An den Kanzler
des Europäischen Gerichtshofs für Menschenrechte
Europarat
F-67075 STRASBOURG CEDEX

Beschwerde

1. des Herrn Patrick Breyer, [...] und
2. des Herrn Jonas Breyer, [...]

gegen

die Bundesrepublik Deutschland

Inhaltsübersicht

A. Sachverhalt

Wir beschweren uns über die Pflicht zur Identifizierung und Vorratsspeicherung aller Inhaber von Telekommunikationsanschlüssen (z.B. Festnetz, Mobilfunk, Internetzugang) in Deutschland (§ 111 TKG), weil sie unsere Rechte auf Achtung der Privatsphäre und der Korrespondenz (Art. 8 EMRK) sowie auf freie Meinungsäußerung und freien Informationszugang (Art. 10 EMRK) verletzt.

I. Gesetzeslage

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

> *§ 111 Daten für Auskunftsersuchen 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 Auskunftsersuchen 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. 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.

Vor Inkrafttreten der vorbezeichneten Vorschriften durften Telekommunikationsanbieter personenbezogene Daten nur erheben, soweit dies betrieblich erforderlich war. Guthaben-Mobilfunkkarten (Prepaid-Karten) wurden ohne Erhebung personenbezogener Daten anonym verkauft und genutzt.[1]

II. Betroffenheit der Beschwerdeführer

Der Beschwerdeführer zu 1 besitzt und benutzt eine vorausbezahlte Mobiltelefonkarte der Firma E-Plus Service GmbH & Co. KG, die er nach In-

[1] Vgl. Bundesverwaltungsgericht, Urteil vom 22. Oktober 2003, AZ: 6 C 23/02.

krafttreten des Telekommunikationsgesetzes 2004 erworben hat. Zur Freischaltung der Karte musste er in Übereinstimmung mit § 111 TKG Name, Anschrift und Geburtsdatum angeben. Der Beschwerdeführer hat sich mit der Aufnahme seiner Daten in ein öffentliches Verzeichnis nicht einverstanden erklärt; seine Rufnummer steht nicht im Telefonbuch.

Der Beschwerdeführer zu 1 nutzt die vorausbezahlte Mobiltelefonkarte zur mobilen Sprachkommunikation, zur Textkommunikation (SMS) und zur Herstellung von Internetverbindungen (UMTS, GRPS, HSDPA). Der Anbieter E-Plus speichert 3-4 Monate lang, von wem der Beschwerdeführer zu 1 Anrufe oder Textnachrichten entgegen genommen hat und wen der Beschwerdeführer zu 1 angerufen oder per SMS kontaktiert hat. Bei jeder ein- oder ausgehenden Verbindung speichert E-Plus zudem den Standort (Funkzelle), die Kartenkennung (IMSI) und die Gerätekennung (IMEI) des Beschwerdeführers zu 1.[2]

Der Beschwerdeführer zu 1 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 zu 1 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 zu 1 fühlt sich in seinen regierungskritischen Aktivitäten beeinträchtigt, weil sein gesamtes mobiles Kommunikations-, Bewegungs- und Internetnutzungsverhalten für staatliche Stellen personenbezogen nachvollziehbar ist. In Anbetracht einer Reihe von Durchsuchungen und Festnahmen staatskritischer Personen in den letzten Jahren, deren Rechtswidrigkeit oder Unbegründetheit später festgestellt wurde, will sich der Beschwerdeführer zu 1 nicht darauf verlassen, dass ihn die legale Ausübung seiner Grundrechte vor Nachteilen bewahrt.

Hinzu kommt, dass der Beschwerdeführer zu 1 im Internet publizistisch tätig ist, sowohl auf dem Internetportal des Arbeitskreises Vorratsdaten-

speicherung als auch auf einem eigenen überwachungskritischen Internetportal.[3] 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 ist der Beschwerdeführer zu 1 Landtagsabgeordneter. Über die nach § 111 TKG anzugebenden Daten kann sein Anschluss überwacht werden, über den er teils vertrauliche Kontakte mit Bürgern und Hinweisgebern abwickelt. Die mangelnde Anonymität des Anschlusses kann Bürger und Hinweisgeber davon abhalten, sich an den Beschwerdeführer zu 1 zu wenden und ihn über Missstände zu informieren.

Der Beschwerdeführer zu 2 besitzt und benutzt eine vorausbezahlte Mobiltelefonkarte (Guthabenkarte oder Prepaid-Karte) der Telekom Deutschland GmbH, die er nach Inkrafttreten des Telekommunikationsgesetzes 2004 erworben hat. Zur Freischaltung der Karte musste er in Übereinstimmung mit § 111 TKG Name, Anschrift und Geburtsdatum angeben. Der Beschwerdeführer hat sich mit der Aufnahme seiner Daten in ein öffentliches Verzeichnis nicht einverstanden erklärt; seine Rufnummer steht nicht im Telefonbuch.

Der Beschwerdeführer zu 2 nutzt die vorausbezahlte Mobiltelefonkarte zur mobilen Sprachkommunikation, zur Textkommunikation (SMS) und zur Herstellung von Internetverbindungen (UMTS, GRPS, HSDPA), jeweils im In- und Ausland. Der Anbieter Telekom Deutschland GmbH speichert 180 Tage lang, von wem der Beschwerdeführer zu 2 Anrufe oder Textnachrichten entgegen genommen hat und wen der Beschwerdeführer zu 2 angerufen oder per SMS kontaktiert hat. Bei jeder ein- oder ausgehenden Verbindung speichert er zudem den Standort (Funkzelle), die Kartenkennung (IMSI) und die Gerätekennung (IMEI) des Beschwerdeführers zu 2.[4]

Auch der Beschwerdeführer zu 2 ist in der Bürgerrechtsorganisation „Arbeitskreis Vorratsdatenspeicherung“ sowie publizistisch auf Online-Blogs im Internet aktiv. Das oben Gesagte gilt entsprechend. Auch nimmt er regelmäßig an öffentlichen Versammlungen teil und koordiniert diese mit,

---

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

[3] http://www.daten-speicherung.de.

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

die Datenschutz und Bürgerrechte zum Gegenstand haben und vom Arbeitskreis Vorratsdatenspeicherung in Kooperation mit zahlreichen anderen Bürgerrechtsorganisationen organisiert. Dies macht eine intensive mobile Kommunikation unentbehrlich. Der Beschwerdeführer zu 2 ist kein Abgeordneter.

Die Anbieter speichern die nach § 111 TKG erhobenen Daten der Beschwerdeführer zusammen mit deren Rufnummern. Die Daten stehen über ein automatisiertes Such- und Abrufverfahren (§ 112 TKG) einer Vielzahl staatlicher Behörden zum direkten Online-Abruf zur Verfügung. Rund 250 Behörden haben zurzeit Zugriff auf die Kundendaten (sog. „Bestandsdaten“) von 140 Telekommunikationsunternehmen.[5] Im Jahr 2011 sind 6.000.000 behördliche Abrufe von bzw. Suchanfragen nach Telekommunikations-Bestandsdaten erfolgt, was über 10.000 Abfragen täglich entspricht.[6] Die Beschwerdeführer werden nicht in Kenntnis gesetzt, wenn ihre Daten ausgelesen werden; sie erhalten auch auf Nachfrage keine Auskunft über behördliche Zugriffe auf ihre Daten.

III. Relevanz von Telekommunikation

99% der Haushalte in Deutschland verfügen gegenwärtig über mindestens einen eigenen Festnetz- oder Mobilfunkanschluss. In 88% der Haushalte gibt es einen Festnetzanschluss, in 86% der Haushalte einen Mobilfunkanschluss, in 66% der Haushalte ein Internetanschluss. 53% der deutschen Haushalte nutzen mindestens eine vorausbezahlte Mobilfunkkarte (Prepaid).[7]

Es gibt in Deutschland 38 Mio. feste Telefonanschlüsse[8], 112 Mio. Mobiltelefonanschlüsse[9] und 27 Mio. feste Breitband-Internetanschlüsse.[10] Die

---

[5] Bundesnetzagentur, Jahresbericht 2011, 112.

[6] Bundesnetzagentur, Jahresbericht 2011, 112.

[7] Eurobarometer, E-Communications Household Survey vom Dezember 2011, http://ec.europa.eu/information_society/digital-agenda/scoreboard/docs/pillar/studies/eb_ecomm/country_fiches/eb381-de-en.pdf.

[8] Bundesnetzagentur, Tätigkeitsbericht 2010/2011, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Presse/Berichte/2011/TaetigkeitsberichtTK20102011pdf.pdf;jsessionid=400A332305D72F7548502A4A4ACE45C6?__blob=publicationFile, 30.

[9] Bundesnetzagentur, Tätigkeitsbericht 2010/2011, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Presse/Berichte/2011/TaetigkeitsberichtTK20102011pdf.pdf;jsessionid=400A332305D72F7548502A4A4ACE45C6?__blob=publicationFile, 50.

Zahl der deutschen E-Mail-Nutzer liegt bei 37 Mio.[11], was 45% der Bevölkerung entspricht.

2011 wurde in Deutschland 191 Mrd. Minuten lang telefoniert.[12] Da die durchschnittliche Verbindungsdauer bei 3 Minuten im Festnetz und 2 Minuten im Mobilfunknetz liegt,[13] dürften jährlich etwa 76 Mrd. Telefonate erfolgen.[14] 2011 wurden außerdem 55 Mrd. SMS-Textnachrichten versandt.[15]

83% der deutschen Haushalte hatten 2011 Zugang zu einem (eigenen oder fremden) Internetanschluss.[16] 77% nutzen das Internet in ihrem Zuhause über einen privaten Anschluss,[17] 37% am Arbeitsplatz,[18] 7% in Bildungseinrichtungen,[19] 18% in Häusern anderer Personen.[20] 10 Mio. Men-

[10] Bundesnetzagentur, Jahresbericht 2011, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Presse/Berichte/2012/Jahresbericht2011pdf.pdf?__blob=publicationFile, 74.

[11] Welt: An der E-Mail kommt fast niemand mehr vorbei (14.05.2007), http://www.welt.de/webwelt/article872219/An_der_E-Mail_kommt_fast_niemand_mehr_vorbei.html.

[12] Bundesnetzagentur, Jahresbericht 2011, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Presse/Berichte/2012/Jahresbericht2011pdf.pdf?__blob=publicationFile, 81.

[13] Schweizer Bundesamt für Kommunikation: Amtliche Fernmeldestatistik 2006, http://www.bakom.admin.ch/dokumentation/zahlen/00744/00746/index.html?lang=de&-downlo-ad=M3wBUQCu/8ulmKDu36WenojQ1NTTjaXZnqWfVpzLhmfhnapmmc7Zi6rZnqCkkIN3fH97bKbXrZ2lhtTN34al3p6YrY7P1oah162apo3X1cjYh2+hoJVn6w==.pdf, 8.

[14] Uhe/Herrmann, Überwachung im Internet (I), 161: 79 Mrd. Verbindungen pro Jahr; vgl. auch Welt, Bamberg steuert 50 Milliarden Telefonate jährlich (04.01.2003), http://www.welt.de/print-welt/article324432/Bamberg_steuert_50_Milliarden_Telefonate_jaehrlich.html für Festnetzverbindungen der Deutschen Telekom AG im Jahr 2003.

[15] Bundesnetzagentur, Jahresbericht 2011, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Presse/Berichte/2012/Jahresbericht2011pdf.pdf?__blob=publicationFile, 86.

[16] Eurostat, Niveau von Internet-Zugang von Haushalten (IACCHOUS).

[17] Eurostat, Internetzugang zuhause (I_IHM).

[18] Eurostat, Internetzugang am Arbeitsplatz (I_IWRK).

[19] Eurostat, Internetzugang in der Bildungseinrichtung (I_IED).

[20] Eurostat, Internetzugang in Häusern anderer Personen (I_IOH).

schen nutzen das Internet über Mobilfunktechnologien,[21] welche vorausbezahlte Mobilfunkkarten einschließen.

63% der Deutschen nutzen das Internet täglich.[22] Internetnutzer verbringen durchschnittlich mehr als zwei Stunden (137 Minuten) pro Tag im Netz.[23] 73% der Deutschen schreiben und lesen Textnachrichten über das Internet (E-Mails),[24] 33% senden Nachrichten über soziale Netzwerke oder Instant Messaging,[25] 18% telefonieren über das Internet.[26] 44% nutzen soziale oder berufliche Netzwerke im Internet.[27] 70% informieren sich online über Waren und Dienstleistungen.[28] 25% hören im Internet Radio oder sehen fern.[29] 38% nutzen das Internet für Zwecke der Ausbildung oder Weiterbildung.[30] 18% suchen im Internet nach einer Arbeitsstelle.[31] 35% informieren sich auf staatlichen Internetportalen,[32] 37% kommunizieren über das Internet mit Behörden.[33]

52% lesen über das Internet Online-Zeitungen und Nachrichtenmagazine.[34] 58% informieren sich in Online-Lexika wie Wikipedia.[35] 22% veröf-

---

[21] Bundesnetzagentur, Jahresbericht 2011, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Presse/Berichte/2012/Jahresbericht2011pdf.pdf?__blob=publicationFile, 88.

[22] Eurostat, Internetnutzung täglich (I_IDAY).

[23] Bundesnetzagentur, Jahresbericht 2011, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Presse/Berichte/2012/Jahresbericht2011pdf.pdf?__blob=publicationFile, 88.

[24] Eurostat, Senden/Empfangen von E-Mails (I_IUEM).

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

[26] Eurostat, Telefonieren oder Videoanrufe (I_IUPH1).

[27] Eurostat, Nutzen von sozialen oder professionellen Netzwerken (I_IUNET).

[28] Eurostat, Suche nach Informationen über Waren und Dienstleistungen (I_IUIF).

[29] Eurostat, Web-Radio/Web-Fernsehen (I_IUWEB).

[30] Eurostat, Personen, die das Internet in den letzten 3 Monaten für Aus- und Weiterbildung verwendet haben (I_IEDUT).

[31] Eurostat, Arbeitssuche oder zur Übermittlung einer Stellenbewerbung (I_IUJOB).

[32] Eurostat, Informationsbeschaffung auf Websites öffentlicher Stellen (I_IGOVIF).

[33] Eurostat, Interaktion mit staatlichen Behörden (I_IUGOV).

[34] Eurostat, Lektüre/das Herunterladen von Online-Zeitungen/Nachrichtenmagazinen (I_IUNW).

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

fentlichen eigene Inhalte im Internet.[36] 23% lesen oder verfassen Meinungsbeiträge über Bürgerangelegenheiten oder politische Themen auf Internetseiten.[37] 11% nehmen sogar an Beratungen oder Abstimmungen im Internet über Bürgerangelegenheiten oder politische Themen oder an Internet-Petitionen teil.[38] 54% beschaffen über das Internet gesundheitsrelevante Informationen.[39]

3% der Haushalte verzichten gänzlich auf einen Internetanschluss, weil sie Bedenken hinsichtlich der Wahrung ihrer Privatsphäre oder Sicherheit haben.[40]

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

[37] Eurostat, Lesen oder Verfassen von Meinungsäusserungen über Bürgerangelegenheiten oder politische Themen auf Internetseiten (I_IUPOL).

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

[39] Eurostat, Beschaffung von gesundheitsrelevanten Informationen (I_IHIF).

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

B. Begründung

I. Verletzung des Art. 8 EMRK

§ 111 TKG verletzt unser Recht auf Achtung der Privatsphäre und der Korrespondenz (Art. 8 EMRK), soweit er uns ohne jeden Anlass zur Preisgabe unserer Identität zwingt, bevor wir über einen eigenen Anschluss telekommunizieren und das Internet nutzen können.

1. Eingriff in den Schutzbereich

Art. 8 EMRK gewährleistet das Recht auf informationelle Selbstbestimmung und auf Schutz personenbezogener Daten.[41] 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. Unter Bezugnahme auf die Datenschutzkonvention erkennt der Gerichtshof an, dass die Sammlung und Speicherung personenbezogener Daten einen Eingriff in das Privatleben des Einzelnen darstellt,[42] ebenso wie die Verwendung solcher Daten und die Verweigerung ihrer Löschung.[43] Ein persönlicher Lebenssachverhalt liegt bereits dann vor, wenn die Verknüpfung des Lebenssachverhalts mit der zugehörigen Person möglich ist.[44]

§ 111 TKG greift in das Recht auf Schutz persönlicher Daten ein, indem er die Verfügbarkeit von Telekommunikationsanschlüssen von der Offenbarung der Identität des Vertragspartners abhängig macht. § 111 Abs. 1 S. 1 und Abs. 2 S. 1 TKG verpflichten Telekommunikationsanbieter zur Identifizierung von Anschlussinhabern, selbst wenn dies 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 offenlegen oder anonym kommunizieren möchten.

Der Einordnung des § 111 TKG als staatlichen Eingriff in die Rechte der Beschwerdeführer steht nicht entgegen, dass der Staat private Telekom-

---

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

[42] Frowein/Peukert-Frowein, Art. 8, Rn. 5 m.w.N.

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

[44] Vgl. BVerfGE 65, 1 (42 und 49); BVerfGE 67, 100 (143); BVerfGE 77, 1 (46); BVerfGE 103, 21 (33); zu Art. 10: BVerfGE 100, 313 (366).

munikationsanbieter 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).

Daneben greift § 111 TKG auch in das Recht auf Achtung der Korrespondenz ein:

Der Gerichtshof hat wiederholt entschieden, dass Telefongespräche als „Korrespondenz" im Sinne des Art. 8 EMRK anzusehen sind[45]. Trotz des jedenfalls im Deutschen abweichenden Wortlauts ist diese Gleichstellung teleologisch geboten, weil sich der Bürger in beiden Fällen in einer vergleichbaren Gefährdungslage bezüglich seiner räumlich distanzierten Kommunikation befindet. Aus demselben Grund liegt es nahe, auch Telekommunikationsdaten unter den Begriff der „Korrespondenz" zu fassen. In vergangenen Urteilen hat der Gerichtshof wiederholt entschieden, dass die Erhebung von Verbindungsdaten ohne Einwilligung des Betroffenen einen Eingriff in dessen Rechte auf Achtung der Korrespondenz und des Privatlebens darstellt[46], weil Verbindungsdaten, „besonders die gewählten Nummern [...] integraler Bestandteil der Kommunikation" seien[47]. Im Zusammenhang mit der Identifizierung eines tatverdächtigen Internetnutzers durch den Internet-Zugangsanbieter hat der Gerichtshof entschieden, Nutzer von Telekommunikations- und Internetdiensten müssten sich darauf verlassen können, dass ihre Privatsphäre geschützt wird.[48]

Gleiches liegt der Empfehlung Nr. R (95)4 des Europarates zum Schutz persönlicher Daten im Bereich der Telekommunikationsdienste vom 7. Februar 1995 zugrunde.[49] Diese regelt die „Sammlung und Verarbeitung personenbezogener Daten im Bereich von Telekommunikationsdiensten"

---

[45] Frowein/Peukert-Frowein, Art. 8, Rn. 34 m.w.N.

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

[47] EGMR, Malone-GB (1984), EuGRZ 1985, 17 (23), Abs. 84.

[48] EGMR, K.U.-FI (2008), Reports of Judgments and Decisions 2008, Abs. 49.

[49] http://www.giodo.gov.pl/plik/id_p/31/j/en/.

einheitlich (Grundsatz 3). Als Oberbegriff wird „Servicedaten“ verwendet, womit Inhaltsdaten, Verkehrsdaten, Bestandsdaten und sonstige personenbezogene Daten gleichermaßen gemeint sind.[50] 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“.

Daten über die Identität von Telekommunikationsteilnehmern in den Schutzbereich des Rechts auf Achtung der Korrespondenz einzubeziehen, entspricht auch dem Zweck dieses Rechts, die Unbefangenheit der Fernkommunikation zu gewährleisten. 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 Telekommunikation[51] 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.“[52]

Die Empfehlung des Europarats über den Datenschutz in der Telekommunikation[53] 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 kom-

---

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

[51] Empfehlung R (95) 4 vom 07.02.1995.

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

[53] Empfehlung R (95) 4 vom 07.02.1995.

munizieren, weil sie zur „Untergrabung der Anonymität“ tendierten. Bedroht die Identifizierung von Teilnehmern aber die Kommunikationsfreiheit, so muss das Recht auf Achtung der Korrespondenz vor einer solchen Identifizierung schützen.

2. Mangelnde Rechtfertigung

Gerechtfertigt ist der mit § 111 TKG verbundene Eingriff in die Rechte der Beschwerdeführer nur, wenn er gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer (Art. 8 EMRK).

In einer demokratischen Gesellschaft erforderlich ist eine Maßnahme nur, wenn ein in Anbetracht des Stellenwerts des garantierten Freiheitsrechts hinreichend dringendes soziales Bedürfnis nach ihr besteht, sie einen legitimen Zweck verfolgt und ihre Belastungsintensität nicht außer Verhältnis zu dem Gewicht des Zwecks steht.[54] Der Gerichtshof hat dazu erklärt, dass das Interesse des Staates gegenüber den Interessen des Einzelnen an der Achtung seiner Privatsphäre abgewogen werden müsse.[55] Eingriffe sind zwar nicht auf das unerlässliche Maß beschränkt, aber ein bloßes Nützlich- oder Wünschenswertsein genügt nicht.[56]

Diese Rechtfertigungsvoraussetzungen fehlen im Fall des § 111 TKG: Die Vorschrift ist in Tragweite wie Auswirkungen nicht hinreichend vorhersehbar und schränkt das Recht auf Achtung der Privatsphäre und der Korrespondenz 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.

---

[54] EGMR, Sunday Times-GB (1979), EuGRZ 1979, 386 (389), Abs. 62; EGMR, Silver u.a.-GB (1983), EuGRZ 1984, 147 (152), Abs. 97; EGMR, Foxley-GB (2000), hudoc.echr.coe.int/Hudoc1doc2/HEJUD/200107/foxley%20-%2033274jv.chb3%2020062000e.doc, Abs. 43.

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

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

a) Mangelnde Vorhersehbarkeit und Präzision

Staatliche Stellen dürfen in die Privatsphäre von Menschen nur eingreifen, wenn der Eingriff gesetzlich vorgesehen ist (Art. 8 Abs. 2 EMRK). Aus dem Erfordernis einer gesetzlichen Grundlage in Verbindung mit dem in der Präambel der EMRK erwähnten Rechtsstaatsprinzip leitet der Gerichtshof ab, dass das eingreifende innerstaatliche Recht hinreichend bestimmt und für den Bürger zugänglich sein muss.[57] Dem Einzelnen muss es möglich sein, sein Verhalten den eingreifenden Vorschriften entsprechend einzurichten, was ein – gemessen an der Schwere des Eingriffs[58] – hinreichendes Maß an Vorhersehbarkeit voraussetzt.[59]

So hat der Gerichtshof im Fall einer Informationssammlung und -speicherung durch einen Geheimdienst entschieden, dass das nationale Recht detailliert festlegen muss, welche Arten von Informationen gespeichert werden dürfen, gegenüber welchen Personengruppen Überwachungsmaßnahmen ergriffen werden dürfen, unter welchen Umständen Informationen gesammelt werden dürfen, welches Verfahren dabei einzuhalten ist, nach welcher Zeitdauer erlangte Informationen zu löschen sind, welche Personen auf den Datenbestand zugreifen dürfen, die Art und Weise der Speicherung, das Verfahren des Informationsabrufs sowie die zulässigen Verwendungszwecke für die abgerufenen Informationen.[60]

Hieran gemessen, wird § 111 TKG dem Erfordernis einer vorhersehbaren und präzisen Regelung nicht gerecht, soweit er die Vergabe „anderer Anschlusskennungen“ als Rufnummern einem Identifizierungszwang unterwirft. Der Begriff der „anderen Anschlusskennung“ ist zu unbestimmt. Es fehlt an einer Definition des Begriffs der „Anschlusskennung“.

Der Rechtsausschuss des Deutschen Bundestages hat nur in seinem unverbindlichen Bericht ausgeführt, Anschlusskennung solle eine dem Anschlussinhaber dauerhaft zugewiesene Kennung (Zeichenfolge) sein, welche Telekommunikation, die vom Anschluss des Anschlussinhabers aus geführt werde, eindeutig und gleichbleibend kennzeichne und damit eine

---

[57] EGMR, Sunday Times-GB (1979), EuGRZ 1979, 386 (387), Abs. 49; EGMR, Silver u.a.-GB (1983), EuGRZ 1984, 147 (150), Abs. 87 und 88; EGMR, Lambert-F (1998), Decisions and Reports 1998-V, Abs. 23.

[58] EGMR, Kruslin-F (1990), Publications A176-A, Abs. 33.

[59] EGMR, Silver u.a.-GB (1983), EuGRZ 1984, 147 (150), Abs. 88; EGMR, Malone-GB (1984), EuGRZ 1985, 17 (20), Abs. 66; EGMR, Amann-CH (2000), Decisions and Reports 2000-II, Abs. 56.

[60] EGMR, Rotaru-ROM (2000), Decisions and Reports 2000-V, Abs. 57.

Funktion habe, die der Rufnummer im Telefoniebereich vergleichbar sei.[61] Als konkretes Beispiel wurden Kennungen von DSL-Anschlüssen genannt.[62] Mit dem Begriff der „anderen Anschlusskennung“ gemeint sind also offenbar nur die Kennungen physikalischer Telekommunikationsanschlüsse, ohne dass diese Frage aber gesetzlich geregelt worden wäre.

Die Regelung der Telekommunikationsüberwachung in § 100b der Strafprozessordnung verwendet ebenfalls den Begriff der Anschlusskennung. Hier wird als „andere Kennung“ jedoch auch eine IP-Adresse verstanden.[63] Würde § 111 TKG auf die Vergabe von IP-Adressen Anwendung finden, wären auch Anbieter von Internetcafés, Proxy-Servern, Anonymisierungsdiensten, WLAN-Internetzugängen verpflichtet, Nutzer zu identifizieren, weil sie diesen IP-Adressen zur Nutzung überlassen. Damit wäre der anonyme Zugang zum Internet gänzlich verboten, viele Dienste müssten wegen der Unpraktikabilität einer Identifizierung eingestellt werden.

Wegen der gravierenden Auswirkungen des Anonymitätsverbots des § 111 TKG ist die Vorschrift nicht hinreichend bestimmt, solange der Begriff der „anderen Anschlusskennung“ nicht eindeutig und vorhersehbar definiert wird.

b) Verletzung des Verhältnismäßigkeitsgebots

aa) Der erhoffte Nutzen des § 111 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 Verfassungsschutzbehörden 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 Verfügbar-

---

[61] BT-Drs. 16/6979, 69.

[62] Bundesregierung, BT-Drs. 16/5846, 68.

[63] Nack in KK-StPO, § 100b StPO, Rn. 8 m.w.N.

keit von Kundendaten zur Erfüllung staatlicher Aufgaben reduziere.[64] 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.[65] 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:

---

[64] Vgl. BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 217.

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

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,[66] während dasselbe Unternehmen heute – trotz eingebrochenen Marktanteils – 120 Mrd. Verbindungsdatensätze pro Jahr verarbeitet.[67] Laut Statistischem Bundesamt hat sich auch das gesamte Gesprächsvolumen in Fest- und Mobilfunknetzen von 2000 bis 2006 von Jahr zu Jahr erhöht[68] und war 2010 so hoch wie noch nie.[69] Laut Eurostat ist dieser jährliche Anstieg schon seit Beginn der Statistik im Jahr 1980 zu verzeichnen.[70] Einem Gesprächsvolumen von 1980 21 Mrd. Gesprächsminuten[71] standen 2008 306 Mrd. Gesprächsminuten[72] gegenüber. 3,6 Mrd. versandten Textnachrichten (SMS) im Jahr 1999 stehen 34 Mrd. versandten Textnachrichten im Jahr 2009 gegenüber.[73] 2002 korrespondierten 38% der Deutschen per E-Mail, 2010 bereits 73%.[74]

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 Bürgerange-

---

[66] Welp, TKÜV, 3 (9).

[67] AP-Meldung vom 02.06.2008, http://www.pr-inside.com/de/milliarden-datensaetze-im-jahr-r619791.htm.

[68] Statistisches Bundesamt, Entwicklung der Informationsgesellschaft (2007), http://www.destatis.de, 51.

[69] Bundesnetzagentur, Tätigkeitsbericht 2010/2011 vom Dezember 2011, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Presse/Berichte/2011/TaetigkeitsberichtTK20102011pdf.pdf;jsessionid=4DDD4A685A58781C4A40B234EA965540?__blob=publicationFile, 53.

[70] Eurostat, Inlandsgespräche (T501).

[71] Eurostat, Inlandsgespräche (T501).

[72] Eurostat, Ausgehender Verkehr aller Netzwerke (T500).

[73] Eurostat, Anzahl der SMS (T510).

[74] Eurostat, Senden/Empfangen von E-Mails (I_IUEM).

legenheiten oder politische Themen oder an Internet-Petitionen teil.[75] 54% beschaffen über das Internet gesundheitsrelevante Informationen.[76]

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 2000[77] auf 12.000 im Jahr 2011[78] angestiegen. Was das Internet-Nutzungsverhalten angeht, forderten deutsche Behörden im Jahr 2011 allein Google 2.491mal zur Offenlegung von Nutzerdaten auf, 2010 waren es nur 1.436 Anforderungen.[79] 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 Analysesysteme („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.

---

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

[76] Eurostat, Beschaffung von gesundheitsrelevanten Informationen (I_IHIF).

[77] Max-Planck-Institut, BT-Drs. 16/7434, 50.

[78] Bundesjustizamt, Übersicht Telekommunikationsüberwachung für 2010, http://www.bundesjustizamt.de/cln_115/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Uebersicht__Verkehrsdaten__2010,templateId=raw,property=publicationFile.pdf/Uebersicht_Verkehrsdaten_2010.pdf.

[79] Google Transparency Report, https://www.google.com/transparencyreport/userdatarequests/DE/?p=2011-12.

Die Bewertung eines Totalverbots anonymer Telekommunikations- und Internetanschlüsse 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 neben Deutschland nur wenige andere Staaten eine allgemeine Identifizierungspflicht für Inhaber von Telekommunikationsanschlüssen für erforderlich halten: Nach einem Bericht der EU-Kommission[80] und einer kanadischen Untersuchung[81] verpflichten nur neun EU-Mitgliedstaaten (Bulgarien, Dänemark, Deutschland, Frankreich, Griechenland, Italien, die Slowakei, Spanien und Ungarn) zur Identifizierung der Nutzer vorausbezahlter SIM-Karten. Teilweise sind vorausbezahlte SIM-Karten vorübergehend anonym nutzbar (Frankreich: 14 Tage). In 18 der 27 EU-Mitgliedsstaaten (Belgien, Estland, Finnland, Irland, Lettland, Litauen, Luxemburg, Malta, Niederlande, Österreich, Polen, Portugal, Rumänien, Schweden, Slowenien, Tschechien, Vereinigtes Königreich, Zypern) besteht keinerlei Identifizierungszwang für Inhaber von Telekommunikationsanschlüssen.[82] In zwei von drei EU-Mitgliedsstaaten werden Straftaten also auch ohne allgemeinen Identifizierungszwang verfolgt, obwohl auch dort ein Großteil der Mobiltelefonanschlüsse vorausbezahlt werden (Belgien: 56%, Estland: 61%, Finnland: 10%, Irland: 70%, Luxemburg: 36%, Niederlande: 39%, Österreich: 32%, Polen: 52%, Portugal: 73%, Schweden: 38%, Slowenien: 32%, Tschechien: 51%, Vereinigtes Königreich: 59%).[83] Dass Straftaten in diesen Ländern weniger erfolgreich als in Deutschland verfolgt würden, ist nicht ersichtlich. Auch in

---

[80] 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.

[81] Centre for Policy Research on Science and Technology of Simon Fraser University Vancoucer, Privacy Rights and Prepaid Communications Services vom März 2006, https://www.sfu.ca/cprost-old/docs/GowPrivacyRightsPrepaidCommServices.pdf, 3.

[82] Europäische Kommission, Room Document, http://www.vorratsdatenspeicherung.de/images/RoomDocumentEvaluationDirective200624EC.pdf, 11.

[83] OECD, Communications Outlook 2009, https://dwmw.files.wordpress.com/2011/06/oecd-commoutlook-2011.pdf, 164.

Deutschland selbst hat der Staat seine Aufgaben bis 2004 ohne Identifizierungspflicht erfüllt.

Dass die Aufgabenerfüllung durch § 111 TKG effektiviert worden wäre, ist nicht belegt oder sonst ersichtlich. Die am 26. Juni 2004 in Kraft getretene Norm 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.).[84] 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.[85] Dass das Internet auch ohne einen generellen und undifferenzierten Identifizierungszwang weit von einem rechtsfreien Raum entfernt ist, ergibt sich indes bereits daraus, dass 20 der 27 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 2004. Es ist nicht einmal belegt, dass der Identifizierungszwang überhaupt eine statistisch nachweisbare Auswirkung auf Aufklärungsquote oder gar Kriminalitätsrate hatte.

(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 leicht verhindern können.[86] Weil die Anbieter zur Überprüfung der Registrierungsangaben nicht verpflichtet sind (§ 95 Abs. 4 TKG), können bei der Anmeldung Fantasieangaben zu Name, Anschrift und Geburtsdatum gemacht

---

[84] Bundeskriminalamt, Polizeiliche Kriminalstatistik 2011 Kurzbericht, 31.

[85] BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 260.

[86] 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.

werden. Ebenso ist die anonyme Weitergabe bereits registrierter SIM-Karten (z.B. gegen Barzahlung) möglich und verbreitet. Viele Händer bieten vorregistrierte Karten an. Ferner können unschwer ausländische unregistrierte SIM-Karten in Deutschland eingesetzt werden. Zuletzt werden Straftäter auch vor dem Diebstahl von Mobiltelefonen mit SIM-Karte nicht zurückschrecken.

Die Folge von alledem ist, dass Straftäter auch nach Einführung des § 111 TKG Guthabenkarten ohne Weiteres einsetzen können, ohne sich identifizieren zu müssen. Gerade bei ernsthaften und daher wirklich gefährlichen Kriminellen wäre es naiv, anzunehmen, dass diese durch die Identifizierungspflicht dazu bewegt werden könnten, bei dem Kauf von Karten für ihr „Arbeitshandy“ brav ihre persönlichen Daten anzugeben. Die Identifizierungspflicht läuft damit faktisch leer[87] bzw. trifft im Wesentlichen nur ehrliche, rechtstreue Bürger.[88]

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*

---

[87] Rannenberg, Identity management in mobile cellular networks and related applications von 2004, http://www.web-portal-sys-tem.de/wps/wse/dl/down/open/rannenberg/f04fedba1e01ddee795db5ebd780739867943ed5b5acf594d3434521796aff787032c8635283ab3c3fed7d349270beae/Identitymanagementinmobilecell965.pdf, 83.

[88] 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.

werde innerhalb eines Jahres verschenkt, größtenteils innerhalb der Familie."[89]

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."[90]

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

---

[89] 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.

> *„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."*[91]

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.[92]

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."*[93]

---

[90] Bundesnetzagentur, Nummerierungskonzept 2011 vom 09.11.2011, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/Nummernverwaltung/Nummerierungskonzept/Nummerierungskonzept2011pdf.pdf?__blob=publicationFile, 24.

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

[92] Arbeitskreis Vorratsdatenspeicherung, Meinungsaustausch mit Strafverfolgern zur Vorratsdatenspeicherung vom 22.04.2012, http://www.vorratsdatenspeicherung.de/content/view/579/55/lang,de/.

[93] Generalstaatsanwaltschaft München vom Juni 2011, http://cryptome.org/isp-spy/munich-spy-all.pdf, 19.

Einer Studie der Bundesnetzagentur zufolge geben mindestens 10 % aller Prepaid-Nutzer von vornherein falsche Personalien an;[94] 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.[95] Es liegt auf der Hand, dass Straftäter in aller Regel zur Gruppe der nicht korrekt registrierten Kunden gehören.

(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.

(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.[96] Die meisten Ermittlungserfolge wegen Be-

---

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

[95] Bundesnetzagentur vom 09.11.2011, http://www.webcitation.org/69997Nqk8, 14.

[96] BVerfG, 1 BvR 1299/05 vom 24.1.2012, Abs. 135.

standsdaten 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.[97] 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).[98] 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).[99] 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.[100]

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 wögen Straftäter in Sicherheit, veranlassten diese zum Einsatz unregistrierter Karten und erlaubten dadurch deren Aufgrei-

---

[97] Generalstaatsanwaltschaft München vom Juni 2011, http://cryptome.org/isp-spy/munich-spy-all.pdf, 19.

[98] Vgl. Europäische Kommission, Room Document, http://www.vorratsdatenspeicherung.de/images/RoomDocumentEvaluationDirective200624EC.pdf, 11.

[99] 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.

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

fen, wo es andernfalls nicht möglich gewesen wäre.[101] 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.“[102]

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.[103]

(6) Zwischenergebnis

Insgesamt ist nicht belegt, dass ein Teil der strafrechtlichen Verurteilungen in Deutschland gerade auf § 111 TKG zurückzuführen sei. Alleine die Verfügbarkeit zusätzlicher Daten – korrekt oder inkorrekt – lässt auf einen effektiven Mehrwert für Zwecke der Strafverfolgung usw. nicht schließen.[104] Die Bundesrepublik hat es unterlassen, eine unabhängige wissenschaftliche Untersuchung über die Frage in Auftrag zu geben, ob § 111 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 Freiheitsvermutung[105] gehen daraus resultierende Zweifel zulasten des eingreifenden Staates. Auch die EU-Kommission stellt fest: „Bislang wurden keine Nachweise für die Wirksam-

---

[101] 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.

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

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

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

[105] Vgl. BVerfGE 6, 55 (72); BVerfGE 32, 54 (72); BVerfGE 55, 159 (165).

keit der einzelstaatlichen Maßnahmen vorgelegt."[106] Wissenschaftler bestätigen das Fehlen empirischer Wirksamkeitsnachweise.[107]

Vor diesem Hintergrund lässt sich nicht vertretbarerweise behaupten, dass die Identifizierungspflicht 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.[108]

In Sachen S. und Marper ist der Gerichtshof zutreffend der Behauptung der britischen Regierung entgegen getreten, die damals angefochtene biometrische Vorratsspeicherung sei „unabdingbar" zur Verfolgung von Straftaten.[109] Dieser Behauptung hat der Gerichtshof erstens entgegen gehalten, dass England die Maßnahme selbst erst 2001 eingeführt habe.[110] Zweitens hat er darauf hingewiesen, dass die Strafverfolgungsbehörden anderer Staaten auch ohne eine solche Maßnahme auskommen.[111]

Nichts anderes gilt auch für das deutsche Anonymitätsverbot. Als § 111 TKG im Jahr 2004 beschlossen wurde, wurden Mobilfunkkarten anonym

---

[106] 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.

[107] 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 Vancoucer, Privacy Rights and Prepaid Communications Services vom März 2006, https://www.sfu.ca/cprost-old/docs/GowPrivacyRightsPrepaidCommServices.pdf, 18.

[108] 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.

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

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

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

verkauft. Die Strafverfolgungsbehörden fast aller anderer demokratischer Staaten kommen bis heute ohne eine vergleichbare Maßnahme aus und leisten gleichwohl eine wirksame Strafverfolgung.

bb) Das Gewicht des mit § 111 TKG verbundenen Grundrechtseingriffs

Um die gebotene Abwägung vornehmen zu können, ist dem vermeintlichen öffentlichen Interesse an § 111 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.[112] Zu berücksichtigen ist auch, ob und in welcher Zahl Personen mitbetroffen werden, die für den Eingriff keinen Anlass gegeben haben.[113] Die Eingriffsintensität hängt bei Informationseingriffen unter anderem von Art, Umfang und denkbarer Verwendungen der erhobenen Daten sowie von der Gefahr ihres Missbrauchs ab.[114] 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.[115] 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.[116]

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

---

[112] Vgl. BVerfGE 109, 279 (353).

[113] Vgl. BVerfGE 109, 279 (353).

[114] Vgl. BVerfGE 65, 1 (46).

[115] Vgl. BVerfGE 100, 313 (376).

[116] Vgl. BVerfGE 65, 1 (45).

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 Missbrauches, das heißt unbegründete Befürchtungen dahin gehend, nicht zu berücksichtigen, weil grundsätzlich davon auszugehen ist, dass eine Norm „in einer freiheitlich-rechtsstaatlichen Demokratie korrekt und fair angewendet wird".[117] Eine reale Missbrauchsgefahr ist im Rahmen der Abwägung demgegenüber durchaus zu berücksichtigen.[118] Die Menschenrechte schützen den Einzelnen nämlich auch „vor fehlerhafter, missbräuchlicher oder exzessiver Verwertung von Kommunikationsdaten durch [...] staatliche Stellen".[119] Die „in der Gesprächsbeobachtung liegende Gefahr einer Menschenrechtsverletzung der [...] Gesprächsteilnehmer wie auch die Gefahr der Sammlung, Verwertung und Weitergabe der Informationen zu anderen Zwecken" als den gesetzlich vorgesehenen darf daher nicht aus den Augen verloren werden.[120] Wenn die EMRK das unbefangene Gebrauchmachen von Freiheiten in einer Demokratie 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.[121] 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 TKG ergibt: Zur Identifizierung von Kommunikationsteilnehmern werden Anbieter frei von jeder Voraussetzung und Eingriffsschwelle dauerhaft und allgemein – mithin global und pauschal[122] – verpflichtet. Es erfolgt eine flächendeckende Massener-

---

[117] Vgl. BVerfGE 30, 1 (27).

[118] Vgl. BVerfGE 65, 1 (45 f.).

[119] Vgl. BVerfGE 85, 386 (397).

[120] Vgl. BVerfGE 85, 386 (400).

[121] Vgl. BVerfGE 100, 313 (376).

[122] Vgl. BVerfGE 313, 100 (376 und 383).

fassung[123] der Identität unbescholtener und ungefährlicher Inhaber von Telekommunikationsanschlüssen. Beeinträchtigt sind sämtliche Grundrechtsträger, die einen Telekommunikationsanschluss unterhalten, und damit potenziell alle Bürger. Eine größere Zahl betroffener Grundrechtsträger infolge einer Grundrechtsbeschränkung ist kaum denkbar. Für ehrliche Personen, die bei Fragen nach ihrer Identität nicht lügen, gibt es praktisch keine Möglichkeit mehr, Ferngespräche anonym anzunehmen. Auch eine anonyme 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.[124] Die Aufzeichnung 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 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 oder der erforderlichen Bereitschaft, falsche Angaben zu machen, auf Dauer nicht möglich oder jedenfalls unzumutbar. Eine vorausbezahlte Karte auf einen falschen Namen zu registrieren, zieht verschiedene Risiken und Nachteile nach sich, selbst wo Normalbürger zu Falschangaben 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 an-

---

[123] Vgl. dazu BVerfGE 313, 100 (377).

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

gerufen werden kann. Die falschen 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.

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:[125]

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,

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

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 Gesichtsverlust (z.B. Auftreten unter dem anderen Geschlecht in einem Chatroom);
14. Schutz der eigenen Persönlichkeit, weil die eigene Identität andere schlichtweg nichts angeht;
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.[126]

(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.

[126] BVerfGE 65, 1 (43).

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.
- Europäische Journalisten, die in autoritären Staaten arbeiten, sind auf anonyme Fernkommunikation angewiesen, um Informationen sicher empfangen und nach Europa 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 Anonymität bereit, Auskunft zu geben. Im Wege anonymer Kommunikation gelingt es dann nicht selten, gravierende Missstände an das Licht der Öffentlichkeit zu bringen.
- Europäische 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 Identifizierungszwang 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.[127]

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

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

Personen, auf die Identität des Absenders der E-Mail oder des Lesers oder Verfassers einer Internetnachricht 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.

(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, 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.[128] 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 unbekannten) 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 vermittels 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 regelmä-

[128] BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 217.

ßig 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 aufgenommen 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 E-Mail verschickt, gibt dem Empfänger eine persönliche Absenderkennung (E-Mail-Adresse, IP-Adresse) 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 Gesprächs-

partnern 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. 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 betrieblich 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.[129] Das Recht soll die Bedingungen einer freien Fernkommunikation aufrechterhalten.[130] 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.[131]

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 eige-

---

[129] Vgl. BVerfG, Beschluss vom 27.7.2005, Az. 1 BvR 668/04, Abs. 81.

[130] 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.

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

nen Verbindungen, Aussagen, Bewegungen oder Interessen befürchten muss.

Der Erläuternde Bericht zur Empfehlung des Europarats zum Datenschutz in der Telekommunikation[132] 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.“[133]

Das Kommunikationsgeheimnis soll eine in allem vertrauliche Fernkommunikation ermöglichen.[134] Eine in allem vertrauliche Fernkommunikation ist aber nur im Schutz der Anonymität möglich. Art. 8 EMRK muss dazu gewährleisten, dass die Fernkommunikation im Alltag anonym erfolgen kann (entgegen § 111 TKG). 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.

---

[132] Empfehlung R (95) 4 vom 07.02.1995.

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

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

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, wovor sich die an einer Fernkommunikation Beteiligten nicht schützen können und was besonders unbemerkt und kostengünstig möglich ist.

Die Bundesrepublik weigert sich, der Identität von Anschlussinhabern den gleichen Schutz zukommen zu lassen wie sonstigen Umständen und Inhalten von Fernkommunikation. Zur Begründung führt sie an, 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.

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 ausgespähte 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.“*[135]

Das Bundesverfassungsgericht meint, der Informationsgehalt der nach § 111 TKG zu erhebenden Daten reiche „nicht sehr weit“.[136] 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.[137]

Bei dieser Betrachtungsweise droht jedoch die Funktion von Identitätsdaten als Schlüssel zu weiteren Kommunikationsdaten aus dem Blick zu geraten: 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

---

[135] LG Frankenthal, Beschluss vom 21.05.2008, Az. 6 O 156/08.

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

[137] BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 256.

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 vergleichbar. Vielmehr können Internet-Nutzungsdaten – anders als Videoaufzeichnungen – maschinell zugeordnet und ausgewertet werden und weisen daher eine besonders „hohe Sensitivität“ auf.[138] 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,[139] 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,

[138] Bundesregierung, Begründung zum TDDSG, BT-Drs. 13/7385, 25.

[139] Vgl. BVerfG MMR 2010, 356.

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.[140] 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.[141] 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.[142] Weiter konnte mit einer 90%igen Genauigkeit vorhergesagt werden, ob sich zwei Personen innerhalb der nächsten Stunde begegnen würden.[143] 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.[144] Auch die Zufriedenheit am Arbeitsplatz konnte anhand der Daten vorhergesagt werden.[145] Die weitere Forschung ar-

---

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

[141] MIT, Relationship Inference, http://reality.media.mit.edu/dyads.php.

[142] MIT, User Behavior Modeling and Prediction, http://reality.media.mit.edu/user.php.

[143] MIT, Relationship Inference, http://reality.media.mit.edu/dyads.php.

[144] MIT, Eigenbehaviors, http://reality.media.mit.edu/eigenbehaviors.php.

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

beitet daran, das Verhalten großer Organisationen und Gruppen anhand von Kommunikations- und Standortdaten vorherzusagen.[146]

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 die Adressen häufig besuchter Bekannter der Zielperson ermittelt.[147] 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.[148] Entscheidend sind Nutzbarkeit und Verwendungsmöglichkeit der Information.[149] Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den bestehenden Verarbeitungsmöglichkeiten und Verknüpfungsmöglichkeiten ab.[150]

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 ist 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.

---

[146] MIT, Machine Perception and Learning of Complex Social Systems, http://reality.media.mit.edu/.

[147] Deutschlandradio vom 02.07.2008, http://www.dradio.de/dlf/sendungen/forschak/810455/.

[148] BVerfGE 65, 1 (45).

[149] BVerfGE 65, 1 (45).

[150] BVerfGE 65, 1 (45).

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 ausforschen oder zuordnen 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) in der EG-Richtlinie 2006/24/EG vorgesehen ist. Unabhängig von der Frage der Vereinbarkeit dieses Instruments mit den Grundrechten ist festzustellen, dass in fast allen EU-Staaten sämtliche Kommunikations-, Bewegungs- und Internetzugangsdaten 6-24 Monate lang 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 Staate oder Dritte (z.B. Urheberrechteinhaber) schützen kann. Die EU-Richtlinie zur Vorratsdatenspeicherung schränkt die Zulässigkeit anonymer Kommunikationsdienste nicht ein, sondern setzt 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 der Auffassung, staatliche Bestandsdatenzugriffe hätten ein erheblich weniger belastendes Gewicht als die nahezu vollständige Speicherung der Daten sämtlicher Telekommunikati-

onsverbindungen auf Vorrat.[151] 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 deutsche Bundesverfassungsgericht wendet gleichwohl eine rein formale Betrachtungsweise an, derzufolge nur die veränderlichen Umstände (Verkehrsdaten) und Inhalte der Fernkommunikation 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).[152] § 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

[151] BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 257.

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

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“[153], 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.[154] Diese regelt die „Sammlung und Verarbeitung personenbezogener Daten im Bereich von Telekommunikationsdiensten“ einheitlich (Grundsatz 3). Als Oberbegriff wird „Servicedaten“ verwendet, womit Inhaltsdaten, Verkehrsdaten, Bestandsdaten und sonstige personenbezogene Daten gleichermaßen gemeint sind.[155] Auch die Weitergabe personenbezogener Daten wird einheitlich geregelt (Grundsatz 4). In Abs.

---

[153] Bundesregierung, BT-Drs. 16/12011, 34.

[154] http://www.giodo.gov.pl/plik/id_p/31/j/en/.

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

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 zur 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 Kommunikationen 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 Kommunikationsge-

heimnisses 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.[156]

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.[157] Es hat einen Eingriff in das Persönlichkeitsrecht bereits dann angenommen, wenn „die entscheidende technische Hürde für eine Ausspähung [...] des Systems genommen“ ist.[158] 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,

---

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

[157] BVerfG, Urteil vom 27.2.2008, Az. 1 BvR 370/07 , Abs. 181.

[158] BVerfG, Urteil vom 27.2.2008, Az. 1 BvR 370/07 , Abs. 205.

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 Auskunftersuchen dient, muss Art. 8 EMRK 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 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 Bundesrepublik 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 Einwohnermelderegelungen 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 minuziös nachvollzogen werden kann. Das Verhalten von Einwohnern

und von Fahrzeugführern wird demgegenüber – bislang – nicht protokolliert. Die Nutzbarkeit und Verwendungsmöglichkeit letzterer Daten ist daher sehr viel geringer.

(3) Die mit § 111 TKG verbundenen Risiken und Nebenwirkungen

Zur Prüfung der Verhältnismäßigkeit des § 111 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 Gerichtshof die Argumentation der britischen Regierung, die bloße Speicherung von Daten ohne ihre Nutzung könne sich auf die Betroffenen nicht nachteilig auswirken.[159] 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.[160]

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:[161]

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.[162] 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.

---

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

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

[161] BVerfGE 107, 299 (321).

Zweitens sind Kommunikationsdaten besonders anfällig für Ermittlungsfehler (z.B. Zahlendreher, Zeitstempel).[163] 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 Zeitzonenprobleme 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.[164] Wegen solcher Fehler wurden 2011 zwei unschuldige Menschen inhaftiert und beschuldigt.[165]

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.[166] 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.[167] Weil ein Kommunikationsdatensatz ein Indiz gegen den Angeklagten bilden

---

[162] Näher Breyer, NJOZ 2010, 1085.

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

[164] Interception of Communications Commissioner, 2011 Annual Report, http://www.intelligencecommissioners.com/docs/0496.pdf, 30.

[165] Interception of Communications Commissioner, 2011 Annual Report, http://www.intelligencecommissioners.com/docs/0496.pdf, 31.

[166] Verbraucherzentrale Bundesverband, Pressemitteilung vom 14.02.2012, http://www.vzbv.de/8829.htm.

[167] Hamm, TKÜV, 81 (86).

kann, muss dieser unter Umständen den Richter von seiner Unschuld überzeugen, um nicht zu Unrecht verurteilt zu werden.[168] 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, Untersuchungshaft, Bewegungseinschränkungen oder Aus- und Einreiseverboten zu führen, was mit schwerwiegenden Belastungen für die Betroffenen verbunden ist.

Folgende Fälle von Fehlurteilen aufgrund einer Analyse von Telekommunikationsdaten sind in Europa bereits bekannt geworden:

- In Österreich wurde ein Nigerianer mehrere Monate lang in Untersuchungshaft genommen, weil er wegen seiner zahlreichen Telefonkontakte als Anführer einer Rauschgiftbande in Verdacht geraten war.[169] Später stellte sich der Verdacht als unbegründet und der Nigerianer lediglich als gefragter Ratgeber in der schwarzen Gemeinschaft in Wien heraus.[170]
- In Schweden gab es Fälle, in denen unschuldige Personen im Zusammenhang mit Ermittlungen wegen Netzkriminalität festgenommen wurden. Später stellte sich heraus, dass die wirklichen Straftäter den Internet-Zugangscode der festgenommenen Personen ohne deren Kenntnis missbraucht hatten.[171]
- Zu Unrecht ins Visier der deutschen Kriminalpolizei ist ein 63-jähriger Mann aus Nürnberg geraten.[172] Er war angezeigt worden, da von seinem Internetanschluss aus kostenpflichtige Erotikseiten besucht wurden, ohne die angefallenen Kosten hierfür zu bezahlen. Das Fachdezernat der Kriminalpolizei konnte anhand der hinterlassenen „Internet-

---

[168] Lisken/Denninger, Handbuch des Polizeirechte (2001), C 26.

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

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

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

[172] Polizeipräsidium Mittelfranken, Zu Unrecht verdächtigt, 29.12.2006, http:// www.presseportal.de/ polizeipresse/ p_story.htx?nr=920697.

spuren“ (IP-Adressen) den 63-Jährigen als verantwortlichen Anschlussinhaber ermitteln. Der überraschte Mann versicherte jedoch, derartige Seiten niemals besucht zu haben. Durch weitere Ermittlungen kam man schließlich dem eigentlichen Täter auf die Spur. Er hatte den Internetzugang des zu Unrecht Verdächtigen über Funknetz (WLAN) genutzt.

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.[173]
- Ein Mitarbeiter des deutschen Bundesnachrichtendienstes, der mit der Überwachung der elektronischen Kommunikation betraut war, nutzte 2007 seine technischen Möglichkeiten privat. Er spähte den Email-

[173] The News.pl, Journalists' phones monitored in politically inspired investigation?, 8 October 2010, http://www.thenews.pl/1/9/Artykul/5241,Journalists-phones-monitored-in-politically-inspired-investigation.

Verkehr eines Deutschen aus, weil dieser ein Verhältnis mit der Ehefrau des BND-Mitarbeiters hatte.[174]

- 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.[175]
- 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.[176] Die Beamtin war in der für Terrorismus und organisierte Kriminalität zuständigen Abteilung der Zentrale der irischen Polizei für Telekommunikationsüberwachung zuständig.
- 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.[177]
- In Frankreich wertete der Inlandsgeheimdienst DCRI Verbindungsdaten aus, um die Quellen von Journalisten offenzulegen.[178] Zuvor hatte ein Staatsanwalt die Verbindungsdaten einer Richterin ausgewertet, um die Quellen investigativer Journalisten der Zeitung „Le Monde“ auf-

---

[174] 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.

[175] http://www.pragerzeitung.cz/?c_id=17621.

[176] http://www.webcitation.org/5xTUKdNqb.

[177] http://www.bigbrotherwatch.org.uk/Police_databases.pdf.

[178] http://www.sueddeutsche.de/medien/poltische-affaeren-erschuettern-frankreich-staatsspionage-gegen-journalisten-1.1144365.

zudecken[179] – wiederum eine Verletzung des Quellenschutzes, wie ein Gericht später feststellte.[180]

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.[181] Das mit Diskretion werbende Erotikunternehmen Beate Uhse veröffentlichte die E-Mail-Adressen Tausender von Personen, die sich Sexfilme im Internet angesehen hatten.[182] In einem Forum des ZDF-Kinderkanals konnten sich beliebige Personen Klarnamen, Adresse, Telefonnummer und Geburtsdatum aller 1.000 registrierter Kinder verschaffen.[183]

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 Char-

---

[179] http://www.oe24.at/welt/Sarkozy-droht-Spitzelaffaere/6900740.

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

[181] Spiegel 43/2008 vom 20.10.2008, Seite 70.

[182] 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.

[183] 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.

lotte Knobloch, Präsidentin des Zentralrats der Juden).[184] 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.[185] Zur Aufklärung des Datenlecks verletzte T-Mobile erneut das Fernmeldegeheimnis und überprüfte illegal Verbindungsdaten.[186]

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.[187]

Einen wirksamen Schutz vor derartigen Datenpannen und Missbrauch ermöglichen alleine anonyme Kommunikationsanschlüsse.[188] 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 inzwischen schon 80% der Bundesbürger „sehr besorgt“ um die Sicherheit ihrer Daten.[189] Eine deutliche Mehrheit der Bevölkerung fordert eine gesetzliche Stärkung des Datenschutzes.[190] 60% der Bürger sorgen sich, dass ihre Daten in die Hände Dritter gelangen könnten.[191]

---

[184] Spiegel vom 04.10.2008, http://www.spiegel.de/wirtschaft/0,1518,581938,00.html.

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

[186] Heise Online vom 29.10.2008, http://heise.de/-214133.

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

[188] Gola/Klug/Reif, Datenschutz- und presserechtliche Bewertung der „Vorratsdatenspeicherung“ (2007), 38; Rusteberg, VBlBW 2007, 171 (175).

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

[190] Emnid-Umfrage vom 02.06.2008, http://www.presseportal.de/pm/13399/1204206/n24/rss.

[191] Microsoft, Umfrage vom Februar 2008, http://www.daten-speicherung.de/?p=267.

53% der Deutschen haben im Internet schon einmal eine andere Identität verwendet.[192] Jeder vierte Internet-Nutzer ist zum Schutz seiner Daten sogar immer oder vorwiegend unter Fantasienamen im Internet unterwegs.[193] Auf diese Weise wollen die Bürger einen Missbrauch ihrer Daten verhindern, Internetangebote anonym nutzen und sich dagegen wehren, dass unangemessen viele Daten abgefragt werden.[194]

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 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 verdächtig zu erschei-

---

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

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

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

nen. 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 telefo-

nisch 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 Sozial-

pädagoge 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.[195] 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.[196] 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.[197]

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 Nachteile 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 Fäl-

[195] http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf.

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

[197] a.a.O., 22.

len 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.[198] 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.[199] 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.[200]

(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.[201]

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 Informatio-

---

[198] 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.

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

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

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

nen über Telekommunikationsteilnehmer anordnen, nicht aber generell und undifferenziert.

(f) Drohender Dammbruch

Wir machen den Gerichtshof darauf aufmerksam, dass die Maßstäbe, die er in der vorliegenden Entscheidung entwickelt, auch in anderen Bereiche angewandt werden 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 im Fall des § 111 TKG würde allgemein einen Dammbruch für den Schutz der Privatsphäre bedeuten. Der Zwang zur anlasslosen Erfassung 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.[202] Aus jedem personenbezogenen Datum können sich im Einzelfall einmal Schlüsse bezüglich einer Gefahr oder Straftat ergeben. Das Grundrecht auf Achtung 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.

---

[202] Klug/Reif, RDV 2008, 89 (93).

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 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 vor dem Bundesverfassungsgericht tatsächlich argumentiert, der Staat dürfe Informationen überall dort erheben, wo er sie finden könne, selbst wenn die Betroffenen vollkommen unverdächtig, ungefährlich und unbeteiligt seien.[203] 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,[204] 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 Identifizierungspflicht im deutschen Recht bisher einmalig. Selbst auf dem Gebiet des Zahlungsverkehrs gewährleisten Bargeld und die Möglichkeit von Bareinzahlungen gewährleisten 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 der Menschenrechtskonvention (z.B. Art. 10, Art. 11 EMRK) und für die unbefangene Mitwirkung der Bürger in einem demokratischen Staat.

---

[203] Stellungnahme des Bevollmächtigten der Bundesregierung vom 31.01.2007, http://daten-speicherung.de/data/TKG-StN.pdf, 65.

[204] Stellungnahme des Bevollmächtigten der Bundesregierung vom 31.01.2007, http://daten-speicherung.de/data/TKG-StN.pdf, 65 f. und 91 f.

Das deutsche Bundesverfassungsgericht hat eine anlasslose Vorratsspeicherung aller Verbindungs- und Bewegungsdaten sinngemäß mit dem Argument akzeptiert, elektronische Kommunikationsspuren seien besonders flüchtig.[205] 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.

Nach dem Willen des Bundesverfassungsgerichts sollte seine Entscheidung zur Vorratsspeicherung von Verkehrsdaten auf andere Datensammlungen nicht übertragen werden. Die Verkehrsdatenspeicherung sollte eine „Ausnahme" bleiben.[206] 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.[207] Hier wird der drohende Dammbruch offenbar. Erklärte der Gerichtshof 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.[208]

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 der Menschenrechtskonvention vor Augen stand.

---

[205] Vgl. BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 260.

[206] BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 218.

[207] BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 138.

[208] BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 218.

cc) Abwägung

In einer demokratischen Gesellschaft erforderlich ist eine Maßnahme nur, wenn ein in Anbetracht des Stellenwerts des garantierten Freiheitsrechts hinreichend dringendes soziales Bedürfnis nach ihr besteht, sie einen legitimen Zweck verfolgt und ihre Belastungsintensität nicht außer Verhältnis zu dem Gewicht des damit verfolgten Zwecks steht.[209] Die nachteiligen Auswirkungen des Eingriffs dürfen nicht schwerer wiegen als die zur Rechtfertigung des Eingriffs angeführten Gründe.[210]

(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.[211] 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.*“[212]

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 un-

---

[209] EGMR, Sunday Times-GB (1979), EuGRZ 1979, 386 (389), Abs. 62; EGMR, Silver u.a.-GB (1983), EuGRZ 1984, 147 (152), Abs. 97; EGMR, Foxley-GB (2000), hudoc.echr.coe.int/Hudoc1doc2/HEJUD/200107/foxley%20-%2033274jv.chb3%2020062000e.doc, Abs. 43.

[210] EGMR, Dudgeon-GB (1981), Publications A45, Abs. 60.

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

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

terschiedslose 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 Millionen 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 Identi-

fizierung 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 viele Fällen ein erfolgreicher Abruf auch tatsächlich zur Verurteilung eines Straftäters geführt habe.[213] Auch sei nicht dargelegt, in wie vielen Fällen hierfür gerade die Vorratsspeicherung der Daten Nichtverurteilter erforderlich gewesen sei.[214] Die meisten der von der Regierung genannten erfolgreichen Abrufe wären auch ohne die beanstandete Vorratsspeicherung möglich gewesen.[215] Wenngleich der Gerichtshof im Ergebnis davon ausging, dass die Vorratsspeicherung biometrischer Daten aller Tatverdächtiger einen gewissen Beitrag zur Strafverfolgung leistete,[216] 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 Internetanschlussinhaber. 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

---

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

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

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

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

Gefahr geführt hat. Vor allem ergibt sich aus der Zugriffsstatistik nicht, in wie vielen Fällen 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.

Die Menschenrechte der EMRK verlangen von den Unterzeichnerstaaten, 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.

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

Soweit der Gerichtshof in einer Kammerentscheidung Finnland verurteilt hat, weil dessen Gesetze im Jahr 1999 die Aufklärung einer im Internet begangenen Straftat nicht zuließen,[217] steht dies der Unverhältnismäßigkeit einer generellen und undifferenzierten Identifizierungspflicht nicht entgegen, weil diese Entscheidung eine andere Fallgestaltung betraf:

[217] EGMR, K.U.-FI vom 02.12.2008, 2872/02.

In jenem Fall verfügte der finnische Internetanbieter über Daten, die eine Identifizierung des mutmaßlichen Täters ermöglicht hätten;[218] das finnische Recht erlaubte die Herausgabe dieser Daten aber nicht.[219] 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.[220] Dieses Gesetz sah eine Befugnis zur Identifizierung von Kommunikationsteilnehmern auf richterliche Anordnung vor,[221] nicht jedoch eine anlasslose und flächendeckende Identifizierungspflicht, die es in Finnland bis heute nicht gibt.

(3) Weitere Rechtsprechung

Nach der Rechtsprechung des Bundesverfassungsgerichts können auf eine Norm, welche die Erhebung personenbezogener Daten lediglich durch das Gebot der Erforderlichkeit zur Erfüllung bestimmter Aufgaben begrenzt, keine Grundrechtseingriffe von erheblichem Gewicht gestützt werden.[222] § 111 TKG ermächtigt zu tiefgreifenden Grundrechtseingriffen, begrenzt die Erhebung personenbezogener Daten aber lediglich durch das Gebot der Erforderlichkeit zur Erfüllung bestimmter Aufgaben. Dies genügt dem Verhältnismäßigkeitsgebot nicht.

Mit Urteil vom 04.04.2006 hat das Bundesverfassungsgericht ausgesprochen:

---

[218] EGMR, K.U.-FI vom 02.12.2008, 2872/02, Abs. 9.

[219] EGMR, K.U.-FI vom 02.12.2008, 2872/02, Abs. 40.

[220] EGMR, K.U.-FI vom 02.12.2008, 2872/02, Abs. 49.

[221] EGMR, K.U.-FI vom 02.12.2008, 2872/02, Abs. 21.

[222] BVerfG, NVwZ 2007, 688, Abs. 53 f.

„Die Anforderungen an den Wahrscheinlichkeitsgrad und die Tatsachenbasis der Prognose dürfen allerdings nicht beliebig herabgesenkt werden, sondern müssen auch in angemessenem Verhältnis zur Art und Schwere der Grundrechtsbeeinträchtigung und zur Aussicht auf den Erfolg des beabsichtigten Rechtsgüterschutzes stehen. Selbst bei höchstem Gewicht der drohenden Rechtsgutbeeinträchtigung kann auf das Erfordernis einer hinreichenden Wahrscheinlichkeit nicht verzichtet werden."[223] *„Der Grundsatz der Verhältnismäßigkeit führt dazu, dass der Gesetzgeber intensive Grundrechtseingriffe erst von bestimmten Verdachts- oder Gefahrenstufen an vorsehen darf [...] Verzichtet der Gesetzgeber auf begrenzende Anforderungen an die Wahrscheinlichkeit des Gefahreneintritts sowie an die Nähe der Betroffenen zur abzuwehrenden Bedrohung und sieht er gleichwohl eine Befugnis zu Eingriffen von erheblichem Gewicht vor, genügt dies dem Verfassungsrecht nicht."*[224]

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.[225] Eine allgemeine Bedrohungslage, deren Realisierung „praktisch nie ausgeschlossen" ist, genügt dem nicht.[226] 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.[227]

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 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

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

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

[225] BVerfGE 115, 320 (320), Ls. 1.

[226] BVerfGE 115, 320 (364).

[227] BVerfGE 115, 320 (359).

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.

Soweit das Bundesverfassungsgericht mit Urteil vom 2. März 2010 eine anlasslose, flächendeckende Vorratsdatenspeicherung unter bestimmten Voraussetzungen als verhältnismäßig bezeichnet hat, kann dies nicht überzeugen. Dem Urteil fehlt eine Auseinandersetzung mit den empirischen Nachweisen des eklatanten Missverhältnisses zwischen Tragweite einer Vorratsdatenspeicherung auf der einen und ihrem Ertrag auf der anderen Seite. Auch fehlt 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 EGMR[228] und des Verfassungsgerichtshofs Rumäniens[229] auseinander, obwohl das Grundgesetz nach Möglichkeit konventionskonform auszulegen ist.[230] Dem Urteil fehlt auch eine Auseinandersetzung mit der früheren Rechtsprechung des Bundesverfassungsgerichts, mit welcher eine allumfassende, permanente Vorratsdatenspeicherung nicht in Einklang zu bringen ist.[231] Die Entscheidung ist dementsprechend vom Bundesdatenschutzbeauftragten[232] und in der Literatur[233] kritisiert worden. Eine inhaltliche Widerlegung der Argumente des Bundesverfassungsgerichts ist hier nicht im Einzelnen vorzunehmen. Es genügt die Anmerkung, dass das Bundesverfassungsgericht seine Rechtsprechung bereits in anderen Fällen im Hinblick auf ein höheres europäisches Grundrechtsschutzniveau korrigieren musste.[234] Das Urteil behandelt im Übrigen die Zulässigkeit einer Identifizierungspflicht nicht, sondern setzt sich nur mit der Zulässigkeit einer Aufbewahrungspflicht für betrieblich ohnehin anfallende Daten auseinander. Ob ohnehin vorhandene

---

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

[229] Verfassungsgerichtshof Rumäniens, 1258 vom 08.10.2009, http://www.vorratsdatenspeicherung.de/content/view/342/79/lang,de/.

[230] BVerfG, 2 BvR 1481/04 vom 14.10.2004, Absatz-Nr. 32.

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

[232] http://www.daten-speicherung.de/index.php/ziercke-greift-ak-vorrat-an/.

[233] Forgó/Grügel, K&R 2010, 218 ff.

[234] BverfG NJW 2008, 1793 – Caroline II; BVerfG NJW 2011, 1931 – Sicherungsverwahrung II.

Daten unter bestimmten Voraussetzungen gespeichert oder beauskunftet werden müssen oder ob die anonyme Überlassung von Anschlüssen allgemein verboten wird, stellt einen grundlegenden Unterschied dar.

Anders als das Bundesverfassungsgericht hat der rumänische Verfassungsgerichtshof die Europäische Menschenrechtskonvention zum Maßstab seiner Prüfung eines Gesetzes zur Vorratsdatenspeicherung gemacht und eine Verletzung des Art. 8 EMRK festgestellt. Der Gerichtshof führte in der Begründung seines Urteils vom 08.10.2009 aus, dass das Gesetz zur Vorratsdatenspeicherung die in der Strafprozessordnung vorgesehenen Ausnahmen vom Fernmeldegeheimnis „zur Regel" mache. Im Fall einer Vorratsdatenspeicherung könne von Fernmeldegeheimnis und Meinungsfreiheit nicht mehr „frei und unzensiert Gebrauch gemacht werden". Eine allgemeine Vorratsdatenspeicherung wecke in den Menschen „die berechtigte Sorge um die Wahrung ihrer Privatsphäre und die Furcht vor einem möglichen Missbrauch". Die dauerhafte und die gesamte Bevölkerung betreffende Vorratsdatenspeicherung drohe die Unschuldsvermutung „auszuhebeln", erkläre die gesamte Bevölkerung zu potenziellen Straftätern und erscheine „exzessiv". Die Erfassung aller Verbindungsdaten könne deshalb „nicht als vereinbar mit den Bestimmungen der Verfassung und der Europäischen Menschenrechtskonvention erachtet werden".[235]

2011 hat sich dann auch der tschechische Verfassungsgerichtshof nicht überzeugt gezeigt, dass eine unterschiedslose und vorsorgliche Speicherung von Verkehrsdaten nahezu jeder elektronischer Kommunikation im Hinblick auf die Intensität des Eingriffs und die Vielzahl der privaten Nutzer elektronischer Kommunikation erforderlich und verhältnismäßig sei.[236] Der Verfassungsgerichtshof äußerte mit Blick auf die vielfältigen Umgehungsmöglichkeiten Zweifel daran, ob eine unterschiedslose und vorsorgliche Speicherung von Verkehrsdaten ein wirksames Mittel ist, um ihren ursprünglichen Zweck (Schutz vor Gefahren und Verhütung besonders schwerer Straftaten) zu erreichen. Eine Analyse von Zahlen des deut-

[235] Englische Urteilsübersetzung: http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html, deutsche Urteilsübersetzung: http://www.vorratsdatenspeicherung.de/content/view/342/1/lang,de/#Urteil.

[236] Urteil vom 22.03.2011, 24/10, englische Urteilsübersetzung: http://www.concourt.cz/clanek/pl-24-10, deutsche Urteilsübersetzung (Auszug): http://www.vorratsdatenspeicherung.de/content/view/437/79/lang,de/.

schen Bundeskriminalamts habe zu dem Ergebnis geführt, dass die unterschiedslose und vorsorgliche Speicherung von Verkehrsdaten wenig Auswirkungen bei der Verringerung der Zahl der begangenen schweren Straftaten hatte.

(4) Kein fairer Ausgleich der widerstreitenden Interessen

Zusammenfassend ist festzuhalten, dass ein dringendes soziales Bedürfnis nach einem Verbot anonymer Telefon- und Internetanschlüsse nicht auszumachen ist. 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 Identifizierungspflicht kommunizieren Straftäter nach Angaben von Strafverfolgern regelmäßig nicht unter ihrer wahren Identität. Da die Behörden von zwei Dritteln aller europäischen Staaten ihre Aufgaben ohne ein Verbot anonymer Telefon- und Internetanschlüsse wirksam wahrnehmen, besteht augenscheinlich kein dringendes soziales Bedürfnis nach einer solchen Maßnahme.

Umgekehrt besteht ein dringendes soziales 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 Identifizierungspflicht belastet unbescholtene Bürger in ganz erheblichem Maße, weil diesen eine anonyme Telekommunikationsnutzung in weiten Bereichen unmöglich gemacht wird. Nur ohne Identifizierungszwang 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 Identifizierungszwang 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 TKG vorgesehenen allgemeinen Registrierungszwangs in keinem Verhältnis zu dem erhofften Zusatznutzen einer solchen Maßnahme für die von der Bundesrepublik angestrebten Zwecke steht. Der gesamten Bevölkerung anonyme Telekommunikation 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 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 Rechte auf Achtung des Privatlebens und der Korrespondenz dar und kann nicht als notwendig in einer demokratischen Gesellschaft angesehen werden.

Der Wunsch, Rechtsgüter zu schützen, kann das Recht auf unbefangene und anonyme Information und Kommunikation allgemein nicht aufheben. Die EMRK setzt ersichtlich auf ein weitaus voraussetzungsreicheres System des Rechtsgüterschutzes als eine generelle und undifferenzierte Aufzeichnung 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 offen-

zulegen. In einer Demokratie erfolgt der Rechtsgüterschutz gezielt und anlassbezogen und nicht durch Totalkontrolle und -erfassung jeglicher Informations- und Kommunikationsteilnehmer.

Die Bundesrepublik argumentiert, Telekommunikation weise ein spezifisches Gefahrenpotential auf. Sie erleichtere die Begehung klassischer Straftaten und habe neue Formen von Straftaten hervor gebracht, deren Begehung sich „weithin der Beobachtung“ entziehe.[237]

Richtig ist, dass Telekommunikation die Begehung klassischer Straftaten erleichtern kann. Auf der anderen Seite erleichtert sie aber die Aufklärung klassischer Straftaten enorm. Immer häufiger nutzen Ermittler Telekommunikationsdaten zur Aufklärung von Straftaten (z.B. Bewegungsdaten) – Informationen, die ohne Telekommunikation und Internet nicht für die Ermittlungsarbeit zur Verfügung stünden. So ist die Zahl der Verkehrsdatenzugriffe von ca. 5.000 im Jahr 2000[238] auf 12.000 im Jahr 2011[239] angestiegen.

Richtig ist auch, dass die Telekommunikation neue Formen von Straftaten hervor gebracht hat, nämlich Angriffe auf die Vertraulichkeit, Integrität oder Verfügbarkeit von Computersystemen unter Verwendung von Telekommunikationsnetzen (beispielsweise durch „Hacking“). Dass sich die Begehung dieser Straftaten „weithin der Beobachtung“ entziehe, mag zutreffen. Vergleichbare Straftaten außerhalb der Telekommunikationsnetze entziehen sich jedoch ebenfalls „weithin der Beobachtung“.

Datenveränderung und Computersabotage (§§ 303a, 303b StGB) können als moderne Form der Sachbeschädigung (§ 303 StGB) angesehen werden. Im Jahr 2011 sind knapp 700.000 Fälle von Sachbeschädigung bei einer Aufklärungsquote von 25% verzeichnet worden.[240] Demgegenüber sind im gleichen Jahr knapp 5.000 Fälle von Datenveränderung und Computersabotage bei einer Aufklärungsquote von 41% verzeichnet worden.[241] Der unerwünschte Zugriff auf fremde Sachen und Anlagen entzieht

---

[237] BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 216.

[238] Max-Planck-Institut, BT-Drs. 16/7434, 50.

[239] Bundesjustizamt, Übersicht Telekommunikationsüberwachung für 2010, http://www.bundesjustizamt.de/cln_115/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Uebersicht__Verkehrsdaten__2010,templateId=raw,property=publicationFile.pdf/Uebersicht_Verkehrsdaten_2010.pdf.

[240] Bundeskriminalamt, Kriminalstatistik 2011 Kurzbericht, 5.

[241] Bundeskriminalamt, Kriminalstatistik 2011 Kurzbericht, 56.

sich somit stets „weithin der Beobachtung“. Im Bereich der Kommunikationsnetze ist eher eine höhere Aufklärbarkeit gegeben.

Spezifischen Gefahren der Telekommunikation und damit einher gehend einem besonderen Aufklärungsinteresse kann auch ohne generelles und undifferenziertes Anonymitätsverbot Rechnung getragen werden, wie die allermeisten europäischen Staaten zeigen. Die Rekonstruktion und Überwachung der Telekommunikation ist technikbedingt ohnehin sehr viel leichter, geheimer und kostengünstiger zu bewerkstelligen als die Rekonstruktion und Überwachung unmittelbarer oder postalischer Kommunikation. Dementsprechend liegt die polizeiliche Aufklärungsquote im Bereich der Straftaten mit Tatmittel Internet bei etwa 65% der bekannt gewordenen Internetkriminalität und übersteigt damit die durchschnittliche Aufklärungsquote von Straftaten deutlich (2011: 54,7%). Der am 26. Juni 2004 in Kraft getretene § 111 TKG 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.).[242]

Der Bundesdatenschutzbeauftragte sowie die Datenschutzbeauftragten von 14 Bundesländern sehen in der generellen und undifferenzierten Identifizierungspflicht des § 111 TKG eine Verletzung des Verhältnismäßigkeitsgebots.[243] Derselben Meinung ist der niederländische Datenschutzbeauftragte.[244]

Die konkrete Ausgestaltung der Identifizierungspflicht in § 111 TKG verstärkt deren allgemeine Unangemessenheit. § 111 TKG schreibt nämlich nicht vor, dass die Angaben von Kunden bezüglich ihrer persönlichen Daten überprüft werden müssen. Eine Nachprüfung der Angaben anhand eines Ausweisdokuments, wie es eine Entscheidung des OVG Münster und ein Kabinettsbeschluss aus dem Jahr 2002 noch vorsahen, schreibt § 111 TKG nicht mehr vor. Vielmehr ist es nach § 95 Abs. 4 TKG den Anbietern überlassen, ob sie sich einen Ausweis vorzeigen lassen oder nicht. Müs-

---

[242] Bundeskriminalamt, Polizeiliche Kriminalstatistik 2011 Kurzbericht, 31.

[243] BVerfG, 1 BvR 1299/05 vom 24.1.2012, Absatz-Nr. 91 ff.

[244] Data Protection Authority of the Netherlands, Stellungnahme vom 12.11.2009, http://ec.europa.eu/dgs/home-affairs/what-is-new/public-consultation/2009/pdf/0008/contributions/dpa/reply_nl_dpa_en.pdf, 5.

[245] OVG Münster, MMR 2002, 563 (563).

[246] Kabinettbeschluss des Bundesregierung vom 17.04.2002, www.dud.de/dud/-documents/tkg-aend-e-020417.pdf.

sen die von Kunden angegebenen persönlichen Daten demnach in keiner Weise überprüft werden, dann ist die „Identifizierungspflicht" des § 111 TKG ohnehin Makulatur. Dasselbe gilt im Hinblick auf die Nutzbarkeit ausländischer anonymer Karten in Deutschland. Die vielfältigen Möglichkeiten zur Umgehung der Bestandsdatenerhebung, angefangen mit dem Tausch vorausbezahlter Telefonkarten, lassen den behaupteten Nutzen der Regelung weit hinter den mit ihr verbundenen Schaden zurücktreten.

Auf dem Gebiet der Verschlüsselung hat die Politik erkannt, dass die Gewährleistung der Vertraulichkeit der Telekommunikation wichtiger ist als die marginalen Sicherheitsgewinne, die eine Kryptoregulierung bestenfalls bewirken könnte. Nicht anders verhält es sich in Bezug auf das Recht auf anonyme Telekommunikation.

3. Ergebnis zu Art. 8 EMRK

§ 111 TKG verletzt die Rechte der Beschwerdeführer auf Achtung des Privatlebens und der Korrespondenz in den folgenden Punkten:

- § 111 TKG regelt den Kreis der betroffenen Anschlüsse und Technologien nicht mit hinreichender Präzision.
- Die in § 111 TKG angeordnete generelle und undifferenzierte Erfassung der Identität aller Inhaber von Telekommunikations- und Internetanschlüssen auf Vorrat, die – wie die Beschwerdeführer – einer Straftat nie auch nur verdächtig waren, stellt einen unverhältnismäßigen Eingriff in die Rechte der Betroffenen auf Achtung ihres Privatlebens und ihrer Korrespondenz dar und kann nicht als notwendig in einer demokratischen Gesellschaft angesehen werden.

II. Verletzung des Art. 10 EMRK

1. Schutzbereich

Art. 10 Abs. 1 S. 1 und 2 EMRK bestimmt:

> *„Jeder hat Anspruch auf freie Meinungsäußerung. Dieses Recht schließt die Freiheit der Meinung und die Freiheit zum Empfang und zur Mitteilung von Nachrichten oder Ideen ohne Eingriffe öffentlicher Behörden und ohne Rücksicht auf Landesgrenzen ein."*

Art. 10 EMRK schützt unter anderem die Mitteilung und den Empfang von Tatsachen und Meinungen[247]. In technischer Hinsicht geschützt sind alle

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

Kommunikationsformen[248], also auch die Nutzung der Telekommunikationsnetze. Es kommt nicht darauf an, ob es sich um private oder um öffentliche, um individuelle oder um Massenkommunikation handelt[249].

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[250] 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.

In einer späteren Entscheidung[251] 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.[252] Es müsse möglich bleiben, anonym Mitglied eines unbeliebten Vereins zu sein, um die Freiheit auch unpopulärer Meinungen zu gewährleisten.

---

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

[249] Vgl. Frowein/Peukert-Frowein, Art. 10, Rn. 15 ff.

[250] 362 U.S. 60 (1960).

[251] McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995).

[252] NAACP v. Alabama ex. rel. Patterson, 357 U.S. 449 (1958).

Gewährleistet ist schließlich auch das Recht, sich anonym zu informieren.[253] 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,[254] 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.“[255] Larios hat eine Übersicht über die US-amerikanische Rechtsprechung zum Schutz der Anonymität von Internetnutzern durch das Grundrecht auf freie Meinungsäußerung veröffentlicht.[256]

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

---

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

[254] Doe v. 2TheMart.com, 140 F.Supp.2d 1088.

[255] Doe v. 2TheMart.com, 140 F.Supp.2d 1088.

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

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.[257] 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 verfälschen. 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 inzwischen der Bundesgerichtshof anerkannt, dass Art. 5 GG das Recht auf anonyme Meinungsäußerung im Internet schützt.[258]

2. Eingriff

§ 111 TKG greift in das Recht der Beschwerdeführer auf anonyme Meinungsäußerung ein, indem er den Beschwerdeführern die – auch im Ver-

---

[257] 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.

[258] BGHZ 181, 328, Abs. 50 ff.

hältnis zu Anbieter und Staat – anonyme Äußerung und Entgegennahme von Meinungen und Informationen über einen eigenen Telefon- oder Internetanschluss unmöglich oder jedenfalls unzumutbar[259] macht. § 111 TKG hindert die Beschwerdeführer daran, über ihre Mobiltelefonkarten anonym und ohne Furcht vor nachteiligen Konsequenzen ihre Meinung oder sonstige Informationen weiterzugeben oder entgegenzunehmen.

3. Mangelnde Rechtfertigung

Gemäß Art. 10 Abs. 2 EMRK kann die Ausübung der in Art. 10 Abs. 1 EMRK genannten Freiheiten eingeschränkt werden, und zwar unter anderem im Interesse der öffentlichen Sicherheit, der Verbrechensverhütung und des Schutzes der Rechte anderer. Hierbei gelten allerdings dieselben einschränkenden Voraussetzungen wie bei Eingriffen in Art. 8 EMRK, insbesondere das Verhältnismäßigkeitsprinzip.

Was den erhofften Nutzen des § 111 TKG angeht, ist zu Art. 8 EMRK bereits ausgeführt worden, dass ein statistisch signifikanter Mehrwert der Norm bei der Verfolgung von Straftätern oder bei sonstigen Staatsaufgaben nicht belegt ist und dass die große Mehrzahl europäischer Staaten ihre staatlichen Aufgaben ohne ein generelles Verbot anonymer Telekommunikations- und Internetanschlüsse erfüllt.

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

Die in § 111 TKG vorgesehene Identifizierung und Registrierung aller Telekommunikationsteilnehmer ermöglicht Staatsbediensteten 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-Meinungsforen[260] oder Kontaktformulare in Rede steht. Sonstigen Informations- und Mei-

---

[259] Näher Seite 33.

[260] 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.

nungsaustausch 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, verdeutlichen aktuelle Umfragen: 73% der Deutschen tauschen danach inzwischen ihre Meinung über das Internet aus (E-Mails),[261] 33% senden Nachrichten über soziale Netzwerke oder Instant Messaging,[262] 18% telefonieren über das Internet.[263] 44% nutzen soziale oder berufliche Netzwerke im Internet.[264] 70% der Deutschen informieren sich online über Waren und Dienstleistungen.[265] 52% lesen über das Internet Online-Zeitungen und Nachrichtenmagazine.[266] 25% hören im Internet Radio oder sehen fern.[267] 58% informieren sich in Online-Lexika wie Wikipedia.[268] 38% nutzen das Internet für Zwecke der Ausbildung oder Weiterbildung.[269] 18% suchen im Internet nach einer Arbeitsstelle.[270] 22% veröffentlichen eigene Inhalte im Internet.[271] 23% lesen oder verfassen Meinungsbeiträge über Bürgerangelegenheiten oder politi-

---

[261] Eurostat, Senden/Empfangen von E-Mails (I_IUEM).

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

[263] Eurostat, Telefonieren oder Videoanrufe (I_IUPH1).

[264] Eurostat, Nutzen von sozialen oder professionellen Netzwerken (I_IUNET).

[265] Eurostat, Suche nach Informationen über Waren und Dienstleistungen (I_IUIF).

[266] Eurostat, Lektüre/das Herunterladen von Online-Zeitungen/Nachrichtenmagazinen (I_IUNW).

[267] Eurostat, Web-Radio/Web-Fernsehen (I_IUWEB).

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

[269] Eurostat, Personen, die das Internet in den letzten 3 Monaten für Aus- und Weiterbildung verwendet haben (I_IEDUT).

[270] Eurostat, Arbeitssuche oder zur Übermittlung einer Stellenbewerbung (I_IUJOB).

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

sche Themen auf Internetseiten.[272] 11% nehmen sogar an Beratungen oder Abstimmungen im Internet über Bürgerangelegenheiten oder politische Themen oder an Internet-Petitionen teil.[273] 54% beschaffen über das Internet gesundheitsrelevante Informationen.[274]

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.[275] 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.[276] 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.[277] Es beeinträchtigt die Meinungsfreiheit massiv, wenn man wegen ihres internetgestützten Gebrauchs jederzeit mit einschneidenden Ermittlungsmaßnahmen rechnen muss.

---

[272] Eurostat, Lesen oder Verfassen von Meinungsäusserungen über Bürgerangelegenheiten oder politische Themen auf Internetseiten (I_IUPOL).

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

[274] Eurostat, Beschaffung von gesundheitsrelevanten Informationen (I_IHIF).

[275] Vgl. BGH, NJW 2009, 2888.

[276] Vgl. BGH, NJW 2009, 2888.

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

§ 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.[278] 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 Tatverdächtigte, 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.“*[279]

Die abschreckende Wirkung einer Erfassung des Informations- und Kommunikationsverhaltens schadet der Meinungsfreiheit und unserem Gemeinwesen insgesamt. Denn nur umfassende Informationen, die man ungehindert und unbefangen zur Kenntnis nehmen kann, ermöglichen eine freie Meinungsbildung und -äußerung für den Einzelnen wie für die Gemeinschaft.[280] Nur auf der Grundlage eines freien und unbefangenen In-

---

[278] BT-Prot. 16/117, 22; BT-Drs. 16/6938.

[279] Tagesspiegel vom 30.09.2007, http://www.tagesspiegel.de/politik/deutschland/BKA-Datenschutz;art122,2390884.

[280] Vgl. BVerfGE 27, 71 (81).

formationszugangs 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. 8 EMRK 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. 8 EMRK angestellte Abwägung[281] Bezug genommen, die für Art. 10 EMRK entsprechend gilt.

[281] Seite 75 ff.

C. Antrag

Wir beantragen, festzustellen, dass § 111 des Telekommunikationsgesetzes vom 22.06.2004 (BGBl. I S. 1190), zuletzt geändert durch Gesetz vom 21.12.2007 (BGBl. I S. 3198), unsere Rechte aus den Artikeln 8 und 10 EMRK verletzt.

D. Angaben zu Art. 35 Abs. 1 der Konvention

Die letzte innerstaatliche Entscheidung über unsere Beschwerde ist der Beschluss des Bundesverfassungsgerichts vom 24. Januar 2012. Weitere innerstaatliche Entscheidungen sind nicht ergangen.

Gegen Grundrechtsverletzungen unmittelbar durch ein Gesetz gibt es in Deutschland lediglich den Rechtsbehelf der Verfassungsbeschwerde. Gegen den Beschluss des Bundesverfassungsgerichts vom 24. Januar 2012, durch den unsere Beschwerde gegen § 111 TKG zurückgewiesen worden ist, ist kein Rechtsmittel gegeben.

Der Beschluss des Bundesverfassungsgerichts vom 24. Januar 2012 ist unserem damaligen Verfahrensbevollmächtigten am 28. Februar 2012 zugestellt worden. Eine frühere Zustellung ist nicht erfolgt.

Die vorstehenden Beschwerdepunkte sind keinem anderen internationalen Untersuchungs- oder Schlichtungsorgan vorgelegt worden.

Sollte der Gerichtshof wegen fehlender Ausführungen oder wegen mangelnder Substantiierung unseres 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.

Wir erklären nach bestem Wissen und Gewissen, dass die von uns in der vorliegenden Beschwerdeschrift gemachten Angaben richtig sind.

Ort, Datum *Unterschrift des Beschwerdeführers zu 1*

Ort, Datum *Unterschrift des Beschwerdeführers zu 2*