bei den anderen Firmen erheben. Wo der Bezug des staatlichen Informationsbedürfnisses zu einem

¹²⁰ BVerfG, Urteil vom 27.2.2008, Az. 1 BvR 370/07, Abs. 205.

konkreten Kommunikationsvorgang fehlt, besteht kein legitimes staatliches Interesse daran, Personendaten gerade von dem grundrechtlich besonders geschützten Kommunikationsmittler zu erheben.

(e) Schutzwürdigkeit der TK-Teilnehmeridentität im Vergleich zu Meldedaten und anderen Registern

Die Bundesregierung zieht zur Rechtfertigung des § 111 TKG eine Parallele zum deutschen Einwohnermelderecht, das ebenfalls eine Identifizierungspflicht aller Einwohner vorsieht. Der Vergleich ist schon deshalb verfehlt, weil die Vereinbarkeit der Einwohnermelderegeln mit der Menschenrechtskonvention ungeklärt ist. Deswegen kann auch die Ausgestaltung der Verarbeitungsregelungen nicht zur Rechtfertigung der vorliegend angegriffenen Normen heran gezogen werden (z.B. fehlende Eingriffsschwelle, automatisierter Abruf, fehlende Benachrichtigungspflicht). Es ist bekannt, dass Einwohnermeldedaten während des Dritten Reiches zu Massenverbrechen missbraucht worden sind. Nicht nur deshalb stellt sich die Frage, ob eine Meldepflicht erforderlich ist oder ob es – wie in vielen europäischen Staaten ohne Probleme praktiziert – genügt, dass jede Behörde die zur Erfüllung ihrer jeweiligen Aufgaben aktuell erforderlichen Daten speichert.

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

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

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

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

(3) Die mit § 111 Abs. 1 S. 3 ff. TKG verbundenen Risiken und Nebenwirkungen

Zur Prüfung der Verhältnismäßigkeit des § 111 Abs. 1 S. 3 ff. TKG ist nicht nur die hohe Bedeutung anonymer Telefon- und Internetanschlüsse in einer demokratischen Gesellschaft zu bedenken, sondern auch die negativen Auswirkungen eines Verbots anonymer Telefon- und Internetanschlüsse.

Im Fall S. und Marper verwarf der Europäische Menschenrechtsgerichtshof die Argumentation der britischen Regierung, die bloße Speicherung von Daten ohne ihre Nutzung könne sich auf die Betroffenen nicht nachteilig auswirken.¹²¹ Der Gerichtshof wies vielmehr darauf hin, dass bereits der Vorhaltung personenbezogener Informationen eine „unmittelbare Auswirkung auf das Interesse der betroffenen Person am Schutz ihrer Privatsphäre“ zukomme, selbst wenn von den Informationen keinerlei Gebrauch gemacht werde.¹²²

¹²¹ EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 121.

¹²² EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 121.

Ebenso zieht die § 111 TKG vorgesehene Vorratsdatenerhebung bereits konkrete Nachteile für die betroffenen Bürger nach sich, und zwar in folgender Hinsicht:

(a) Risiko des falschen Verdachts

Anonyme Kommunikationsanschlüsse schützen davor, Opfer eines falschen Verdachts zu werden. Eine generelle und undifferenzierte Vorratsdatenerhebung erhöht dagegen die allgemeine Gefahr, unschuldig einer Straftat oder Urheberrechtsverletzung verdächtigt zu werden:¹²³

Erstens beziehen sich Kommunikationsdaten stets nur auf den Inhaber eines Anschlusses. Wird der Anschluss von anderen Personen genutzt, dann kann der Inhaber leicht unschuldig in einen falschen Verdacht geraten. Nicht nur in Familie und Betrieb werden Internetanschlüsse gemeinsam genutzt.¹²⁴ Über offene WLAN-Funknetze oder Dienste wie TOR kann jeder Internetnutzer zum Internetanbieter für die Öffentlichkeit werden, ohne dass dies aus der genutzten Internetkennung hervor ginge und vor unbegründeten Ermittlungen schützte. Nur eine anonyme Kommunikationskennung bietet einen solchen Schutz.

Zweitens sind Kommunikationsdaten besonders anfällig für Ermittlungsfehler (z.B. Zahlendreher, Zeitstempel).¹²⁵ Der britische Interception of Communications Commissioner nennt insbesondere Fälle der Abfrage falscher Kommunikationskennungen und der Abfrage falscher Kommunikationszeitpunkte. Ursache können Zahlendreher bei Rufnummern oder IP-Adressen sein, aber auch technische Ungenauigkeiten oder Zeitonenprobleme bei der Verkehrsdatenspeicherung. Fehler unterlaufen sowohl bei Ermittlungsbehörden als auch bei Kommunikationsanbietern. Insgesamt registrierte der britische Interception of Communications Commissioner alleine im Jahr 2011 895 Fehler bei dem staatlichen Zugriff auf Kommunikationsdaten.¹²⁶ Wegen solcher Fehler wurden 2011 zwei unschuldige Menschen inhaftiert und beschuldigt.¹²⁷

Fehler treten auch bei der Kommunikationsdatenabfrage für private Zwecke der Rechtsverfolgung auf. Laut Verbraucherzentrale Bundesverband erhalten immer wieder Bürger, die weder Computer noch DSL-Router besitzen oder zum fraglichen Zeitpunkt nachweislich nicht im Netz waren, Abmahnungen wegen über ihren Internetanschluss angeblich begangener Urheberrechtsverletzungen.¹²⁸ Anonyme Kommunikationskennungen schützen vor falscher Verdächtigung.

Drittens 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 dem Opfer einer Straftat E-Mails geschickt 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.¹²⁹ Weil ein Kommunikationsdatensatz ein Indiz gegen den Angeklagten bilden kann, muss dieser unter Umständen den Richter von seiner Unschuld überzeugen, um nicht zu Unrecht verurteilt zu werden.¹³⁰ Mangels eines Alibis wird Unschuldigen die Erschütterung der Indizienkette keineswegs immer gelingen. Aber auch, wenn sich die Unschuld einer Person noch vor ihrer Verurteilung herausstellt, kann ein falscher Verdacht ausreichen, um zu Hausdurchsuchungen, Untersu-

¹²³ BVerfGE 107, 299 (321).

¹²⁴ Näher Breyer, NJOZ 2010, 1085.

¹²⁵ Arbeitskreis Vorratsdatenspeicherung, http://wiki.vorratsdatenspeicherung.de/images/Bericht_Sicherheit-vor-Sammelwut.pdf, 7.

¹²⁶ Interception of Communications Commissioner, 2011 Annual Report, <http://www.intelligencecommissioners.com/docs/0496.pdf>, 30.

¹²⁷ Interception of Communications Commissioner, 2011 Annual Report, <http://www.intelligencecommissioners.com/docs/0496.pdf>, 31.

¹²⁸ Verbraucherzentrale Bundesverband, Pressemitteilung vom 14.02.2012, <http://www.vzbv.de/8829.htm>.

¹²⁹ Hamm, TKÜV, 81 (86).

¹³⁰ Lisken/Denninger, Handbuch des Polizeirechte (2001), C 26.

chungshaft, Bewegungseinschränkungen oder Aus- und Einreiseverboten zu führen, was mit schwerwiegenden Belastungen für die Betroffenen verbunden ist.

Folgender Fall von Fehltritten aufgrund einer Analyse von Telekommunikationsdaten ist 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.¹³¹ Später stellte sich der Verdacht als unbegründet und der Nigerianer lediglich als gefragter Ratgeber in der schwarzen Gemeinschaft in Wien heraus.¹³²

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. Anonyme Kommunikationsanschlüsse schützen vor diesem besonderen Risiko falscher Verdächtigung.

(b) Risiko von Datenpannen und Missbrauch

Anonyme Kommunikationsanschlüsse schützen außerdem davor, Opfer von Datenpannen und Datenmissbrauch zu werden.

Die Erfassung und Vorhaltung von Informationen über alle Telekommunikationsteilnehmer schafft unvermeidbare Risiken eines gesetzwidrigen Missbrauchs dieser Informationen. Dass Kommunikationsdaten und Kundendaten immer wieder versehentlich verloren oder absichtlich zweckentfremdet werden, zeigen die Erfahrungen der Vergangenheit:

- 2005-2007 veranlassten die polnische Polizei und zwei große Geheimdienste, dass die Kommunikationsdaten von mindestens 10 Journalisten gespeichert wurden, um deren Quellen aufzudecken. Der Zugriff auf die Daten durch Polizei und Geheimdienste erfolgte ohne gerichtlichen Beschluss oder eine andere Legitimation, und die Ermittlungen waren nicht Teil eines laufenden Verfahrens.¹³³
- Ein Mitarbeiter des deutschen Bundesnachrichtendienstes, der mit der Überwachung der elektronischen Kommunikation betraut war, nutzte 2007 seine technischen Möglichkeiten privat. Er spähte den Email-Verkehr eines Deutschen aus, weil dieser ein Verhältnis mit der Ehefrau des BND-Mitarbeiters hatte.¹³⁴
- Ein tschechischer Polizist fragte 2009 und 2010 im Auftrag einer privaten Sicherheitsfirma und politischer Kreise illegal Handy-Verbindungsdaten und Standortdaten über Personen des öffentlichen Lebens ab. Die Liste der so Ausspionierten umfasste den Vorsitzenden des tschechischen Verfassungsgerichtes, Journalisten zweier Tageszeitungen, Geschäftsleute aus der Sicherheits-, Energie- und Rüstungsbranche sowie mehrere Spitzenpolitiker verschiedener Parteien – darunter Vertraute von Staatspräsident Václav Klaus.¹³⁵
- Eine 40-jährige irische Polizeibeamtin wurde 2010 versetzt, weil sie nach der Trennung von ihrem Exfreund unter Missbrauch ihres Amtes dessen Telefon-Verbindungs- und Standortdaten abgerufen haben soll, um ihm nachzuspionieren.¹³⁶ Die Beamtin war in der für Terrorismus und organisierte Kriminalität zuständigen Abteilung der Zentrale der irischen Polizei für Telekommunikationsüberwachung zuständig.

¹³¹ Kreml, 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.

¹³² Kreml, 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.

¹³³ The News.pl, Journalists' phones monitored in politically inspired investigation?, 8 October 2010, <http://www.the-news.pl/1/9/Artykul/5241,Journalists-phones-monitored-in-politically-inspired-investigation>.

¹³⁴ <http://www.berliner-zeitung.de/archiv/bka-reform---das-bundeskriminalamt-soll-per-gesetz-mehr-befugnisse-bei-der-terrorabwehr-bekommen--neue-fahndungsmethoden-sollen-die-jagd-auf-staatsfeinde-erleichtern--beamter-unter-verdacht,10810590,10501420.html>.

¹³⁵ http://www.pragerzeitung.cz/?c_id=17621.

¹³⁶ <http://www.webcitation.org/5xTUKdNqb>.

- In Großbritannien wurden 2007-2010 über 900 Disziplinarverfahren gegen Polizist/innen wegen des Verdachts der Verletzung des Datenschutzgesetzes geführt. 243 Beamte und Mitarbeiter der Polizei wurden wegen Datenschutzverletzungen strafrechtlich verurteilt, 98 wurden entlassen. Der Grund dafür war meist der Abruf polizeilicher Daten zu privaten Zwecken. Beispielsweise wurden polizeiliche Daten verwendet, um einem potenziellen Partner belästigende Nachrichten zu senden. Ausgeforscht wurden auch Exfrauen, Nachbarn und Arbeitskollegen von Polizist/innen.¹³⁷
- In Frankreich wertete der Inlandsgeheimdienst DCRI Verbindungsdaten aus, um die Quellen von Journalisten offenzulegen.¹³⁸ Zuvor hatte ein Staatsanwalt die Verbindungsdaten einer Richterin ausgewertet, um die Quellen investigativer Journalisten der Zeitung „Le Monde“ aufzudecken¹³⁹ – wiederum eine Verletzung des Quellenschutzes, wie ein Gericht später feststellte.¹⁴⁰

Daneben gab es zahllose Abhörskandale auch in Griechenland, Großbritannien, Italien, Portugal, der Slowakei und Slowenien.

In der letzten Zeit häufen sich in Deutschland zudem Fälle versehentlicher und absichtlicher Veröffentlichung und Zweckentfremdung von Informationen über Telekommunikations- und Internetnutzer. Beispielsweise mussten 18.000 Personen, die im Internet bei der Anzeigenblatt-Tochter WBV Wochenblatt des Axel Springer Verlages – zum Teil unter Chiffre – Anzeigen aufgegeben hatten, ihre Privatanschrift, E-Mail-Adresse, Handynummer und Kontodaten öffentlich zugänglich im Internet wieder finden.¹⁴¹ Das mit Diskretion werbende Erotikunternehmen Beate Uhse veröffentlichte die E-Mail-Adressen Tausender von Personen, die sich Sexfilme im Internet angesehen hatten.¹⁴² In einem Forum des ZDF-Kinderkanals konnten sich beliebige Personen Klarnamen, Adresse, Telefonnummer und Geburtsdatum aller 1.000 registrierter Kinder verschaffen.¹⁴³

Auch ein Fall des Verlustes von Teilnehmerdaten ist bekannt geworden: Im Jahr 2006 verkaufte ein Mitarbeiter von T-Mobile die Daten sämtlicher 17 Mio. Prepaid- und Postpaid-Kunden des Mobilfunkunternehmens. Die Daten umfassen den Namen, die Mobilfunknummer, die Anschrift, teils das Geburtsdatum und in einigen Fällen auch die E-Mail-Adresse. Die Daten wurden in kriminellen Kreisen zum Kauf angeboten. In den Daten fanden sich nach Angaben des Nachrichtenmagazins „Der Spiegel“ nicht nur viele Prominente aus Kultur und Gesellschaft, sondern auch eine erstaunliche Anzahl geheimer Nummern und Privatadressen von bekannten Politikern, Ministern, Ex-Bundespräsidenten, Wirtschaftsführern, Milliardären und Glaubensvertretern, für die eine Verbreitung ihrer Kontaktdaten in kriminellen Kreisen eine Gefährdung ihrer Sicherheit darstellte (etwa Charlotte Knobloch, Präsidentin des Zentralrats der Juden).¹⁴⁴ Das Bundeskriminalamt erstellte eine Gefährdungsanalyse, um Betroffene schützen zu können. Die Daten gelangten auch an die Moderation der Comedy-Sendung „Schmidt & Pocher“ in der ARD, die dies zum Anlass nahm, den Fernsehmoderator Günther Jauch vor laufender Kamera unter dessen Privatnummer anzurufen und öffentlich vorzuführen.¹⁴⁵ Zur Aufklärung des Datenlecks verletzte T-Mobile erneut das Fernmeldegeheimnis und überprüfte illegal Verbindungsdaten.¹⁴⁶

¹³⁷ http://www.bigbrotherwatch.org.uk/Police_databases.pdf.

¹³⁸ <http://www.sueddeutsche.de/medien/politische-affaeren-erschuettern-frankreich-staatsspionage-gegen-journalisten-1.1144365>.

¹³⁹ <http://www.oe24.at/welt/Sarkozy-droht-Spitzelaffaere/6900740>.

¹⁴⁰ <http://www.franceinfo.fr/france-justice-police-2011-05-06-affaire-woerth-bettencourt-l-enquete-du-procureur-courroye-sur-la-534584-9-11.html>.

¹⁴¹ Spiegel 43/2008 vom 20.10.2008, Seite 70.

¹⁴² Die Welt vom 04.09.2008: Beate Uhse verschlampt E-Mail-Adressen im Web, http://www.welt.de/welt_print/article2398543/Beate-Uhse-verschlampt-E-Mail-Adressen-im-Web.html.

¹⁴³ Spiegel Online vom 16.10.2008: Kika stellt Daten von Kindern ungeschützt ins Web, <http://www.spiegel.de/netzwelt/web/0,1518,584525,00.html>.

¹⁴⁴ Spiegel vom 04.10.2008, <http://www.spiegel.de/wirtschaft/0,1518,581938,00.html>.

¹⁴⁵ Sendung Nr. 22 vom 9. Oktober 2008, http://www.schmidt-news.com/showguide_schmidt-pocher2008.php.

¹⁴⁶ Heise Online vom 29.10.2008, <http://heise.de/-214133>.

Untersuchungen des ungarischen Datenschutzbeauftragten haben viele Fälle unzulässiger Datenverwendung durch Mobilfunkanbieter festgestellt, beispielsweise die rechtswidrige Verwendung von Kundendaten zu Werbezwecken, die Anfertigung rechtswidriger Kopien von Dokumenten und rechtswidrige Datensammlungen.¹⁴⁷

Einen wirksamen Schutz vor derartigen Datenpannen und Missbrauch ermöglichen alleine anonyme Kommunikationsanschlüsse.¹⁴⁸ Nur nicht gespeicherte oder nicht zuzuordnende Daten sind sichere Daten. § 111 TKG stellt diese Erkenntnis auf den Kopf und ist deshalb mit dem Wesen des Art. 8 EMRK unvereinbar.

Wegen der vielen Fälle von Datenmissbrauch sind nach einer Umfrage 80% der Bundesbürger „sehr besorgt“ um die Sicherheit ihrer Daten.¹⁴⁹ Eine deutliche Mehrheit der Bevölkerung fordert eine gesetzliche Stärkung des Datenschutzes.¹⁵⁰ 60% der Bürger sorgen sich, dass ihre Daten in die Hände Dritter gelangen könnten.¹⁵¹

53% der Deutschen haben im Internet schon einmal eine andere Identität verwendet.¹⁵² Jeder vierte Internet-Nutzer ist zum Schutz seiner Daten sogar immer oder vorwiegend unter Fantasienamen im Internet unterwegs.¹⁵³ Auf diese Weise wollen die Bürger einen Missbrauch ihrer Daten verhindern, Internetangebote anonym nutzen und sich dagegen wehren, dass unangemessen viele Daten abgefragt werden.¹⁵⁴

Diese Umfrage zeigt, dass es ein großes und berechtigtes Bedürfnis rechtstreuer Bürger nach Anonymität zum Zwecke des Selbstschutzes gibt. Dieser Selbstschutz wird durch den Identifizierungszwang des § 111 TKG unmöglich gemacht.

(c) Abschreckungswirkung

Da mit der generellen Identifizierbarkeit des elektronischen Kommunikations- und Informationsverhaltens notwendig das Risiko verbunden ist, dass dem Betroffenen aus dem Bekanntwerden seiner Kontakte und Interessen Nachteile entstehen können, entfaltet § 111 Abs. 1 S. 3 ff. TKG eine Abschreckungswirkung. Diese hält Menschen in bestimmten Situationen davon ab, sich über Telefon oder Internet zu informieren oder zu kommunizieren. Dies wiederum hat teilweise schwere Nachteile für Einzelpersonen und für unsere Gesellschaft insgesamt zur Folge. Dies belegen die deutschen Erfahrungen mit der Vorratsspeicherung von Kommunikationsdaten bei Telekommunikationsunternehmen.

Nach Umsetzung der Richtlinie 2006/24/EG zur Vorratsdatenspeicherung in Deutschland berichteten viele Menschen der Bürgerrechtsorganisation Arbeitskreis Vorratsdatenspeicherung, dass sie seit Inkrafttreten der Vorratsdatenspeicherung ihr Handy, E-Mail oder Internet seltener nutzten oder dass sie in ihrem privaten Umfeld solche Einschränkungen erlebten. Amina R. aus Niedersachsen teilt beispielsweise mit, sie schränke sich stark in der E-Mail-Kommunikation mit ihrer Familie in Marokko ein, weil sie befürchtet, durch ihre Kontakte in diesen Staat ver-

¹⁴⁷ Centre for Policy Research on Science and Technology of Simon Fraser University Vancouver, Privacy Rights and Prepaid Communications Services vom März 2006, <https://www.sfu.ca/cprost-old/docs/GowPrivacyRightsPrepaidCommServices.pdf>, 38.

¹⁴⁸ Gola/Klug/Reif, Datenschutz- und presserechtliche Bewertung der „Vorratsdatenspeicherung“ (2007), 38; Rusteberg, VBIBW 2007, 171 (175).

¹⁴⁹ Unisys-Umfrage vom 01.10.2008, <http://www.unisyssecurityindex.com/resources/reports/Germany%20security%20index%20Oct%201-08.pdf>.

¹⁵⁰ Emnid-Umfrage vom 02.06.2008, <http://www.presseportal.de/pm/13399/1204206/n24/rss>.

¹⁵¹ Microsoft, Umfrage vom Februar 2008, <http://www.daten-speicherung.de/?p=267>.

¹⁵² Norton Cybercrime Report 2010, https://us.norton.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_German-DataSheet_A4_Aug12.pdf.

¹⁵³ Fittkau und Maaß, Umfrage unter 121.233 deutschsprachigen Internet-Nutzern im Frühjahr 2009, <http://www.w3b.org/nutzerverhalten/furcht-vor-datenmissbrauch-beeinflusst-nutzerverhalten.html>.

¹⁵⁴ Fittkau und Maaß, Umfrage unter 121.233 deutschsprachigen Internet-Nutzern im Frühjahr 2009, <http://www.w3b.org/nutzerverhalten/furcht-vor-datenmissbrauch-beeinflusst-nutzerverhalten.html>.

dächtig zu erscheinen. Anna T. (Name geändert) ist Opfer sexuellen Missbrauchs und tauschte sich früher in entsprechenden Foren und Chatrooms aus. Seit anhand ihrer IP-Adresse ihre Identität ermittelt werden konnte, zog sie sich aus diesem Austausch zurück und hatte somit keine Möglichkeit mehr, sich mit anderen anonymen Opfern auszutauschen. In dieselbe Situation versetzt § 111 TKG Inhaber fester und mobiler Internetzugänge.

Eine Vorratsdatenerfassung schreckt weiters Informanten davon ab, vertrauliche Informationen per Telefon oder Internet an die Presse weiterzugeben, weil der Kontakt und ihre Identität jederzeit nachvollzogen werden kann. Ohne solche Informationen kann die Presse öffentliche Missstände nicht aufdecken und ihrer Kontrollfunktion gegenüber dem Staat nicht mehr nachkommen. Die Rundfunkjournalistin Hilde W. aus Thüringen schrieb dem Arbeitskreis Vorratsdatenspeicherung, sie recherchiere die Unterbringung von Flüchtlingen und Asylbewerbern in Thüringen, habe aber nach Inkrafttreten der Vorratsdatenspeicherung Probleme, telefonisch oder per E-Mail Auskunft über sensible Daten wie illegale Flüchtlinge, Namen und Adressen zu erhalten. Der Journalist Gerrit W. aus Nordrhein-Westfalen befasst sich im Rahmen seiner Arbeit unter anderem mit Menschenrechtsverletzungen der EU-Agentur Frontex. Schon in den ersten Wochen nach Inkrafttreten der Vorratsdatenspeicherung lehnten zwei Kontaktpersonen den Informationsaustausch via E-Mail ab. Der freiberufliche Journalist Peter H. aus Hessen schrieb, nach Inkrafttreten der Vorratsdatenspeicherung sei die Kommunikation mit Informanten aus Firmen, Behörden, Parteien, Stadtverwaltungen und sonstigen Institutionen erschwert, teilweise auch unmöglich geworden. Auch § 111 TKG führt zur Identifizierbarkeit sämtlicher Fernkommunikation und Internetnutzung über Privatanschlüsse. Er untergräbt dadurch den Schutz journalistischer Quellen und beschädigt die Pressefreiheit.

Kommunikationsstörungen sind auch im Bereich der wirtschaftlichen und rechtlichen Beratung die Folge einer totalen Nachvollziehbarkeit, wo oftmals schon der Kontakt zu einem – möglicherweise auf ein bestimmtes Gebiet wie Steuerstrafrecht spezialisierten – Berater vertraulich bleiben muss. So stellte der Steuerberater Matthias M. aus Baden-Württemberg bei einigen Mandanten fest, dass sie den Weg der Kommunikation über das Telefon nach Inkrafttreten des verfassungswidrigen Gesetzes zur Vorratsdatenspeicherung scheuten. Dies hielt er für sehr bedenklich, weil in der Vergangenheit immer wieder der Fall eingetreten war, dass Mandanten angefragt haben, ob diese oder jene steuerliche Gestaltung noch mit dem Steuerrecht konform ist. Solche Fälle konnte Herr M. häufig telefonisch mit einem kurzen Ja oder Nein beantworten und dem Mandant aufzeigen, dass es immer besser ist, auf dem ‚Pfad der Tugend‘ zu bleiben. Seine Befürchtung war, dass es Mandanten zu kompliziert oder zeitaufwendig wird, derartige Dinge jedes Mal persönlich zu klären und somit auch schneller der Fall eintreten kann, dass sich die Mandanten mangels Beratung strafbar machen. Der Rechtsanwalt und Notar Dr. Engelbert S. aus Hessen hat wegen der Vorratsdatenspeicherung Mandanten ernsthaft davor gewarnt, durch Telefon, Fax oder E-Mail mit ihm Kontakt aufzunehmen oder Schriftstücke zu übermitteln. Dies habe zu einem Rückgang von Anfragen geführt, weil persönliche Besuche mit höherem Aufwand verbunden sind. Der Wirtschafts- und Finanzberater Jens-Oliver W. berichtet, nach Inkrafttreten der Vorratsdatenspeicherung sei mit einigen Mandanten eine telefonische Kommunikation nicht mehr möglich gewesen. Vermutlich werde er diese Mandanten nicht mehr betreuen können, da die Wege- und Zeitaufwandskosten in keinem Verhältnis mehr zum Verdienst stehen. § 111 TKG zieht dieselben Nachteile nach sich, etwa wo Menschen keine wirtschaftliche und rechtliche Beratung ohne Furcht vor Rückverfolgung mehr in Anspruch nehmen können.

Der Betriebsrat Joachim B. aus Bayern berichtete, dass sich Mitarbeiter nach Inkrafttreten des Gesetzes zur Vorratsdatenspeicherung nicht mehr per E-Mail an ihn wendeten, obwohl einige arbeitsrechtlich relevante Fälle möglichst unverzüglich geklärt werden müssten. Von § 111 TKG gehen ähnliche Wirkungen auf die Arbeit von Betriebs- und Personalräten aus, soweit sie nicht mehr ohne Furcht vor Identifizierung privat angerufen werden können.

Torsten T. aus Hessen ist Firmeninhaber und schaltete sein Mobiltelefon nach Inkrafttreten der Vorratsdatenspeicherung ab, weil er befürchtete, mit Straftaten in Verbindung gebracht zu werden, in deren Nähe er zufällig telefoniert hat. Die Deaktivierung des Mobiltelefons schade ihm jedoch wirtschaftlich. Ein ähnlicher Schaden geht von § 111 TKG aus, wo Menschen auf Telekommunikation möglichst verzichten, um ihre Kommunikation nicht dem Risiko der Rückverfolgbarkeit auszusetzen.

Schließlich sind Menschen in besonderen Situationen (z.B. Notlagen, Krankheiten) zur Suche nach Informationen, zur Inanspruchnahme von Beratung und Hilfe sowie zum Austausch untereinander (z.B. Chatrooms für Opfer sexuellen Missbrauchs) nur bereit, wenn dies anonym und nicht rückverfolgbar möglich ist. Oftmals lässt sich bereits aus dem Kontakt zu einer bestimmten Beratungsstelle oder zu einem bestimmten Arzt auf die zugrunde liegende Erkrankung, Abhängigkeit o.ä. schließen. Der Sozialpädagoge und Suchtberater Konstantin H. aus Schleswig-Holstein berichtete, in der niedrigschwelligen Arbeit mit Drogenabhängigen sei die Zahl der telefonischen Kontakte seit der in Deutschland zum 1.1.2008 aufgenommenen Vorratsdatenspeicherung „stark zurückgegangen“. Die Abhängigen fürchteten eine Strafverfolgung. Durch die Personalstruktur in der Beratungsstelle – ein Berater müsse 200 Klienten betreuen – sei eine andere als telefonische Beratung oft nicht möglich; zudem bedürften die Klienten aufgrund von Begleiterkrankungen wie Hepatitis oftmals akuter medizinischer Behandlung. Der Rückgang der telefonischen Beratungsanfragen könne den Gesundheitszustand der Betroffenen sehr verschlechtern. Der Facharzt Achim R., der in einem Berliner Klinikum arbeitet, berichtete von mehreren Patienten, die nach Inkrafttreten der Vorratsdatenspeicherung von telefonischen Kontaktaufnahmen zwecks Beratung abgesehen hätten, wodurch medizinisch gefährliche Verzögerungen des Therapiebeginns entstanden seien. Beispielsweise habe sich die Behandlung einer Tumorerkrankung verzögert und sei der Tumor in der Zwischenzeit weiter gewachsen. Die Psychotherapeutin Cornelia P. aus Baden-Württemberg hat im Monat nach Inkrafttreten der Vorratsdatenspeicherung nahezu keine Anfragen per E-Mail oder Telefon nach Paartherapie, Eheberatung und Psychotherapie mehr erhalten. Auch § 111 TKG macht es Menschen in besonderen Situationen (z.B. Notlagen, Krankheiten) unmöglich, ohne Furcht vor Bekanntwerden ihrer Situation im Internet nach Informationen zu suchen, Beratung und Hilfe in Anspruch zu nehmen oder sich mit anderen Menschen in ähnlicher Situation auszutauschen (z.B. Chatrooms für Opfer sexuellen Missbrauchs). Der Staat bietet Menschen in besonderen Situationen (z.B. Notlagen, Krankheiten) teilweise selbst Informationen, Beratung und Hilfe über Hotlines und im Internet an, die wegen § 111 TKG jedoch nicht mehr ohne das Risiko eines Bekanntwerdens in Anspruch genommen werden kann.

(d) Meinungsumfragen belegen Abschreckungswirkung

Um einen repräsentativen Überblick über die Auswirkungen einer generellen Nachvollziehbarkeit des Kommunikationsverhaltens zu gewinnen, ist eine repräsentative Umfrage des Meinungsforschungsinstituts Forsa unter 1.002 Bundesbürgern am 27./28. Mai 2008 in Auftrag gegeben worden.¹⁵⁵ Dem Umfrageergebnis zufolge würde die Mehrheit der Befragten wegen der damals praktizierten Vorratsdatenspeicherung davon absehen, per Telefon, E-Mail oder Handy Kontakt zu einer Eheberatungsstelle, einem Psychotherapeuten oder einer Drogenberatungsstelle aufzunehmen, wenn sie deren Rat benötigten (517 der Befragten). Hochgerechnet entspricht dies über 43 Mio. Deutschen. Jede dreizehnte Person gab an, wegen der Verbindungsdatenspeicherung bereits mindestens einmal darauf verzichtet zu haben, Telefon, Handy oder E-Mail zu benutzen (79 der Befragten). Hochgerechnet entspricht dies 6,5 Mio. Deutschen. Jede sechzehnte Person hatte den Eindruck, dass andere Menschen seit Beginn der Vorratsdatenspeicherung seltener per Telefon, Handy oder E-Mail Kontakt mit ihr aufnehmen (62 der Befragten). Hochgerechnet entspricht dies 5 Mio. Deutschen. Besonders stark war die Veränderung des Kommunikationsverhaltens unter Menschen mit geringem Bildungsniveau (Haupt- oder Grundschulabschluss).

Des Weiteren gab der Deutsche Fachjournalistenverband eine Online-Befragung (Vollerhebung) freier Journalisten in Auftrag, die vom 8. bis 27. April 2008 durchgeführt wurde.¹⁵⁶ Es nahmen 1.630 freie Journalisten teil. Jeder vierzehnte Journalist erklärte, die Vorratsdatenspeicherung habe sich bereits negativ auf die Kommunikation mit seinen Informanten ausgewirkt. Jeder fünfte hielt abschreckende Auswirkungen der Vorratsdatenspeicherung zumindest für möglich.¹⁵⁷

Die genannten Umfragen weisen nach, dass von einer generellen und undifferenzierten Vorratsdatenspeicherung und dem ihr inhärenten Risiko einer Offenlegung oder Auswertung der protokollierten Informationen schwere Nach-

¹⁵⁵ http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf.

¹⁵⁶ Meyen/Springer/Pfaff-Rüdiger, Freie Journalisten in Deutschland, http://www.dfjv.de/fileadmin/user_upload/pdf/DFJV_Studie_Freie_Journalisten.pdf.

¹⁵⁷ a.a.O., 22.

teile ausgehen, unabhängig von der Frage, ob auf die Daten später tatsächlich zugegriffen wird oder nicht. Viele Menschen können wegen auch § 111 TKG in bestimmten Situationen bereits auf Kontaktaufnahmen verzichtet haben, weil sie etwaige Nachteile infolge der Identifizierbarkeit des Kontakts nicht verhindern können. Tausende von Journalisten und Berufsgeheimnisträger werden in ihrer beruflichen Tätigkeit durch die globale Protokollierung sämtlicher elektronischer Kontakte gestört. Jede zweite Person würde im Fall der Hilfsbedürftigkeit keine Hilfe über Telefon oder Internet mehr in Anspruch nehmen. Es liegt auf der Hand, dass in vielen dieser Fälle auch eine persönliche Kontaktaufnahme zu einer Hilfseinrichtung unterbleiben wird und dass daraus – etwa in Fällen von Gewaltproblemen – Gesundheits- und Lebensgefahren für die Betroffenen und ihre Mitmenschen erwachsen können.

Eine Untersuchung 38 afrikanischer Staaten hat festgestellt, dass die Einführung einer Identifizierungspflicht zu einem Rückgang der Zahl aktiver Mobiltelefonanschlüsse führte und dass die Verbreitung von Mobiltelefonie auch in den Folgejahren langsamer zunahm als ohne Identifizierungszwang.¹⁵⁸ Auch diese Zahlen weisen auf einen kommunikationshindernde Wirkung eines Anonymitätsverbots hin.

Im Fall S. und Marper argumentierte der EGMR, die Vorratsspeicherung biometrischer Daten sei im Fall besonderer Personengruppen besonders schädlich, namentlich im Fall von Minderjährigen.¹⁵⁹ Wie oben gezeigt, ist auch die Nachvollziehbarkeit von Telekommunikation für bestimmte Personengruppen besonders schädlich (z.B. Personen in Not, Journalisten, Berater). Außerdem wird gewarnt, dass eine Identifizierungspflicht für Mobiltelefonkarten sozial Benachteiligte wie Obdachlose, Einwanderer und Menschen mit schlechter Bonität besonders hart trifft, weil diese auf solche Karten oftmals angewiesen sind.¹⁶⁰

(e) Verletzung der Unschuldsvermutung

Im Fall S. und Marper leitete der EGMR aus dem Grundgedanken der Unschuldsvermutung ab, dass Nichtverurteilte einen Anspruch darauf hätten, nicht ebenso wie verurteilte Straftäter behandelt zu werden. In einer solchen Gleichbehandlung von Ungleichem liege eine Stigmatisierung der Betroffenen.¹⁶¹

Dasselbe gilt für § 111 TKG. Nach dieser Vorschrift wird nicht nur das Kommunikationsverhalten Verdächtiger identifizierbar, sondern sogar das Kommunikationsverhalten gänzlich Unverdächtiger und Unbeteiligter. Rechtschaffene Bürger haben aber einen Anspruch darauf, nicht allesamt wie potenziell Verdächtige einer Straftat behandelt zu werden. Nur bei dem Verdacht einer Straftat darf der Staat die Erfassung von Informationen über Telekommunikationsteilnehmer anordnen, nicht aber generell und undifferenziert.

(f) Drohender Dambruch

Die Maßstäbe, die das Bundesverfassungsgericht im vorliegenden Verfahren entwickelt, werden auch in anderen Bereiche angewandt werden. § 111 TKG stellt einen Präzedenzfall für eine immer weiter reichende vorsorgliche staatliche Identifizierung menschlichen Verhaltens dar. Diese Entwicklung droht schrittweise zu einem gläsernen Bürger zu führen, wenn nicht strenge Anforderungen zum Schutz der Privatsphäre der Bürger aufgestellt werden.

Die Zulassung eines Anonymitätsverbots und einer Ausweispflicht im Fall des § 111 TKG würde allgemein einen Dambruch für den Schutz der Privatsphäre bedeuten. Der Zwang zur anlasslosen Erfassung und Verifizierung der Identität allein für eine mögliche künftige staatliche Verwendung würde allmählich alle Lebensbereiche erfassen, denn sie ist für den Staat stets und in allen Bereichen nützlich.¹⁶² Aus jedem personenbezogenen Datum können sich im Einzelfall einmal Schlüsse bezüglich einer Gefahr oder Straftat ergeben. Das Grundrecht auf Achtung

¹⁵⁸ Jentzsch, Implications of Mandatory Registration of Mobile Phone Users in Africa von 2012, https://www.diw.de/documents/publikationen/73/diw_01.c.394079.de/dp1192.pdf, 19.

¹⁵⁹ EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 124.

¹⁶⁰ Centre for Policy Research on Science and Technology of Simon Fraser University Vancouver, Privacy Rights and Prepaid Communications Services vom März 2006, <https://www.sfu.ca/cprost-old/docs/GowPrivacyRightsPrepaidCommServices.pdf>, 55.

¹⁶¹ EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 122.

¹⁶² Klug/Reif, RDV 2008, 89 (93).

der Privatsphäre und das gesamte Datenschutzrecht beruhen indes auf dem Gedanken, dass nicht bereits die bloße Möglichkeit, dass ein Datum irgendwann in der Zukunft einmal gebraucht werden könnte, dessen Speicherung rechtfertigt, weil ansonsten sämtliche personenbezogene Daten unbegrenzt auf Vorrat gespeichert werden dürften. Dies aber wäre eine unverhältnismäßige und unangemessene Beeinträchtigung des Persönlichkeitsrechts der Betroffenen, denen aus der Aufbewahrung und späteren Verwendung personenbezogener Daten schwere Nachteile entstehen können.

Mit der Aufgabe des Verbots einer anlasslosen, permanenten oder flächendeckenden Erhebung und Speicherung personenbezogener Daten auf Vorrat würden letztlich das gesamte Grundrecht auf Datenschutz und ihm folgend das gesamte Datenschutzrecht obsolet. Denn die Grundidee des Datenschutzes liegt gerade darin, die informationelle Selbstbestimmung zum Regelfall und den staatlichen Eingriff gegen den Willen des Betroffenen zum Ausnahmefall zu definieren. Die Pflicht des § 111 TKG zur generellen Vorratsdatenerhebung verkehrt die Grundidee der informationellen Selbstbestimmung in ihr Gegenteil.

Wenn eine flächendeckende Erfassung der Identität ins Blaue hinein selbst bei der besonders sensiblen und geschützten Telekommunikation und Internetnutzung zulässig wäre, wäre sie auch überall sonst zulässig. Der Staat könnte Büchereien, Geschäfte, Freizeiteinrichtungen, Vereine, Cafés, die Post usw. allesamt verpflichten, die Identität jedes Kunden immer und überall zu erfassen, zu überprüfen und festzuhalten. Ein solcher Staat wäre nicht der freiheitliche und demokratische Rechtsstaat, wie ihn die Menschenrechtskonvention ausweislich ihrer Präambel garantieren will.

Der Bevollmächtigte der Bundesregierung hat im Vorverfahren tatsächlich argumentiert, der Staat dürfe Informationen überall dort erheben, wo er sie finden könne, selbst wenn die Betroffenen vollkommen unverdächtig, ungefährlich und unbeteiligt seien.¹⁶³ Die diesbezüglichen Ausführungen des Bevollmächtigten der Bundesregierung machen deutlich, welche Konsequenzen es hätte, eine allgemeine Identifizierungspflicht vor den Grundrechten bestehen zu lassen. Denn dann wären in der Tat, wie der Bevollmächtigte der Bundesregierung bereits heute wahr wähnt,¹⁶⁴ die Kategorien „verdächtig – unverdächtig“ und „Nähebeziehung – Unbeteiligter“ obsolet. Dann könnte in allen Bereichen des öffentlichen Lebens ein Identifizierungszwang und eine Vorratsspeicherungspflicht eingeführt werden, um die lückenlose staatliche Überwachung der Bürger zu ermöglichen.

Abgesehen von Sondergebieten wie dem Bereich finanzieller Transaktionen (Geldwäschegesetz) ist eine staatlich angeordnete Identifizierungs- und Ausweispflicht im deutschen Recht bisher einmalig. Selbst auf dem Gebiet des Zahlungsverkehrs gewährleistet Bargeld unser Recht auf Anonymität im Alltag bislang. § 111 TKG macht dagegen eine anonyme Telekommunikation selbst durch Privatpersonen in weiten Bereichen unmöglich. Hinzu kommt, dass der bargeldlose Zahlungsverkehr nicht annähernd so grundrechtsrelevant ist wie die freie Telekommunikation und Internetnutzung: Nur die freie Information und Kommunikation der Bürger ist heutzutage Grundvoraussetzung für die Ausübung mehrerer Grundrechte (z.B. Art. 5 GG) und für die unbefangene Mitwirkung der Bürger in einem demokratischen Staat.

Das Bundesverfassungsgericht hat eine anlasslose Vorratsspeicherung aller Verbindungs- und Bewegungsdaten sinngemäß mit dem Argument verteidigt, elektronische Kommunikationsspuren seien besonders flüchtig.¹⁶⁵ Dieses Argument ist auf einen generellen Identifizierungszwang aber nicht übertragbar. Hier geht es gerade nicht darum, die Löschung flüchtiger Datenspuren zu verhindern, sondern zusätzliche Informationen überhaupt erst zu gewinnen. Eine „Vorratsdatengewinnung“ weist gegenüber einer bloßen Aufbewahrung vorhandener Informationen nochmals eine neue Qualität auf: Mit § 111 Abs. 1 S. 1 und Abs. 2 S. 1 TKG will der deutsche Gesetzgeber die Kommunikationsvermittlung erstmals zur Gewinnung zusätzlicher Informationen instrumentalisieren.

¹⁶³ Stellungnahme des Bevollmächtigten der Bundesregierung vom 31.01.2007, <http://datenspeicherung.de/data/TKG-StN.pdf>, 65.

¹⁶⁴ Stellungnahme des Bevollmächtigten der Bundesregierung vom 31.01.2007, <http://datenspeicherung.de/data/TKG-StN.pdf>, 65 f. und 91 f.

¹⁶⁵ Vgl. BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 260.

Nach dem Willen des Bundesverfassungsgerichts sollte seine Entscheidung zur Vorratsspeicherung von Verkehrsdaten auf andere Datensammlungen nicht übertragen werden. Die Verkehrsdatenspeicherung sollte eine „Ausnahme“ bleiben.¹⁶⁶ Die Entscheidung über § 111 TKG gibt diesen Vorsatz jedoch bereits wieder auf und hält fest, „vorsorgliche Datensammlungen [könnten] als Grundlagen vielfältiger staatlicher Aufgabenwahrnehmung ihre Berechtigung“ haben.¹⁶⁷ Hier wird der drohende Dammbbruch offenbar. Erklärte das Gericht das Verbot anonymer Telefon- und Internetanschlüsse für gerechtfertigt, würde es schrittweise dazu kommen, dass alle für die Strafverfolgung oder Gefahrenprävention nützlichen Daten vorsorglich erfasst werden.¹⁶⁸

Noch stärker als bei einer „Vorratsdatenspeicherung“ wohnte der Zulassung einer „Vorratsdatengewinnung“ die Gefahr inne, dass sie auf immer weitere Lebensbereiche übergreift. Würde der Identifizierungszwang für Inhaber von Telekommunikationsanschlüssen mit der heutigen Bedeutung der Telekommunikation gerechtfertigt, so würde schon bald die heutige Bedeutung des Reiseverkehrs, des elektronischen Geschäftsverkehrs oder sonstigen Alltagsverhaltens herangezogen, um die Identifizierung der gesamten Bevölkerung bei alltäglichen Verrichtungen zu erzwingen. Auf diese Weise entstünde eine grundlegend andere als die freiheitliche Gesellschaft, die den Verfassern des Grundgesetzes vor Augen stand.

cc) Abwägung

Verhältnismäßig ist ein Grundrechtseingriff nur, wenn er einen legitimen Zweck verfolgt und seine Belastungsintensität nicht außer Verhältnis zu dem Gewicht des damit verfolgten Zwecks steht. Die nachteiligen Auswirkungen des Eingriffs dürfen nicht schwerer wiegen als die zur Rechtfertigung des Eingriffs angeführten Gründe.

(1) Übertragbarkeit des Urteils in Sachen S. und Marper

Dass § 111 TKG das Grundrecht auf Achtung der Privatsphäre (Art. 8 EMRK) verletzt, ergibt sich aus dem Urteil der Großen Kammer des Europäischen Gerichtshofs für Menschenrechte vom 04.12.2008.¹⁶⁹ In diesem Urteil hat der Gerichtshof ausgeführt:

„In conclusion, the Court finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society.“¹⁷⁰

Der Gerichtshof hat also die „flächendeckende und unterschiedslose Natur der Befugnisse zur Vorratsspeicherung der Fingerabdrücke, Zellproben und DNA-Profile“ Verdächtiger als „unverhältnismäßigen Eingriff in das Recht des Beschwerdeführers auf Achtung seiner Privatsphäre“ bezeichnet und die entsprechende Eingriffsbefugnis des englischen Rechts als grundrechtswidrig verworfen. Er hat dabei wohlgemerkt nicht auf die Dauer der Speicherung abgestellt, sondern auf die „flächendeckende und unterschiedslose Natur der Befugnisse“, wie sie auch bei § 111 TKG gegeben ist.

Im Vergleich zu der vom Gerichtshof verworfenen Vorratsspeicherung von Fingerabdrücken greift § 111 TKG sogar noch weit tiefer in unser Recht auf Achtung der Privatleben ein.

Erstens ist § 111 TKG quantitativ weit eingriffsintensiver:

- a) Während die englische Befugnis nur Personen betraf, die einer Straftat verdächtig waren, betrifft § 111 TKG jeden Menschen, der einen Festnetz-, Mobilfunk- oder Internetanschluss hat. In Großbritannien waren einige Mil-

¹⁶⁶ BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 218.

¹⁶⁷ BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 138.

¹⁶⁸ BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 218.

¹⁶⁹ EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 66 ff.

¹⁷⁰ EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 125.

tionen von Personen von einer Speicherung ihrer biometrischen Daten betroffen. Von § 111 TKG sind demgegenüber praktisch alle 70 Mio. Volljährige in Deutschland betroffen.

- b) In der englischen Datensammlung waren von jedem Verdächtigen bis zu drei Angaben gespeichert: Fingerabdruck, Gewebeprobe und DNA-Profil. Über § 111 TKG wird demgegenüber alltägliches Telekommunikations- und Informationsverhalten identifizierbar. Es handelt sich um eine weitaus größere Menge an Informationen. Anhand biometrischer Merkmale lässt sich menschliches Verhalten nur punktuell rekonstruieren. Anhand der Teilnehmeridentität ist dagegen eine massenhafte Auswertung von Daten über das tägliche Informations- und Kommunikationsverhalten möglich.

Zweitens ist § 111 TKG auch qualitativ weit eingriffsintensiver:

- a) Die in England gesammelten biometrischen Informationen konnten zur Identifizierung Verdächtiger verwendet werden; im Fall von Gewebeproben und DNA-Profilen auch zur Gewinnung von Informationen über Herkunft und Krankheiten. Die unter § 111 TKG gesammelten und ausgewerteten Informationen erlauben demgegenüber nicht nur eine Identifizierung von Bürgern, sondern die Überwachung deren alltägliches Kommunikations-, Informations- und Bewegungsverhaltens. Verkehrs- und Internetnutzungsdaten können Rückschlüsse auf unsere sozialen Kontakte, auf unseren Tagesablauf, auf unsere Interessen und – anhand der Kommunikationspartner – teilweise auch auf sensible Informationen wie unsere Krankheiten (Information bei der Bundeszentrale für gesundheitliche Aufklärung), unsere Herkunft, unser Sexualleben oder politische Einstellungen zulassen. Sie können einen erheblichen Teil der Persönlichkeit und des privaten und beruflichen Lebens von Menschen offen legen. Sie weisen damit einen unvergleichlich höheren Aussagegehalt auf als biometrische Merkmale zur Identifizierung von Personen, wie sie in England erfasst worden waren. § 111 TKG macht eine Telekommunikation und Internetnutzung im Schutz der Anonymität für Normalbürger auf Dauer praktisch unmöglich.
- b) Während in England nur Personen, die einer Straftat verdächtig waren, biometrische Merkmale abgenommen wurden, trifft § 111 TKG sogar Menschen, die nie auch nur im Verdacht einer Straftat gestanden haben. Selbst der rechtstreueste Bürger kann die Erfassung seines Kommunikations- und Bewegungsverhaltens infolge § 111 TKG nicht vermeiden.

Verletzt nach der Entscheidung des Europäischen Gerichtshofs für Menschenrechte die Sammlung biometrischer Daten aller Verdächtiger das Verhältnismäßigkeitsgebot, so tut es die generelle Identifizierbarkeit des Kommunikations-, Informations- und Bewegungsverhaltens der gesamten (auch unverdächtigen) Bevölkerung erst Recht.

In dem Fall S. und Marper hat der Gerichtshof zutreffend die von der britischen Regierung vorgelegten Statistiken über die Zahl der erfolgreichen Abrufe aus der Datenbank hinterfragt. Er hat kritisiert, dass die Zahl der erfolgreichen Abrufe keinen Aufschluss darüber gebe, in wie vielen Fällen ein erfolgreicher Abruf auch tatsächlich zur Verurteilung eines Straftäters geführt habe.¹⁷¹ Auch sei nicht dargelegt, in wie vielen Fällen hierfür gerade die Vorratsspeicherung der Daten Nichtverurteilter erforderlich gewesen sei.¹⁷² Die meisten der von der Regierung genannten erfolgreichen Abrufe wären auch ohne die beanstandete Vorratsspeicherung möglich gewesen.¹⁷³ Wenngleich der Gerichtshof im Ergebnis davon ausging, dass die Vorratsspeicherung biometrischer Daten aller Tatverdächtiger einen gewissen Beitrag zur Strafverfolgung leistete,¹⁷⁴ verwarf er sie gleichwohl als unverhältnismäßig weitgehend.

Nichts anderes gilt auch für die in § 111 TKG vorgesehene generelle und undifferenzierte Identifizierung und Registrierung sämtlicher privater Telekommunikations- und Internetanschlusshaber. Aus der Zahl der staatlichen Zugriffe auf Kundendaten ergibt sich nicht, ob und in wie vielen Fällen dies auch tatsächlich zur Bestrafung einer Straftat oder Abwehr einer Gefahr geführt hat. Vor allem ergibt sich aus der Zugriffsstatistik nicht, in wie vielen Fäl-

¹⁷¹ EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 116.

¹⁷² EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 116.

¹⁷³ EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 116.

¹⁷⁴ EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 117.

len dazu gerade die anlasslose und flächendeckende Identifizierung erforderlich gewesen sei und betrieblich gespeicherte Daten oder andere Ermittlungsinstrumente nicht ausgereicht hätten.

Wie oben dargelegt, ist ein messbarer Beitrag gerade des § 111 TKG zum Rechtsgüterschutz nicht feststellbar. Selbst wenn man unterstellte, dass die Vorschrift einen gewissen Beitrag leistete, greift ein flächendeckendes und permanentes Verbot anonymer Information und Kommunikation über Privatanschlüsse doch unverhältnismäßig weit in die Rechte auf Achtung der Privatsphäre und der Vertraulichkeit der Fernkommunikation ein. Selbst die (unterstellte) Verurteilung einzelner sonst nicht überführbarer Straftäter rechtfertigte in einem demokratischen Staat nicht die unterschiedslose Eliminierung anonymer Informations- und Kommunikationskanäle für die gesamte Bevölkerung. In Deutschland werden jährlich ca. 6 Mio. Straftaten registriert, von denen ca. 3,3 Mio. Taten aufgeklärt werden und ca. 2,7 Mio. Straftaten nicht. In einer demokratischen Gesellschaft ist nie jede Straftat aufklärbar und darf dies auch nie um jeden Preis angestrebt werden.

Das Grundgesetz verlangt vom Gesetzgeber, zwischen dem Rechtsgüterschutz und den Auswirkungen auf die Grundrechte der Betroffenen einen angemessenen Ausgleich herzustellen. An einem solchen rechtsstaatlichen Ausgleich fehlt es hier. Mit einer globalen und pauschalen Identifizierung wird dem öffentlichen Anliegen, Rechtsgüter zu schützen, kaum Rechnung getragen, aber jedenfalls zu einseitig der Vorrang gegenüber den berechtigten Interessen der Kommunizierenden und sich Informierenden an der Wahrung ihrer Privatsphäre und an unbefangener Information und Kommunikation eingeräumt.

Anonyme Telekommunikation generell ausschließen zu wollen, selbst wenn der Anschlussinhaber nicht einmal entfernt in Verbindung zu einer Straftat oder Gefahr steht, setzt das staatliche Identifizierungsinteresse absolut und macht legitime Anonymität unmöglich. Dies gleicht die wechselseitigen Interessen nicht aus, sondern soll einer absoluten Identifizierbarkeit und Nachverfolgbarkeit elektronischer Kommunikation und Bewegungen dienen.

Internet-Kommunikationsdienste wie Whatsapp können Telefonate in vielen Fällen nicht ersetzen. Außerdem fallen bei ihren Anbietern vielfach Daten an, die sich auf den genutzten Anschluss zurückführen lassen (z.B. IP-Adresse). Internetdienste sind deshalb kein Ersatz für anonyme Telefonie und Internetzugang.

(2) Übertragbarkeit der EuGH-Rechtsprechung zur Vorratsdatenspeicherung

Der EuGH hat Pflichten zur Vorratsspeicherung von Verkehrs-, aber auch von Bestandsdaten als unverhältnismäßig verworfen, wenn sie wahllos für alle Bürger gelten und nicht auf Personen beschränkt sind, die in einer Nähebeziehung zu Straftaten oder Gefahren stehen. Die EU-Richtlinie zur Vorratsdatenspeicherung galt ausdrücklich auch für Bestandsdaten, nämlich unter anderem für Anschlusskennung, Name und Anschrift des Anschlussinhabers. Der EuGH hat sie auch insoweit verworfen und in seinem Urteil mehrfach neben den Verkehrsdaten auch die Teilnehmeridentität angesprochen.

Ist die verdachtslose Vorratsspeicherung der Identität aller Anschlussinhaber aber unverhältnismäßig und europarechtswidrig, so muss dies erst Recht für die Erhebung und Verifizierung der Identität aller Anschlussinhaber auf Vorrat gelten.

Sollte das Bundesverfassungsgericht daran Zweifel haben, mag eine Vorabentscheidung des EuGH eingeholt werden.

Soweit das Bundesverfassungsgericht mit Urteil vom 2. März 2010 eine anlasslose, flächendeckende Vorratsdatenspeicherung unter bestimmten Voraussetzungen noch als verhältnismäßig angesehen hat, kann dies heute nicht mehr überzeugen. Dem Urteil fehlte eine Auseinandersetzung mit den empirischen Nachweisen des eklatanten Missverhältnisses zwischen Tragweite einer Vorratsdatenspeicherung auf der einen und ihrem Ertrag auf der anderen Seite. Auch fehlte eine Auseinandersetzung mit den Belegen für die ebenso hohe Aufklärungsrate ohne Vorratsdatenspeicherung. Das Urteil setzte sich ferner nicht mit der Europäischen Menschenrechtskonvention und der diesbezüglichen Rechtsprechung des EGMR¹⁷⁵ und nationaler Verfassungsgerichte auseinander, obwohl das Grundgesetz nach Möglichkeit konventionskonform auszulegen ist.¹⁷⁶ Dem Urteil fehlt auch eine Auseinandersetzung

¹⁷⁵ EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, NJOZ 2010, 696.

¹⁷⁶ BVerfG, 2 BvR 1481/04 vom 14.10.2004, Absatz-Nr. 32.

zung mit der früheren Rechtsprechung des Bundesverfassungsgerichts, mit welcher eine allumfassende, permanente Vorratsdatenspeicherung nicht in Einklang zu bringen ist.¹⁷⁷ Die Entscheidung ist dementsprechend vom Bundesdatenschutzbeauftragten¹⁷⁸ und in der Literatur¹⁷⁹ kritisiert worden.

(3) Mangelnde Übertragbarkeit des Urteils in Sachen K.U. vs. Finnland

Soweit der EGMR in einer Kammerentscheidung Finnland verurteilt hat, weil dessen Gesetze im Jahr 1999 die Aufklärung einer im Internet begangenen Straftat nicht zuließen,¹⁸⁰ steht dies der Unverhältnismäßigkeit einer generellen und undifferenzierten Identifizierungspflicht nicht entgegen, weil diese Entscheidung eine andere Fallgestaltung betraf:

In jenem Fall verfügte der finnische Internetanbieter über Daten, die eine Identifizierung des mutmaßlichen Täters ermöglicht hätten,¹⁸¹ das finnische Recht erlaubte die Herausgabe dieser Daten aber nicht.¹⁸² Der Gerichtshof hat mit seiner Entscheidung beanstandet, dass das finnische Recht einen Zugriff auf ohnehin vorhandene Daten selbst zur Aufklärung einer vom Gerichtshof als schwer angesehenen Straftat (sexuelle Verleumdung eines Kindes in der Öffentlichkeit, welche das Kind der Gefahr sexueller Übergriffe aussetzte) nicht zuließ.

Dass der Staat zur Aufklärung schwerer Straftaten auf ohnehin zu betrieblichen Zwecken gespeicherte Daten zugreifen darf, steht hier nicht in Frage. Der Gerichtshof hat in der genannten Entscheidung demgegenüber nicht gefordert oder zugelassen, zur Aufklärung möglicher zukünftiger Straftaten oder Abwehr möglicher zukünftiger Gefahren rein vorsorglich die Identität sämtlicher Teilnehmer auf Vorrat erfassen zu lassen.

Gegen diese Annahme spricht auch die Anmerkung des Gerichtshofs, wonach Finnland das „Defizit“ in seinem Prozessrecht in einem späteren „Gesetz über die Ausübung der Meinungsfreiheit in Massenmedien“ angegangen sei.¹⁸³ Dieses Gesetz sah eine Befugnis zur Identifizierung von Kommunikationsteilnehmern auf richterliche Anordnung vor,¹⁸⁴ nicht jedoch eine anlasslose und flächendeckende Identifizierungspflicht, die es in Finnland bis heute nicht gibt.

(4) Weitere Rechtsprechung

Das Bundesverfassungsgericht hat entschieden, dass allgemein gesteigerte Risiken von Rechtsgutgefährdungen oder –verletzungen („allgemeine Bedrohungslage“) Grundrechtseingriffe von erheblichem Gewicht nicht rechtfertigen, sondern „eine konkrete Gefahr für hochrangige Rechtsgüter“ gegeben sein muss.¹⁸⁵ Eine allgemeine Bedrohungslage, deren Realisierung „praktisch nie ausgeschlossen“ ist, genügt dem nicht.¹⁸⁶ Zur Begründung führte das Gericht aus, die Befugnis zur Rasterfahndung gleiche den zu Zwecken der strategischen Kontrolle vorgenommenen Eingriffen in das Fernmeldegeheimnis insofern, als auch sie verdachtslos erfolgende Grundrechtseingriffe in großer Streubreite vorsehe.¹⁸⁷

Auch § 111 TKG sieht Grundrechtseingriffe in großer Streubreite vor, die ohne jeden Verdacht vorgenommen werden. Die Identität sämtlicher Telefon- und Internetteilnehmer erfassen zu lassen ist ein derart tiefgreifender Grundrechtseingriff, dass er – wie eine Rasterfahndung – allenfalls zur Abwehr einer konkreten Gefahr für hochrangige

¹⁷⁷ Näher Schriftsatz vom 13.08.2008 im Verfahren 1 BvR 256/08, http://www.vorratsdatenspeicherung.de/images/schriftsatz_2008-08-13.pdf, 33.

¹⁷⁸ <http://www.daten-speicherung.de/index.php/ziercke-greift-ak-vorrat-an/>.

¹⁷⁹ Forgó/Grügel, K&R 2010, 218 ff.

¹⁸⁰ EGMR, K.U.-FI vom 02.12.2008, 2872/02.

¹⁸¹ EGMR, K.U.-FI vom 02.12.2008, 2872/02, Abs. 9.

¹⁸² EGMR, K.U.-FI vom 02.12.2008, 2872/02, Abs. 40.

¹⁸³ EGMR, K.U.-FI vom 02.12.2008, 2872/02, Abs. 49.

¹⁸⁴ EGMR, K.U.-FI vom 02.12.2008, 2872/02, Abs. 21.

¹⁸⁵ BVerfGE 115, 320 (320), Ls. 1.

¹⁸⁶ BVerfGE 115, 320 (364).

¹⁸⁷ BVerfGE 115, 320 (359).

Rechtsgüter zulässig sein kann. Die Hoffnung, mehr zutreffende Identifizierungsangaben zu generieren, stellt offenkundig kein wichtiges Rechtsgut dar, welches ein globales und pauschales Verbot anonymer Fernkommunikation rechtfertigen könnte. § 111 TKG verzichtet auf jeden Verdachtsgrad und auf jede Nähe der Betroffenen zu einer Gefahr, stellt gleichzeitig aber einen schwerwiegenden Grundrechtseingriff dar, indem er das Recht auf anonyme Kommunikation und Internetnutzung über einen eigenen Anschluss aufhebt. Dies ist mit dem Verhältnismäßigkeitsgebot offensichtlich unvereinbar.

Schließlich ist darauf hinzuweisen, dass das Koreanische Verfassungsgericht im Jahr 2012 eine Identifizierungspflicht für alle Nutzer von Internetforen als unverhältnismäßigen Grundrechtseingriff verworfen hat.¹⁸⁸

(5) Kein fairer Ausgleich der widerstreitenden Interessen

Zusammenfassend ist festzuhalten: Mit der Identifizierungs- und Ausweispflicht will der Gesetzgeber ein absolutes Verbot anonymer Telekommunikation durchsetzen, selbst wo Teilnehmer nicht einmal in einer entfernten Beziehung zu einer Straftat oder Gefahr stehen. Der Gesetzgeber setzt das Identifizierungsinteresse absolut und macht legitime Anonymität von Kontakten unmöglich. Er nimmt keinen Ausgleich der Rechte und Interessen der Beteiligten vor, sondern verfolgt das Ziel einer absoluten Identifizierbarkeit und Rückverfolgbarkeit elektronischer Kommunikation.

Ein angemessener Interessensausgleich lässt sich nur ohne Identifizierungs- und Ausweispflicht erreichen. Im Grundsatz bleibt eine anonyme Telekommunikation auf diese Weise möglich. Im Ausnahmefall kann eine Identifikation mithilfe betrieblicher Daten (z.B. Bestands-, Verkehrs- oder Aufladedaten) vorgenommen werden. Diese Identifizierungsmöglichkeiten lassen mit einer größeren Zuverlässigkeit auf den Nutzer schließen als Bestandsdaten. Es ist nicht ersichtlich, dass die Aufklärung von Straftaten oder die Gefahrenabwehr merklich darunter leiden würde.

Das Ziel einer verstärkten Verfolgung von Straftaten und Erfüllung sonstiger staatlicher Aufgaben ist zwar legitim. Es fehlt aber jeder Beleg dafür, dass im Fall eines Verbots anonymer Telefon- und Internetanschlüsse tatsächlich mehr Straftäter identifiziert und verurteilt würden als ohne ein solches unterschiedsloses Verbot. Auch unter Geltung einer Identifizierungs- und Verifizierungspflicht werden Straftäter regelmäßig nicht unter ihrer wahren Identität kommunizieren. Da die Behörden vieler europäischer Staaten ihre Aufgaben ohne ein Verbot anonymer Telefon- und Internetanschlüsse wirksam wahrnehmen, besteht augenscheinlich kein dringendes Bedürfnis nach einer solchen Maßnahme.

Umgekehrt besteht ein dringendes Bedürfnis nach anonymen privaten Telefon- und Internetanschlüssen zum Zweck der Information und Kommunikation ohne Furcht vor Nachteilen, beispielsweise als Voraussetzung anonymer Beratung und Hilfeleistung oder für Recherchezwecke der Presse. Eine generelle und undifferenzierte Identifizierungs- und Verifizierungspflicht belastet unbescholtene Bürger in ganz erheblichem Maße, weil diesen eine anonyme Telekommunikationsnutzung in weiten Bereichen unmöglich gemacht wird. Nur ohne Identifizierungs- und Ausweiszwang können Personen wie Journalisten, die staatliche Missstände recherchierten, Organisatoren staatskritischer Demonstrationen oder Vertreter von Wirtschaftsunternehmen, die Wirtschaftsspionage befürchteten, durch die Benutzung vorausbezahlter Mobiltelefonkarten anonym telefonieren. Ein Identifizierungs- und Ausweiszwang zieht dagegen die Gefahr nach sich, dass auf den Austausch sensibler Informationen mittels Telekommunikation zunehmend verzichtet wird. Damit drohen Beeinträchtigungen der gesamtgesellschaftlichen Kommunikation und, wo es sich um politische Kommunikation handelt, auch eine Beeinträchtigung der Funktionsfähigkeit unseres demokratischen Systems. Wenn Menschen aus Furcht vor sozialer Stigmatisierung, vor Nachteilen am Arbeitsplatz, vor Strafverfolgungsmaßnahmen oder vor geheimdienstlicher Beobachtung auf Kommunikation mit anderen verzichten, schadet dies nicht nur ihnen, sondern der demokratischen Gesellschaft insgesamt. Die Gemeinschaft ist darauf angewiesen, dass die Bürgerinnen und Bürger unbefangen kommunizieren und sich informieren können.

Angesichts dessen liegt auf der Hand, dass die aufgezeigten schädlichen Nebenwirkungen des in § 111 Abs. 1 TKG vorgesehenen allgemeinen Identifizierungs- und Ausweiszwangs für Inhaber vorausbezahlter Mobiltelefonkar-

¹⁸⁸ 24-2(A) KCCR 590, 2010Hun-Ma47, 252(consolidated), August 23, 2012.

ten in keinem Verhältnis zu dem erhofften Zusatznutzen einer solchen Maßnahme für die von der Bundesrepublik angestrebten Zwecke steht. Der gesamten Bevölkerung anonyme Mobiltelekommunikation und Internetnutzung zu verbieten, nur weil diese Möglichkeit in einem Bruchteil aller Fälle missbraucht wird, ist in einer demokratischen Gesellschaft nicht akzeptabel.

Die generelle und undifferenzierte Erfassung und Verifizierung der Identität aller Inhaber von Telekommunikations- und Internetanschlüssen auf Vorrat, die – wie die Beschwerdeführer – einer Straftat nie auch nur verdächtig waren, stellt keinen fairen Ausgleich zwischen den widerstreitenden öffentlichen und privaten Interessen her. Die Bundesrepublik hat jeden akzeptablen Ermessensspielraum in dieser Hinsicht überschritten. Die Zwangsidentifizierung der Beschwerdeführer stellt einen unverhältnismäßigen Eingriff in deren Recht auf informationelle Selbstbestimmung dar und kann nicht als gerechtfertigt angesehen werden.

Der Wunsch, Rechtsgüter zu schützen, kann das Recht auf unbefangene und anonyme Information und Kommunikation allgemein nicht aufheben. Das Grundgesetz setzt ersichtlich auf ein weitaus voraussetzungsreicheres System des Rechtsgüterschutzes als eine generelle und undifferenzierte Aufzeichnung und Überprüfung der Identität jedes Inhabers eines Kommunikations- und Internetanschlusses. Zwar besteht ein legitimes Interesse am Schutz von Rechtsgütern. Doch darf, wo mehrere Prinzipien in Widerstreit geraten können, nicht eines auf Kosten des anderen schematisch oder gar absolut zur Geltung gebracht werden. Insofern ist es von vornherein unstatthaft, eine Diskussion um Schutzmaßnahmen zu führen, ohne den Ausgleich zwischen öffentlichen Interessen und Privatheit mit einzubeziehen. Wissen und Aufklärung gehören zur Demokratie ebenso wie der rechtsstaatliche und schonende Umgang mit personenbezogenen Daten. Mit der Forderung nach totaler Identifizierbarkeit jeglichen Kommunikationsteilnehmers und Internetnutzers werden gläserne Verhältnisse verlangt, der Bürger soll dem Staat zeigen, was er tut und wer er ist. Ein Rechtsstaat benötigt und erlaubt indes kein jakobinisches Schwert, mit dem man die Hülle privater Abwehrrechte durchschlagen könnte, um die „wahren“ Verhältnisse offenzulegen. In einer Demokratie erfolgt der Rechtsgüterschutz gezielt und anlassbezogen und nicht durch Totalkontrolle und -erfassung jeglicher Informations- und Kommunikationsteilnehmer.

3. Ergebnis

§ 111 Abs. 1 S. 3 ff. TKG verletzt das Recht der Beschwerdeführer auf informationelle Selbstbestimmung, wenn man nicht bereits Art. 10 GG für einschlägig erachtet. Die in § 111 Abs. 1 S. 3 ff. TKG angeordnete generelle und undifferenzierte Erfassung und Überprüfung der Identität aller Inhaber von Telekommunikations- und Internetanschlüssen auf Vorrat, die – wie der Beschwerdeführer – einer Straftat nie auch nur verdächtig waren, stellt einen unverhältnismäßigen Eingriff in die Rechte der Betroffenen dar und kann nicht als verhältnismäßig angesehen werden.

II. Verletzung des Art. 5 GG

1. Schutzbereich

Dass das Recht auf freie Meinungsäußerung den Anspruch auf anonyme Meinungsäußerung umfasst, hat der US-amerikanische Oberste Gerichtshof (Supreme Court) schon früh anerkannt. Er hat dies in der Entscheidung *Talley v. California*¹⁸⁹ damit begründet, dass die „anonyme Meinungsäußerung“ eine wertvolle Rolle für den „Fortschritt der Menschheit“ gespielt habe. Verfolgte Gruppen seien im Lauf der Geschichte nur im Schutz der Anonymität in der Lage gewesen, Unterdrückungspraktiken und -gesetze zu kritisieren. Auch könne eine „Identifizierung und die Furcht vor Vergeltung von vollkommen friedlichen Diskussionen wichtiger öffentlicher Angelegenheiten abschrecken“. Eine Pflicht zur Nennung der Verantwortlichen auf Flugzetteln hat der Gerichtshof daher als Verstoß gegen die Meinungsfreiheit verworfen.

¹⁸⁹ 362 U.S. 60 (1960).

In einer späteren Entscheidung¹⁹⁰ hat der Oberste Gerichtshof ausgeführt, Anonymität stelle oft ein „Schutzschild vor der Tyrannei der Mehrheit“ dar. Nur im Schutz der Anonymität könne man seine Meinung äußern, ohne dass sie (auch unbewusst) allein wegen der Person des Äußernden (z.B. wegen seines Geschlechts, seiner Rasse, seiner Hautfarbe, seiner Religion, seiner Herkunft) abgelehnt werde. Auf diese Weise helfe die Anonymität der Verbreitung von Ideen. Anonyme Meinungsäußerungen „exemplifizieren den Zweck des Grundrechtskatalogs und insbesondere der Meinungsfreiheit: unbeliebte Personen vor Vergeltung in einer intoleranten Gesellschaft zu schützen – und ihre Ideen vor Unterdrückung“. Der Oberste Gerichtshof hat auch anerkannt, dass Vereine die Liste ihrer Mitglieder nicht offen legen müssen.¹⁹¹ Es müsse möglich bleiben, anonym Mitglied eines unbeliebten Vereins zu sein, um die Freiheit auch unpopulärer Meinungen zu gewährleisten.

Gewährleistet ist schließlich auch das Recht, sich anonym zu informieren.¹⁹² Dies gebietet der Zweck der Meinungsfreiheit. Anonyme Informationskanäle erweitert den Zuhörerkreis von Meinungsäußerungen und erlaubt einen unbefangenen Zugang zu einer breiten Auswahl an Informationen. Dies ist etwa für die Verbreitung der Anliegen stigmatisierter und finanzschwacher „kleiner Leute“ besonders wichtig. Wenn Menschen das Stigma vermeiden können, das mit dem Anhören bestimmter Tatsachen und Meinungen verbunden ist, werden sie eher bereit sein, sich damit vorurteilsfrei auseinanderzusetzen.

In den letzten Jahren haben die US-amerikanischen Instanzgerichte das Recht auf Anonymität auch auf das Internet angewandt. Der Washington District Court entschied 2001,¹⁹³ das Recht auf anonyme Meinungsäußerung sei von grundlegender Bedeutung für die Verabschiedung der US-amerikanischen Verfassung selbst gewesen, weil sowohl Befürworter („Federalist Papers“) wie auch Widersacher ohne Namensnennung über die Ratifizierung der Verfassung stritten. Das Gericht entschied wörtlich: „Das Internet begünstigt den reichhaltigen, vielfältigen und weitreichenden Austausch von Ideen. Die Möglichkeit, seine Meinung im Internet äußern zu können, ohne dass die andere Seite alle Tatsachen über die eigene Identität kennt, kann offene Kommunikation und robuste Debatte fördern.“¹⁹⁴ Larios hat eine Übersicht über die US-amerikanische Rechtsprechung zum Schutz der Anonymität von Internetnutzern durch das Grundrecht auf freie Meinungsäußerung veröffentlicht.¹⁹⁵

Auch in Europa haben sich die politische Opposition und der Widerstand gegen die Obrigkeit immer wieder der Anonymität bedienen müssen. Berühmte Schriftsteller wie Erich Kästner oder Kurt Tucholsky schrieben nicht unter ihrem eigenen Namen. 1849 veröffentlichte der Rechtswissenschaftler Theodor Mommsen einen Kommentar über die in der neuen Verfassung von 1848 garantierten „Grundrechte des deutschen Volkes“ – anonym. Im gleichen Jahr veröffentlichte Adolph Streckfuß sein Werk „Das freie Preußen. Geschichte des Berliner Freiheitskampfes vom 18. März 1848 und seine Folgen“, ohne seinen Namen zu nennen.

Mit Urteil vom 25.03.2010 hat der Oberste Gerichtshof Israels bekräftigt, dass ein „Recht auf Anonymität“ bestehe.¹⁹⁶ Unter Bezugnahme auf die Rechtsprechung des US-amerikanischen Supreme Court führte der Gerichtshof aus, dass Bestandteil des Rechts auf freie Meinungsäußerung auch das Recht auf anonyme Meinungsäußerung sei. Teilweise setze die Möglichkeit und Bereitschaft zur Äußerung einer Meinung voraus, dass dies anonym geschehen könne. Ursache könnten persönliche Gefühle wie Scham oder Mutlosigkeit sein, externer Druck oder die Besorgnis über Reaktionen der Außenwelt. Mitunter sei die Anonymität aber auch Bestandteil der zu äussernden Botschaft. Sie verhindere etwa, dass Annahmen über den Verfasser die geäußerte Meinung überlagern und verfä-

¹⁹⁰ McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995).

¹⁹¹ NAACP v. Alabama ex. rel. Patterson, 357 U.S. 449 (1958).

¹⁹² Crump, 56 Stanford Law Review (2003), <http://www.thefreelibrary.com/Data+retention%3A+privacy,+anonymity,+and+accountability+online.-a0110534145>.

¹⁹³ Doe v. 2TheMart.com, 140 F.Supp.2d 1088.

¹⁹⁴ Doe v. 2TheMart.com, 140 F.Supp.2d 1088.

¹⁹⁵ Larios, Rutgers Law Record, Vol. 37, p. 36, 2010, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1640133.

¹⁹⁶ Oberster Gerichtshof Israels, 4447/07 vom 25.03.2010, <http://elyon1.court.gov.il/files/07/470/044/p10/07044470.p10.htm>, Absatz-Nr. 11.

schen. Anonymität sei zugleich auch im Rahmen des Grundrechts auf Privatsphäre geschützt und ein wichtiger Bestandteil dieses Rechts. Anonymität gebe dem Betroffenen Kontrolle über Informationen über ihn. Im Bereich des Internets komme der Anonymität eine verstärkte Bedeutung zu. Das Internet ermögliche eine freie Meinungsäußerung in besonderem Maße. Auch im Rahmen des Rechts auf Privatsphäre komme der Anonymität im Internet besondere Bedeutung zu. Bei der Internetnutzung fielen – zum Teil unfreiwillig – Informationen über das Nutzungsverhalten an. Im Laufe der Zeit bildete sich so eine Datenbank mit persönlichen Daten, Meinungen und Interessen. Während früher alle Handlungen im Schutz der eigenen Wohnung vor Blicken von außen geschützt gewesen seien, könne im Zeitalter des Internets direkt und indirekt tief „in die Seele der Person eingedrungen“ werden. Diese Verletzung der Privatsphäre müsse „minimiert“ werden. Je größer die Möglichkeiten einer Auswertung des Nutzungsverhaltens, desto eher sei eine erhebliche Verhaltensänderung auf Seiten der Nutzer zu erwarten.

In Deutschland hat der Bundesgerichtshof anerkannt, dass Art. 5 GG das Recht auf anonyme Meinungsäußerung im Internet schützt.¹⁹⁷

2. Eingriff

§ 111 Abs. 1 S. 3 TKG greift in das Recht auf anonyme Meinungsäußerung ein, indem er die – auch im Verhältnis zu Anbieter und Staat – anonyme Äußerung und Entgegennahme von Meinungen und Informationen über einen eigenen Telefon- oder Internetanschluss unmöglich oder jedenfalls unzumutbar¹⁹⁸ macht. § 111 Abs. 1 S. 3 TKG hindert daran, über Mobiltelefonkarten anonym und ohne Furcht vor nachteiligen Konsequenzen seine Meinung oder sonstige Informationen weiterzugeben oder entgegenzunehmen.

3. Mangelnde Rechtfertigung

Was den erhofften Nutzen der Norm angeht, ist oben bereits ausgeführt worden, dass ein statistisch signifikanter Mehrwert bei der Verfolgung von Straftätern oder bei sonstigen Staatsaufgaben nicht belegt ist und dass viele europäische Staaten ihre staatlichen Aufgaben ohne ein generelles Verbot anonymer Telekommunikations- und Internetanschlüsse erfüllen.

Auf der anderen Seite bewirkt die Vorschrift einen tiefgreifenden Eingriff in das Recht nahezu jedes volljährigen Bürgers auf freien und unbefangenen Meinungs- und Informationsaustausch. Die in § 111 Abs. 1 S. 3 TKG vorgesehene generelle und undifferenzierte Ausweispflicht beseitigt für rechtstreue Bürger die Möglichkeit des anonymen Informationsaustauschs über Telekommunikationsnetze und Internet weitgehend. Praktisch jede digitale Meinungsäußerung wird identifizierbar.

Die in § 111 Abs. 1 S. 3 ff. TKG vorgesehene Identifizierung und Registrierung aller Telekommunikationsteilnehmer ermöglicht Staatsbediensteten teilweise die Feststellung, wer per Individualkommunikation oder über Telemedien bestimmte Meinungen oder Tatsachenbehauptungen geäußert oder abgerufen hat. Dies kann dem Staat unmittelbar möglich sein, wo Telekommunikation mit Staatsbediensteten oder die Nutzung staatlicher Internet-Meinungsforen¹⁹⁹ oder Kontaktformulare in Rede steht. Sonstigen Informations- und Meinungsaustausch kann der Staat unter Zuhilfenahme von Kommunikations- und Zugriffsprotokollen aufdecken, die er anfordern kann.

Gerade im Internet protokollieren die meisten Anbieter, über welche IP-Adresse wann welche Information oder Meinung gesendet oder abgerufen wurde. Die meisten Internet-Zugangsanbieter in Deutschland speichern eine Woche lang, welchem Kunden wann welche IP-Adresse zugeordnet war. Damit entscheidet letztlich die Anonymität des Internetanschlusses darüber, ob man sich ohne Furcht vor Konsequenzen über das Internet informieren und seine Meinung äußern kann. Dass ein Meinungs- und Informationsaustausch ohne das Internet heute in weiten Bereichen nicht mehr denkbar ist, liegt auf der Hand.

¹⁹⁷ BGHZ 181, 328, Abs. 50 ff.

¹⁹⁸ Näher Seite 17.

¹⁹⁹ Beispielsweise http://www.bmg.bund.de/bmg_forum/ und http://www.cio.bund.de/kbst_forum/, wo ausdrücklich auch die IP-Adressen der Nutzer festgehalten werden.

Über elektronische Kanäle kann der Bürger seine Meinung wegen § 111 TKG weithin nicht mehr ohne das Risiko einer Nachverfolgung anonym äußern. Auch kann er Meinungen und Informationen nicht mehr ohne das Risiko einer Nachverfolgung anonym abrufen. Dieses Risiko kann von dem unbefangenen Gebrauch der Meinungs- und Informationsfreiheit abschrecken.²⁰⁰ Die Identifizierbarkeit jeder Person, die eine bestimmte Meinung äußert, begründet die Gefahr, dass der Einzelne aus Furcht vor Repressalien oder sonstigen negativen Auswirkungen sich dahingehend entscheidet, seine Meinung gegenüber Bundesorganen nicht zu äußern. Dieser Gefahr der Selbstzensur soll das Grundrecht auf freie Meinungsäußerung gerade entgegen wirken.²⁰¹ Eine abschreckende Wirkung ist besonders in Bezug auf die Rückverfolgbarkeit staatskritischer Meinungen und Tatsachendarstellungen zu erwarten, deren freier Austausch in einer Demokratie von besonders hohem Wert ist.

Die von § 111 TKG bewirkte Identifizierbarkeit jedes Internetnutzers bedeutet eine schwere Beeinträchtigung der Informationsfreiheit im Internet, weil man Nachteile durch den Aufruf „potenziell verdächtiger“ Seiten oder die Verwendung „potenziell verdächtiger“ Suchwörter befürchten muss. 2007 hat ein deutsches Gericht eine – ergebnislose – Wohnungsdurchsuchung bei Globalisierungskritikern damit begründet, der Betroffene habe eine „umfassende Internetrecherche“ zu einer Firma vorgenommen, die später Ziel eines Brandanschlags wurde.²⁰² Es beeinträchtigt die Meinungsfreiheit massiv, wenn man wegen ihres internetgestützten Gebrauchs jederzeit mit einschneidenden Ermittlungsmaßnahmen rechnen muss.

§ 111 TKG schreckt auch von dem unbefangenen Abruf öffentlich zugänglicher Telemedien ab. Diese Gefahr besteht etwa dort, wo aus dem Seitenabruf wegen des Inhalts der Seite oder des Telemediums auf politische Meinungen, religiöse Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben des Internetnutzers geschlossen werden kann. Beispielsweise ermittelte das Bundeskriminalamt bis 2008 gegen Nutzer des Portals www.bka.de, die mit „signifikanter Zugriffsfrequenz“ Informationen über bestimmte kriminelle oder terroristische Vereinigungen von dem Portal abriefen. Die Kundendaten entsprechender Nutzer wurden anhand ihrer IP-Adresse abgefragt und mit verschiedenen Datenbanken abgeglichen. Die aufgezeigte Verfahrensweise hat die Bundesregierung auf parlamentarische Anfragen öffentlich bestätigt.²⁰³ Identifizierung und Datenbankabgleich wurden nach unbestrittenen Presseinformationen bei einer dreistelligen Anzahl von Personen durchgeführt, die in keinerlei Verbindung mit einer Straftat standen. In dem Pressebericht heißt es:

„Ursprünglich hatte das BKA die Identität von 417 Personen feststellen wollen. Dabei handelte es sich nicht um Tatverdächtige, sondern offenbar um alle Personen, die sich zwischen dem 28. März und dem 18. April diesen Jahres auf den Internetseiten des Bundeskriminalamtes über die ‚Militante Gruppe‘ informieren wollten. Weil aber ein großer Teil der IP-Adressen von Providern stammte, die diese nur kurze Zeit speichern, wurde die Identifizierung von ‚nur‘ rund 120 Telekom-Kunden beantragt. Das BKA habe ‚einen weiteren Teil‘ der IP-Adressen ‚Presseorganen bzw. einzelnen Firmen oder Universitäten‘ zugeordnet, heißt es. ‚Anhand dieser Daten werden weiterführende polizeiliche Ermittlungen wie unter anderem die Identifizierung weiterer Mitglieder der ‚militanten gruppe‘ (mg) ermöglicht‘, begründen die Beamten ihren Antrag.“²⁰⁴

Die abschreckende Wirkung einer Erfassung des Informations- und Kommunikationsverhaltens schadet der Meinungsfreiheit und unserem Gemeinwesen insgesamt. Denn nur umfassende Informationen, die man ungehindert und unbefangenen zur Kenntnis nehmen kann, ermöglichen eine freie Meinungsbildung und -äußerung für den Einzelnen wie für die Gemeinschaft.²⁰⁵ Nur auf der Grundlage eines freien und unbefangenen Informationszugangs

²⁰⁰ Vgl. BGH, NJW 2009, 2888.

²⁰¹ Vgl. BGH, NJW 2009, 2888.

²⁰² ngo online: Rechtswidrige Hausdurchsuchungen zum Datensammeln über „bürgerlichen Protest“ (10.05.2007), http://www.ngo-online.de/ganze_nachricht.php?Nr=15912.

²⁰³ BT-Prot. 16/117, 22; BT-Drs. 16/6938.

²⁰⁴ Tagesspiegel vom 30.09.2007, <http://www.tagesspiegel.de/politik/deutschland/BKA-Datenschutz;art122,2390884>.

²⁰⁵ Vgl. BVerfGE 27, 71 (81).

kann der Bürger informiert politische Entscheidungen treffen und am freiheitlichen demokratischen Gemeinwesen mitwirken. Ein nicht rückverfolgbarer Informationszugang ist heutzutage elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens.

Wie bereits zu Art. 2, 1 GG aufgezeigt, ist es evident unverhältnismäßig, alle Grundrechtsträger der Möglichkeit des anonymen und dadurch unbefangenen elektronischen Meinungs- und Informationsaustauschs zu berauben, nur um gegen den Missbrauch einiger weniger leichter vorgehen zu wollen. Dies gilt insbesondere in Anbetracht der Tatsache, dass sich die staatliche Aufgabenwahrnehmung in der Praxis auch ohne eine generelle und undifferenzierte Erfassung der Identität unbescholtener Bürger gewährleisten lässt. Wie die Praxis der allermeisten europäischen Staaten zeigt, ermöglichen anlassbezogene Ermittlungen einen ebenso guten, in jedem Fall aber einen hinreichenden Rechtsgüterschutz.

Zur Vermeidung von Wiederholungen wird im Übrigen auf die zu Art. 2, 1 GG angestellte Abwägung²⁰⁶ Bezug genommen, die für Art. 5 GG entsprechend gilt.

D. Zum Verfahren

Beim Europäischen Menschenrechtsgerichtshof ist unter dem Az. 50001/12 meine Beschwerde gegen die Entscheidung des Bundesverfassungsgerichts vom 24.1.2012 (Az. 1 BvR 1299/05) anhängig, soweit der Verfassungsbeschwerde gegen § 111 TKG nicht abgeholfen wurde. Die Beschwerde wurde der Bundesregierung zur Stellungnahme übersandt. Es wird angeregt, das vorliegende Verfahren bis zur Entscheidung über diese Beschwerde auszusetzen.

Sollte das Gericht wegen fehlender Ausführungen oder wegen mangelnder Substantiierung meines Vortrags 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.

Kiel, 31.07.2017

Ort, Datum

Unterschrift des Beschwerdeführers

²⁰⁶ Seiten 40 ff.