

Meinhard Starostik

Rechtsanwalt/vereidigter Buchprüfer

RA Starostik, Schillstraße 9, 10785 Berlin
An das
Bundesverfassungsgericht
Schloßbezirk 3
76131 Karlsruhe

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

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

Berlin, den 23. Februar 2009

AZ: 82/06 (bitte stets angeben)

In den Verfahren

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

ergänze ich die bisherigen Ausführungen wie folgt:

1 Antrag auf Vorlage an den Europäischen Gerichtshof

Mit Urteil vom 10. Februar 2008 hat der Europäische Gerichtshof die Nichtigkeitsklage Irlands, mit der die formelle Nichtigkeit der Richtlinie 2006/24/EG geltend gemacht worden war, abgewiesen und die Vereinbarkeit der Richtlinie mit den Grundrechten offen gelassen.

Vor diesem Hintergrund wiederhole ich den Antrag,

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

Dass aus dem Grundgesetz (Art. 19 Abs. 4, 103 GG), dem Europarecht (Art. 234 EG) und der Europäischen Menschenrechtskonvention (Art. 13 EMRK) ein Recht auf und eine **Pflicht zur Vorlage** dieser Frage an den Europäischen Gerichtshof folgt, ist bereits mit Schriftsatz vom 13.08.2008 umfassend ausgeführt worden.¹ Soweit der Bevollmächtigte der Bundesregierung auf Rechtsprechung verweist, wonach zwingende Vorgaben des Gemeinschaftsrechts nicht der Überprüfung deutscher Gerichte unterlägen, hat das Bundesverfassungsgericht stets nur eine Überprüfung „am Maßstab der Grundrechte des Grundgesetzes“ ausgeschlossen.² Eine Überprüfung am Maßstab höherrangigen Europarechts und insbesondere der Gemeinschaftsgrundrechte ist von Art. 234 EG demgegenüber ausdrücklich gefordert. Denn nur, wenn das nationale Gericht die Gültigkeit entscheidungserheblichen Sekundärrechts prüft, kann es die eventuelle Ungültigkeit des Europarechtsaktes feststellen und seine Vorlagepflicht erfüllen.

Der Bevollmächtigte der Bundesregierung meint, Rechtsschutz gegen die Vorratsdatenspeicherung stehe bereits dadurch offen, dass die Betroffenen im Fall einer Abfrage von Vorratsdaten **ordentlichen oder verwaltungsrechtlichen Rechtsschutz** in Anspruch nehmen könnten und das Gericht dann inzident auch die Vereinbarkeit der Richtlinie zur Vorratsdatenspeicherung mit den Gemeinschaftsgrundrechten prüfen würde.³ Dies ist in mehrfacher Hinsicht unzutreffend: Erstens gewährleistet es keinen effektiven Rechtsschutz der von § 113a TKG Betroffenen, wenn sie nur im Fall einer Abfrage ihrer Daten gegen die Vorratsdatenspeicherung vorgehen können, sonst aber nicht. Zweitens ist aus mehreren Untersuchungen bekannt, dass ein staatlich veranlasster Zugriff auf Verkehrsdaten in den meisten Fällen nicht zur Kenntnis der Betroffenen gelangt und Rechtsschutz dadurch auch in diesem Stadium meist vereitelt wird. Drittens muss im Prozess über die Zulässigkeit einer Nutzung von Vorratsdaten regelmäßig nicht überprüft werden, ob § 113a TKG wirksam ist oder nicht. Denn die Rechtsprechung nimmt ein Verwertungsverbot für – zumal von Privaten – rechtswidrig erhobene Daten nur ausnahmsweise an. Mangels Entscheidungserheblichkeit kann ein Prozess um die Nutzung von Vorratsdaten also keinen wirksamen Rechtsschutz gegen die grundrechtswidrige Sammlung der Daten bieten.

Vertieft werden soll im Folgenden, warum die Richtlinie zur Vorratsdatenspeicherung auch nach europäischem Rechtsverständnis mit den Grundrechten unvereinbar und daher nichtig ist. Voraussetzung für eine Vorlage an den Europäischen Gerichtshof sind nämlich Zweifel des

¹ Seiten 21-23.

² BVerfGE 102, 147 (174 f.); BVerfGE 118, 79 (95).

³ Schriftsatz vom 28.11.2008, 21.

erkennenden Gerichts an der Vereinbarkeit der Richtlinie mit höherrangigem Europarecht.⁴ Dass zumindest **Zweifel an der Vereinbarkeit** der Richtlinie 2006/24/EG mit den Grundrechten bestehen, hat der Europäische Gerichtshof in seiner neuerlichen Entscheidung zu der Richtlinie selbst ausgesprochen. Er spricht nämlich ausdrücklich von einer „eventuelle[n] Verletzung der Grundrechte“ durch die Richtlinie.⁵

Dass der Europäische Gerichtshof das Grundrecht auf Schutz der Privatsphäre und auch das Verhältnismäßigkeitsgebot anerkennt, ist bereits ausgeführt worden.⁶ In der Beschwerdeschrift ist ebenfalls ausgeführt, dass der Europäische Gerichtshof in der Regel die **Europäische Menschenrechtskonvention** in ihrer Auslegung durch den Europäischen Gerichtshof für Menschenrechte anwendet und dass die Richtlinie zur Vorratsdatenspeicherung danach gegen die Art. 8 und 10 EMRK und 1 ZEMRK verstößt.⁷

Zur Stützung der Auffassung, dass die Vorratsdatenspeicherung das Grundrecht auf Achtung der Privatsphäre (Art. 8 EMRK) verletzt, ist nun auch das **Urteil der Großen Kammer des Europäischen Gerichtshofs für Menschenrechte vom 04.12.2008** anzuführen.⁸ Darin hat der Gerichtshof erstens bestätigt, dass bereits die Speicherung von Daten über das Privatleben einer Person einen Eingriff in Art. 8 EMRK darstellt.⁹ Zweitens hat der Gerichtshof ausgeführt:¹⁰

*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.*

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

Im **Vergleich zu der vom Gerichtshof verworfenen Vorratsspeicherung von Fingerabdrücken** greift die Richtlinie zur Vorratsspeicherung von Telekommunikationsdaten noch weit tiefer in unser Recht auf Achtung der Privatleben ein.

Erstens ist die Vorratsdatenspeicherung **quantitativ** weit eingriffsintensiver:

- a) Während die englische Befugnis nur Personen betraf, die einer Straftat **verdächtig** waren, betrifft die Vorratsdatenspeicherung quasi jeden Menschen. In Großbritannien waren einige Million Personen von einer Speicherung biometrischer Daten nach der

⁴ EuGH, Hinweise zur Vorlage von Vorabentscheidungsersuchen durch die nationalen Gerichte vom 11.06.2006, 2005/C 143/01, <http://curia.europa.eu/de/instit/txtdocfr/autrestxts/txt8.pdf>.

⁵ EuGH, C-301/06 vom 10.02.2009, Abs. 57.

⁶ Beschwerdeschrift vom 31.12.2007, 23.

⁷ Beschwerdeschrift vom 31.12.2007, 23 ff.

⁸ Az. 30562/04 und 30566/04.

⁹ EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 67.

¹⁰ EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 125.

verworfenen Befugnis betroffen. Von der Richtlinie zur Vorratsdatenspeicherung sind demgegenüber praktisch alle 365 Mio. Europäer betroffen.

- b) In der englischen Datensammlung waren von jedem Verdächtigen bis zu **drei Angaben** gespeichert: Fingerabdruck, Gewebeprobe und DNA-Profil. Unter der Vorratsdatenspeicherung wird demgegenüber unser gesamtes tägliches Telekommunikations-, Informations- und Bewegungsverhalten erfasst. Es handelt sich um eine weit größere Menge an Informationen.

Daneben ist die Vorratsdatenspeicherung 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 der Vorratsdatenspeicherung gesammelten Informationen betreffen zwar auch unsere Identität und erlauben die Identifizierung von Gesprächsteilnehmern (Bestandsdaten, §§ 111, 112 TKG). Sie betreffen vor allem aber unser tägliches Kommunikations-, Informations- und Bewegungsverhalten (Verbindungs-, Internetzugangs- und Standortdaten, § 113a TKG). Diese Informationen lassen Rückschlüsse auf unsere sozialen Kontakte, auf unseren Tagesablauf, auf unsere Interessen und – im Fall der Kommunikationspartner – teilweise auch auf sensible Informationen wie unsere Krankheiten (Anruf bei AIDS-Hotline), unsere Herkunft oder unser Sexualleben zu. Die über Monate aufbewahrten Verkehrsdaten legen einen großen Teil unserer Persönlichkeit und unseres privaten und beruflichen Lebens offen. Sie weisen damit einen unvergleichlich höheren Aussagegehalt auf als biometrische Merkmale zur Identifizierung von Personen, wie sie in England erfasst worden waren.
- b) Während in England nur Personen, die einer Straftat **verdächtig** waren, biometrische Merkmale abgenommen wurden, trifft die Vorratsdatenspeicherung sogar Menschen, die nie auch nur im Verdacht einer Straftat gestanden haben. Selbst der rechtstreueste Bürger kann die Erfassung seines Kommunikations- und Bewegungsverhaltens infolge der Vorratsdatenspeicherung nicht vermeiden.

Verletzt nach der Entscheidung des Europäischen Gerichtshofs für Menschenrechte die Sammlung biometrischer Daten aller Verdächtiger das **Verhältnismäßigkeitsgebot**, so tut es die weitgehende Sammlung des Kommunikations-, Informations- und Bewegungsverhaltens der gesamten Bevölkerung erst Recht. Von diesem Vergleich wird sich auch der Gerichtshof der Europäischen Gemeinschaften leiten lassen und die Richtlinie zur Vorratsspeicherung als unverhältnismäßigen Grundrechtseingriff verwerfen.

Der EGMR ist zutreffend der Behauptung der britischen Regierung entgegen getreten, die angefochtene Vorratsspeicherung sei „**unabdingbar**“ zur Verfolgung von Straftaten.¹¹ Dieser Behauptung hat der Gerichtshof erstens entgegen gehalten, dass England die Maßnahme selbst erst 2001 eingeführt habe.¹² Zweitens hat er darauf hingewiesen, dass die Strafverfolgungsbehörden anderer Staaten auch ohne eine solche Maßnahme auskommen.¹³ Nichts anderes gilt auch für die Vorratsspeicherung von Telekommunikationsdaten.

¹¹ EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 115.

¹² EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 115.

¹³ EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 112.

Zutreffend hat der Gerichtshof auch die von der britischen Regierung vorgelegten **Statistiken** über die Zahl der erfolgreichen Abrufe aus der Datenbank hinterfragt. Er hat kritisiert, dass die Zahl der erfolgreichen Abrufe keinen Aufschluss darüber gebe, in wie vielen Fällen ein erfolgreicher Abruf auch tatsächlich zur Verurteilung eines Straftäters geführt habe.¹⁴ Auch sei nicht dargelegt, in wie vielen Fällen hierfür gerade die Vorratsspeicherung der Daten Nichtverurteilter erforderlich gewesen sei.¹⁵ Die meisten der von der Regierung genannten erfolgreichen Abrufe wären auch ohne die beanstandete Vorratsspeicherung möglich gewesen.¹⁶ Wenngleich der Gerichtshof im Ergebnis davon ausging, dass die Vorratsspeicherung biometrischer Daten einen gewissen Beitrag zur Strafverfolgung leistete,¹⁷ verwarf er sie gleichwohl als unverhältnismäßig weitgehend. Nichts anderes gilt auch für die Vorratsspeicherung von Telekommunikationsdaten.

Der Gerichtshof verwarf ferner die Argumentation der britischen Regierung, die **bloße Aufbewahrung der Daten** ohne ihre Nutzung könne sich auf die Betroffenen nicht nachteilig auswirken.¹⁸ 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.¹⁹ Der Gerichtshof leitete 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 Ungleichen liege eine Stigmatisierung der Betroffenen.²⁰ – All dies gilt entsprechend auch für die Vorratsspeicherung von Telekommunikationsdaten. Nach § 113a TKG wird nicht nur das Kommunikationsverhalten Verdächtiger aufgezeichnet (§ 100g StPO), sondern sogar das Kommunikationsverhalten gänzlich Unverdächtiger und Unbeteiligter. Rechtschaffene Bürger haben aber einen Anspruch darauf, nicht allesamt wie Verdächtige einer Straftat behandelt zu werden.

Der Gerichtshof hat schließlich angeführt, dass die Vorratsspeicherung biometrischer Daten im Fall **besonderer Personengruppen** besonders schädlich sei, nämlich im Fall von Minderjährigen.²¹ Gleiches gilt im Fall der Vorratsdatenspeicherung insbesondere im Hinblick auf besondere Vertrauensverhältnisse.

Soweit der Europäische Gerichtshof für Menschenrechte in einer **Kammerentscheidung** Finnland verurteilt hat, weil dessen Gesetze im Jahr 1999 die Aufklärung einer im Internet begangenen Straftat nicht zuließen,²² steht dies der Unverhältnismäßigkeit der Vorratsdatenspeicherung nicht entgegen, weil diese Entscheidung eine andere Fallgestaltung betraf: In jenem Fall verfügte der finnische Internetanbieter über Daten, die eine Identifizierung des mutmaßlichen Täters ermöglicht hätten;²³ das finnische Recht erlaubte die Herausgabe dieser Daten aber nicht.²⁴ 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

¹⁴ EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 116.

¹⁵ EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 116.

¹⁶ EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 116.

¹⁷ EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 117.

¹⁸ EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 121.

¹⁹ EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 121.

²⁰ EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 122.

²¹ EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 124.

²² EGMR, K.U.-FI vom 02.12.2008, 2872/02.

²³ EGMR, K.U.-FI vom 02.12.2008, 2872/02, Abs. 9.

²⁴ EGMR, K.U.-FI vom 02.12.2008, 2872/02, Abs. 40.

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, stellt die vorliegende Beschwerde nicht in Frage. Der Gerichtshof hat in der genannten Entscheidung demgegenüber nicht gefordert oder zugelassen, zur Aufklärung möglicher zukünftiger Straftaten rein vorsorglich das Kommunikations- und Bewegungsverhalten der gesamten Bevölkerung 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.²⁵ Dieses Gesetz sah eine Befugnis zur Identifizierung von Kommunikationsteilnehmern auf richterliche Anordnung vor,²⁶ nicht jedoch eine anlasslose und flächendeckende Vorratsdatenspeicherung.

Auch jenseits der Europäischen Union finden sich Argumente gegen die Vereinbarkeit der Vorratsdatenspeicherung mit den Grundrechten. In den **Vereinigten Staaten** wird hauptsächlich die Meinungsfreiheit für einschlägig erachtet, die beeinträchtigt wird, wenn jede Kundgabe einer Meinung über Telekommunikationsnetze anhand von Vorratsdaten rückverfolgbar wird.

Der US-amerikanische Oberste Gerichtshof (**Supreme Court**) hat bereits in der frühen Entscheidung *Talley v. California*²⁷ ausgesprochen, dass die „anonyme Meinungsäußerung“ eine wertvolle Rolle für den „Fortschritt der Menschheit“ gespielt habe. Anonymität sei mitunter für überaus wertvolle Zwecke genutzt worden. 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“, weshalb der Oberste Gerichtshof die Wahrung der Anonymität als notwendig zum Schutz der Meinungsfreiheit erachtet hat. Eine Pflicht zur Nennung der Verantwortlichen auf Flugzetteln hat er daher als Verstoß gegen die Meinungsfreiheit verworfen.

In einer späteren Entscheidung²⁸ 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 allein wegen der Person des Äußernden 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.²⁹ Es müsse möglich bleiben, anonym Mitglied eines unbeliebten Vereins zu sein, um die Freiheit auch unpopulärer Meinungen zu gewährleisten.

In einer ausführlichen Untersuchung gelangt Catherine Crump ausgehend von dieser Rechtsprechung des Obersten Gerichtshofs zu dem Ergebnis, dass eine **Vorratsdatenspeicherung** das Recht auf freie Meinungsäußerung verletzt.³⁰ Eine Vorratsdatenspeicherung eliminiere die anonyme Äußerung von Meinungen im Internet, weil durch sie jede Meinungsäußerung über Telekommunikationsnetze rückverfolgbar werde.

²⁵ EGMR, K.U.-FI vom 02.12.2008, 2872/02, Abs. 49.

²⁶ EGMR, K.U.-FI vom 02.12.2008, 2872/02, Abs. 21.

²⁷ 362 U.S. 60 (1960).

²⁸ *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995).

²⁹ *NAACP v. Alabama ex. rel. Patterson*, 357 U.S. 449 (1958).

³⁰ Crump: *Data Retention*, *Stanford Law Review*, Vol. 56:191.

Außerdem werde die anonyme Bildung von Vereinigungen über Telekommunikationsnetze unmöglich, weil sich Mitgliedschaften in einer Internet-Vereinigung – etwa derjenigen des Beschwerdeführers zu 3 bzw. 8³¹ – mithilfe von Telekommunikationsdaten aufdecken ließen.

Dass der Oberste Gerichtshof die **Aufklärung von Straftaten** zur Rechtfertigung einer flächendeckenden Vorratsdatenspeicherung nicht würde genügen lassen, begründet die Autorin mit den folgenden Ausführungen des Gerichtshofs in einem Urteil aus dem Jahr 2002: „Das Argument geht im Kern dahin, dass geschützte Meinungsäußerungen verboten werden dürften, um ungeschützte Meinungsäußerungen verhindern zu können. Diese Analyse stellt die Meinungsfreiheit auf den Kopf. Der Staat darf rechtmäßige Meinungsäußerungen nicht unterdrücken, um unrechtmäßige Meinungsäußerungen zu verhindern. [...] Die Verfassung gebietet das Gegenteil.“³² Schon in einer früheren Entscheidung hatte der Gerichtshof ausgeführt, „in unserer Gesellschaft hat der Wert freier Meinungsäußerung ein höheres Gewicht als die Gefahren ihres Missbrauchs“.³³ Die Autorin sieht in einer Vorratsdatenspeicherung eine Verletzung dieser Grundsätze, weil eine Vorratsdatenspeicherung zur Aufklärung unrechtmäßiger Handlungen unterschiedslos auch rechtmäßige Meinungsäußerungen erfasst und rückverfolgbar macht.

Die Autorin gelangt zu dem folgenden Ergebnis: „Untersucht man eine Vorratsspeicherungspflicht im Lichte der vom Gerichtshof anerkannten Bedeutung anonymer Meinungsäußerung, so gibt es überzeugende Gründe dafür, sie wegen ihrer **Auswirkungen auf anonyme Meinungsäußerungen** als verfassungswidrig anzusehen.“³⁴

Dass in den **USA** auch tatsächlich keine Pflicht zur Vorratsdatenspeicherung besteht und anonyme Dienste uneingeschränkt angeboten werden können, ist bereits aufgeführt worden.

Im Ergebnis ist festzuhalten, dass die anlasslose Protokollierung des Kommunikations-, Informations- und Bewegungsverhaltens der gesamten Bevölkerung nicht nur aus Sicht des deutschen Verfassungsrechts unsere Grundrechte verletzt, sondern auch aus **europäischer und internationaler Sicht**. Die Vorlage der Frage an den EuGH, ob die Richtlinie zur Vorratsdatenspeicherung wegen Verletzung der Grundrechte nichtig ist, wird daher zur Nichtigerklärung der Richtlinie führen und dem Bundesverfassungsgericht ermöglichen, Rechtsschutz auch gegen § 113a TKG zu gewähren.

Es wird angeregt, dass das Hohe Gericht in seinem **Vorlageschluss** an den EuGH nicht nur Zweifel an der Vereinbarkeit der Vorratsdatenspeicherung mit den Grundrechten anmelden möge, sondern deutlich machen möge, dass es von der Unvereinbarkeit der Richtlinie zur Vorratsdatenspeicherung mit den Grundrechten überzeugt ist. Eine solche Beurteilung durch das international hoch angesehene Bundesverfassungsgericht wird den Europäischen Gerichtshof bei seiner Entscheidung maßgeblich leiten können. Auf diese Weise kann das bisher weitgehend nur erhoffte Kooperationsverhältnis zwischen beiden Gerichten tatsächlich einmal zur Geltung kommen und Nutzen zum Schutz der Grundrechte und -freiheiten sämtlicher EU-Bürgerinnen und -Bürger entfalten.

³¹ Beschwerdeschrift vom 31.12.2007, 8.

³² Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002).

³³ McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995).

³⁴ Crump, Stanford Law Review, Vol. 56, 191 (223 f.).

2 Hauptsacheantrag

2.1 Empirische Erkenntnisse und aktuelle Entwicklungen

Zu dem **Missbrauch von Verbindungsdaten** bei der Deutschen Telekom AG gibt es neue Erkenntnisse: Die Darstellung, Ziel des Missbrauchs von Verbindungsdaten sei nur die Aufdeckung der Weitergabe von Interna an die Presse gewesen, lässt sich kaum noch halten. Die etwa 60 Zielpersonen der Verbindungsdatenmissbräuche waren nicht nur Aufsichtsräte der Deutschen Telekom AG und deren Tochterfirma T-Mobile, ein Vorstandsmitglied der Telekom und Journalisten, sondern auch Angehörige und Mitarbeiter von Betriebsräten und „dem Konzernbereich nicht zuzuordnende Dritte“ wie Ver.di-Funktionäre. Laut Spiegel³⁵ zählten zu den Zielpersonen des Missbrauchs von Verbindungsdaten:

- a) Angehörige der Dienstleistungsgewerkschaft Ver.di, die bei der Telekom eine Funktion wie etwa ein Aufsichtsratsmandat hatten. Dazu zählen unter anderem Ver.di-Bundesvorstand und Telekom-Aufsichtsrat Lothar Schröder, DGB-Chef Michael Sommer oder Telekom-Aufsichtsrat Josef Falbisoner.
- b) Ver.di-Mitglieder, die keinen oder kaum Zugang zu Telekom-Interna hatten, wie etwa Betriebsräte des Unternehmens oder Ver.di-Chef Frank Bsirske, der nicht einmal eine Funktion bei der Telekom hatte, als Chef der Dienstleistungsgewerkschaft aber offenbar interessant für die Späher war.
- c) Telekom-Mitarbeiter, die im Verdacht standen, im Jahr 2006 am Diebstahl von 17 Millionen Mobilfunkdatensätzen beteiligt gewesen zu sein. Ihre Telefonverbindungsdaten wurden widerrechtlich erhoben, um möglichen Tätern auf die Spur zu kommen.
- d) Angestellte oder Manager der Deutschen Telekom, die keiner dieser Gruppen zuzuordnen sind, wie etwa die damalige Chefsekretärin von Telekom-Chef Kai-Uwe Ricke oder Ex-Personalvorstand Heinz Klinkhammer.
- e) Fachjournalisten wie etwa Anne Preissner und Eva Müller vom „manager magazin“, Jürgen Berke und Thomas Kuhn von der „Wirtschaftswoche“, Reinhard Kowalewsky von „Capital“ oder Heinz W. Dieckmann vom „Handelsblatt“.

Die Ermittlung „undichter Stellen“ im Aufsichtsrat kann nicht **Ziel sämtlicher Aktionen** gewesen sein, weil viele der Zielpersonen keinen Zugang zu Informationen des Aufsichtsrats hatten. Es ist auch auffällig, dass die Verbindungsdaten der Gewerkschaftsvertreter immer während Tarifauseinandersetzungen überprüft wurden, was ein entsprechendes Ziel der Maßnahmen nahe legt.³⁶

Auch hat sich heraus gestellt, dass die Auswertungen Verbindungen eingeschlossen haben, die Kunden von **Wettbewerbern** wie O2 und E-Plus hergestellt haben.³⁷ Missbraucht worden sind also auch Verbindungs- und Bewegungsdaten von Personen, die nicht einmal Kunden der Deutschen Telekom oder ihrer Tochterfirma T-Online waren.

Bei den missbräuchlichen Auswertungen von Verkehrsdaten durch die Deutsche Telekom AG in den Jahren 2005 und 2006 handelte es sich um **keine Einzelfälle**, sondern um einen systematischen Missbrauch von Verbindungsdaten. Es kam auch nicht nur bei der Deutschen

³⁵ Spiegel Online vom 19.11.2008, <http://www.spiegel.de/wirtschaft/0,1518,591374,00.html>.

³⁶ Report Mainz vom 22.12.2008, <http://www.swr.de/report/-/id=233454/nid=233454/did=4196196/drio2h/index.html>.

³⁷ Handelsblatt vom 20.11.2008, <http://www.handelsblatt.com/unternehmen/it-medien/telekom-spitzelte-auch-im-festnetz;2093529:0>.

Telekom AG zum Missbrauch von Verbindungsdaten. Ein Wettbewerber der Deutschen Telekom stellte dieser ebenfalls illegal Verbindungsdaten zur Verfügung.³⁸ Europaweit erfolgten in den letzten Jahren wiederholt versehentliche und absichtliche Weitergaben und Missbräuche von Informationen über unsere Telekommunikation, so in Italien,³⁹ Griechenland,⁴⁰ Lettland,⁴¹ Bulgarien,⁴² der Slowakei⁴³ und in Ungarn.⁴⁴

Nach dem Ende der Amtszeit des US-Präsidenten George Bush hat der ehemalige Mitarbeiter der Nationalen Sicherheitsbehörde **NSA** Russell Tice enthüllt, dass die NSA illegal sämtliche in den USA anfallende Verkehrsdaten auf Vorrat speichert und auswertet und es insbesondere auf die Kommunikation und Bewegungen von Journalisten abgesehen hat.⁴⁵ Die Vorratsdatenspeicherung ermöglicht ähnlichen Missbrauch auch in Deutschland.

Pannen gab es auch bei **Bestandsdaten**. Im Jahr 2006 verkaufte ein Mitarbeiter von T-Mobile die Daten der 17 Mio. Anschlussinhaber des Mobilfunkunternehmens. Die Daten umfassen den Namen, die Mobilfunknummer, die Anschrift, teils das Geburtsdatum und in einigen Fällen auch die E-Mail-Adresse der Handy-Nutzer. Die Daten werden inzwischen in kriminellen Kreisen angeboten. Unter den Daten finden sich 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 Bedrohung ihrer Sicherheit darstellt (etwa Charlotte Knobloch, Präsidentin des Zentralrats der Juden). Das Bundeskriminalamt musste eine Gefährdungsanalyse erstellen, um Betroffene schützen zu können.⁴⁶ Zur Aufklärung des Datenlecks verletzte T-Mobile erneut das Fernmeldegeheimnis und überprüfte illegal Verbindungsdaten.⁴⁷

In den vergangenen Schriftsätzen ist ausgeführt worden, dass auch die durch § 113a TKG bewirkte Verfügbarkeit weiterer Verkehrsdaten wegen verschiedener **Umgehungsmöglichkeiten** oftmals nicht geeignet ist, Ermittlungsverfahren zum Erfolg zu führen. Nun gesteht auch der Bevollmächtigte der Bundesregierung ein, dass die Verschleierung der Telekommunikationsnutzung „milieutypisch“ ist⁴⁸ und Straftäter „so gut wie immer“ Anschlüsse anderer Personen einsetzen⁴⁹. Diese Erfahrungen bestätigen nicht nur den marginalen Zusatznutzen des § 113a TKG. Sie bestätigen auch die Richtigkeit der Warnung, dass die Vorratsdatenspeicherung Straftäter zur Nutzung von Umgehungstechniken veranlasst, durch welche Überwachungsmaßnahmen selbst im Verdachtsfall vereitelt werden und insgesamt betrachtet eine kontraproduktive Wirkung auf die Strafverfolgung eintritt.⁵⁰

In vergangenen Schriftsätzen ist gewarnt worden, dass eine auch nur teilweise Aufrechterhaltung des § 113a TKG zu einem **Dambruch** auf breiter Front führen würde, weil die

³⁸ Handelsblatt vom 13.11.2008, <http://www.handelsblatt.com/unternehmen/it-medien/detektivische-suche-nach-den-schnuefflern;2087697:0>.

³⁹ http://en.wikipedia.org/wiki/SISMI-Telecom_scandal.

⁴⁰ http://en.wikipedia.org/wiki/Greek_telephone_tapping_case_2004-2005.

⁴¹ <http://www.baltictimes.com/news/articles/18576/>.

⁴² http://www.novinite.com/view_news.php?id=17103.

⁴³ http://www.freemedia.at/cms/ipi/freedom_detail.html?country=/KW0001/KW0003/KW0080/&year=2003.

⁴⁴ <http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559531>.

⁴⁵ Russell Tice, former NSA analyst, 23.01.2009, http://www.mediabistro.com/fishbowIDC/television/nsa_spied_on_journalists_106514.asp.

⁴⁶ Spiegel Online vom 04.10.2008, <http://www.spiegel.de/wirtschaft/0,1518,581938,00.html>.

⁴⁷ Heise Online vom 29.10.2008, <http://www.heise.de/newsticker/meldung/118106>.

⁴⁸ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 63.

⁴⁹ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 49.

⁵⁰ Näher Beschwerdeschrift vom 31.12.2007, 69 und 100 f.; Schriftsatz vom 28.02.2008, 4 f.

Zulassung einer globalen und pauschalen Informationssammlung allein für eine mögliche künftige staatliche Verwendung der Daten schrittweise alle Lebensbereiche erfassen würde.⁵¹ Die Bundesjustizministerin hat zwischenzeitlich angekündigt, EU-Pläne zur jahrelangen Vorratsspeicherung des Flugreiseverkehrs nur vorübergehend bis zur Entscheidung des Hohen Gerichts im vorliegenden Verfahren zurückzustellen.⁵² An diesem neuerlichen Vorhaben wird sehr deutlich, dass eine flächendeckende und anlasslose Erfassung unseres Telekommunikations- und Bewegungsverhaltens sehr schnell auf andere Bereiche ausgeweitet werden würde, wenn sie nicht von Anfang an verfassungsrechtlich konsequent unterbunden wird.

2.2 Erwiderung auf den Schriftsatz des Bevollmächtigten der Bundesregierung vom 09.09.2008

Soweit die Ausführungen des Bevollmächtigten der Bundesregierung mit Schriftsatz vom 09.09.2008 für die Hauptsache von Bedeutung sind, wird auf sie wie folgt erwidert:

Der Bevollmächtigte der Bundesregierung behauptet, das Hohe Gericht sei in seinem Beschluss vom 11.03.2008 davon ausgegangen, dass die von § 113a TKG ausgehende **Einschüchterungswirkung** für das vorliegende Verfahren nicht von Bedeutung sei.⁵³ Richtig ist demgegenüber, dass das Hohe Gericht lediglich entschieden hat, dass die einschüchternde Wirkung des § 113a TKG nicht die Aussetzung eines durch zwingendes Europarecht vorgegebenen Parlamentsgesetzes im Wege der einstweiligen Anordnung gebiete.⁵⁴ Das Bundesverfassungsgericht hat jedoch bestätigt, dass „die in § 113a TKG angeordnete umfassende und anlasslose Bevorratung sensibler Daten über praktisch jedermann für staatliche Zwecke [...] einen erheblichen Einschüchterungseffekt bewirken“ kann.⁵⁵ Auch hat das Gericht „die durch §§ 113a und 113b TKG begründete Beeinträchtigung der allgemeinen Unbefangtheit des elektronischen Informations- und Gedankenaustauschs“ anerkannt.⁵⁶

Die Behauptung des Bevollmächtigten der Bundesregierung, in den Ergebnissen der repräsentativen **Forsa-Umfrage** spiegele sich eine „fehlerhafte Darstellung des Regelungsgehalts der angegriffenen Normen“⁵⁷ und ein „falsche[s] Verständnis der Regelungen“⁵⁸ wider, ist falsch. Bereits durch die erste Frage der Umfrage ist den Teilnehmer/innen deutlich gemacht worden, was § 113a TKG zum Gegenstand hat. Insbesondere ist entgegen den Unterstellungen des Bevollmächtigten der Bundesregierung deutlich gemacht worden, dass „Verbindungsdaten“ und nicht Inhalte betroffen sind. Auch ist in der ersten Frage deutlich gemacht worden, dass die Speicherung – und nicht automatisch auch die staatliche Nutzung – dieser Verkehrsdaten in Rede steht. Die erste Frage lautete wörtlich:

An Verbindungsdaten lässt sich ablesen, wer wann, wo und mit wem per Telefon, Handy oder E-Mail in Verbindung gestanden hat. Seit Beginn des Jahres 2008 müssen alle Verbindungsdaten jedes Bürgers in Deutschland sechs Monate lang gespeichert werden. Ist Ihnen das bekannt?

⁵¹ Schriftsatz vom 13.08.2008, 36.

⁵² Spiegel Online vom 28.11.2008, <http://www.spiegel.de/reise/aktuell/0,1518,593378,00.html>.

⁵³ Bevollmächtigter der Bundesregierung, Schriftsatz vom 09.09.2008, 2.

⁵⁴ Beschluss vom 11.03.2008, Abs. 150.

⁵⁵ Beschluss vom 11.03.2008, Abs. 148.

⁵⁶ Beschluss vom 28.10.2008, Abs. 92.

⁵⁷ Bevollmächtigter der Bundesregierung, Schriftsatz vom 09.09.2008, 2.

⁵⁸ Bevollmächtigter der Bundesregierung, Schriftsatz vom 09.09.2008, 3.

Die Behauptung des Bevollmächtigten der Bundesregierung, in der „unermüdlichen **Öffentlichkeitsarbeit** der Antragsteller“ (in welcher?) werde „pauschal die Speicherung als solche bereits als ‚Überwachung‘ bezeichnet“,⁵⁹ ist falsch und mangels Beleg auch nicht näher einlassungsfähig.

Entgegen der Behauptung des Bevollmächtigten der Bundesregierung⁶⁰ sind die vom Hohen Gericht angeforderten **Statistiken** nicht allgemein als irrelevant bezeichnet worden. Es ist vielmehr mit Schriftsatz vom 13.08.2008 ausgeführt worden, dass und weshalb die Abrufstatistik keinen Rückschluss auf einen Bedarf nach Vorratsdaten erlaubt.⁶¹ Im Übrigen hat das Hohe Gericht die Statistik selbst nur für seine Entscheidung über den Antrag auf Erlass einer einstweiligen Anordnung angefordert und nicht für seine Hauptsacheentscheidung. Der Beschluss vom 11.03.2008 führt insoweit wörtlich aus (Abs. 178):

Die Informationen sollen dem Senat die Entscheidung ermöglichen, ob gegebenenfalls von Amts wegen eine Änderung der einstweiligen Anordnung vorzunehmen und ob sie zu verlängern ist.

Der Bevollmächtigte der Bundesregierung meint, die Zahl der Zugriffe auf Verkehrsdaten widerlege den Einwand, § 113a TKG komme nur eine **marginale Bedeutung** zu.⁶² Demgegenüber bleibt die Berechnung im Schriftsatz vom 17.03.2008 richtig, wonach § 113a TKG die Verfolgung von Straftaten bestenfalls zu 0,002% effektiver machen kann.⁶³ Die Statistik der Bundesregierung erlaubt eine diesbezügliche Aussage nicht, weil sie keinen Aufschluss darüber gibt, in wie vielen Fällen Vorratsdaten nicht nur angefordert wurden sondern auch erforderlich waren und weiter geführt haben.⁶⁴ Insbesondere beantwortet die Statistik nicht die Frage, bei wie vielen der Zugriffe auf Vorratsdaten nicht auch die Erhebung von Abrechnungsdaten ausgereicht hätte. Die Praxis verlangt nach Möglichkeit standardmäßig die Beauskunftung von Vorratsdaten mit, ohne sich zunächst auf Abrechnungsdaten zu beschränken und zu überprüfen, ob diese ausreichen. Auch gibt die Statistik keinen Aufschluss über das Ergebnis einer Abfrage von Vorratsdaten.

Der Bevollmächtigte der Bundesregierung kritisiert, die erhöhte **Menge** an verfügbaren Verkehrsdaten in den letzten Jahren besage noch nichts darüber, ob die Daten zur Strafverfolgung genutzt werden konnten oder nicht.⁶⁵ Dagegen bleibt der Bevollmächtigte einen Beleg für seine Behauptung schuldig, dass die Abfragen der Strafverfolgungsbehörden nach § 100g StPO in den letzten Jahren zunehmend erfolglos geblieben sein sollen. Dass dies tatsächlich nur in den seltensten Fällen der Fall war, ergibt sich aus der Untersuchung des Max-Planck-Instituts.

Zu dem Datenmissbrauch bei der **Deutschen Telekom AG** führt der Bevollmächtigte der Bundesregierung aus, dieser sei vor Inkrafttreten des § 113a TKG erfolgt und habe Vorratsdaten nicht zum Gegenstand gehabt.⁶⁶ Der Bevollmächtigte bleibt aber eine Erklärung dafür schuldig, weshalb von einem heute stattfindenden Datenmissbrauch ausgerechnet Daten nach § 113a TKG ausgenommen sein sollten. Einem heute stattfindenden Missbrauch von

⁵⁹ Bevollmächtigter der Bundesregierung, Schriftsatz vom 09.09.2008, 3.

⁶⁰ Bevollmächtigter der Bundesregierung, Schriftsatz vom 09.09.2008, 3.

⁶¹ Schriftsatz vom 13.08.2008, 6 f.

⁶² Bevollmächtigter der Bundesregierung, Schriftsatz vom 09.09.2008, 4.

⁶³ Bevollmächtigter der Bundesregierung, Schriftsatz vom 17.03.2008, 1 f.

⁶⁴ Näher Schriftsatz vom 13.08.2008, 6 f.

⁶⁵ Bevollmächtigter der Bundesregierung, Schriftsatz vom 17.03.2008, 4.

⁶⁶ Bevollmächtigter der Bundesregierung, Schriftsatz vom 17.03.2008, 5.

Kommunikationsdaten würden wegen § 113a TKG sehr viel größere Datenmengen sowie eine sehr viel größere Zahl von Kontakten und Personen anheim fallen. Die bisherigen Möglichkeiten zum Schutz vor einer Protokollierung des Kommunikations-, Bewegungs- und Informationsverhaltens – und damit auch vor einem Missbrauch dieser Informationen – sind mit § 113a TKG entfallen. Seit 2009 ist zusätzlich der gesamte E-Mail-Verkehr der Gefahr einer missbräuchlichen Auswertung durch die Anbieter, ihre Mitarbeiter oder Dritte ausgesetzt.

Der Bevollmächtigte der Bundesregierung merkt an, die weiteren **Datenskandale** der vergangenen Zeit seien für das vorliegende Verfahren unerheblich.⁶⁷ Dagegen ist die Vielzahl der in den letzten Monaten bekannt gewordenen Datenschutzverstöße insofern für das vorliegende Verfahren von Bedeutung, als sie belegt, dass die Gefahr von Datenpannen und Missbräuchen real ist und solche Fälle eine notwendige Begleiterscheinung von Datensammlungen wie derjenigen nach § 113a TKG darstellen. Im Übrigen ist kriminologisch gesichert, dass nur ein Bruchteil aller Gesetzesverletzungen an das Licht der Öffentlichkeit gelangt. Auch der Telekom-Skandal ist erst nach Jahren und durch zufällige Erkenntnisse eines Nachrichtenmagazins bekannt geworden. Tatsächlich ist davon auszugehen, dass bei der Deutschen Telekom AG und auch bei vielen anderen Telekommunikationsanbietern in weitaus mehr Fällen Pannen und Missbrauch aufgetreten sind als heute bekannt.

Der Bevollmächtigte der Bundesregierung will nicht anerkennen, dass § 113a TKG die **Informationsfreiheit im Internet** schwer beeinträchtigt, weil aufgerufene Webseiten und eingegebene Suchworte nach § 113a TKG nicht zu speichern sind.⁶⁸ Der Bevollmächtigte bleibt aber eine Begründung schuldig, warum § 113a Abs. 4 TKG die Protokollierung der Internet-Nutzungskennungen (IP-Adressen) sämtlicher Internetnutzer vorschreibt, wenn nicht zur Offenlegung ihrer Internetnutzung. Es ist bekannt, dass Anbieter von Telemedien vielfach unter Verstoß gegen § 15 TMG Internet-Nutzungsprotokolle mitsamt der verwendeten IP-Adresse erstellen und alle staatlichen Eingriffsbehörden über §§ 15 Abs. 5 S. 4, 14 Abs. 2 TMG darauf Zugriff haben, z.B. nach §§ 95 StPO, 20m BKA-G, 8a BVerfSchG, 101 UrhG. Die Bundesregierung will eine freiwillige Vorratsspeicherung der Internetnutzung mit dem „Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes“ jetzt sogar legalisieren.⁶⁹ Bisher hat das an deutsche Internet-Zugangsanbieter gerichtete Verbot des § 96 TKG, die zugeteilte IP-Adresse zu protokollieren, eine personenbezogene Rückverfolgung unserer elektronischen Mediennutzung weitgehend verhindert. § 113a TKG hebt diesen Schutz nun jedoch auf und ermöglicht es, jeden unserer Klicks auf Internet-Portalen wie Google, eBay oder Amazon über Monate hinweg nach zu verfolgen.

Soweit mit Schriftsatz vom 13.08.2008 ausgeführt worden ist, § 113a TKG erfasse auch nichtkommerzielle und private Anbieter,⁷⁰ bedarf dies einer Einschränkung: § 113a TKG gilt nach § 3 Nr. 24 TKG nur für Anbieter, die ihre Dienste gewöhnlich **gegen Entgelt** erbringen.⁷¹

Der Bevollmächtigte der Bundesregierung behauptet, ohne § 113a Abs. 4 TKG werde die **Verfolgung im Internet begangener Straftaten** „zum weitaus überwiegenden Teil vereitelt“.⁷² Das Gegenteil folgt bereits daraus, dass bis 2008 eine angemessene Strafverfolgung auch im Internetbereich ohne § 113a TKG möglich war und in vielen Staaten weltweit bis heute ist. Es ist

⁶⁷ Bevollmächtigter der Bundesregierung, Schriftsatz vom 17.03.2008, 5.

⁶⁸ Bevollmächtigter der Bundesregierung, Schriftsatz vom 17.03.2008, 11.

⁶⁹ BR-Drs. 62/09.

⁷⁰ Schriftsatz vom 13.08.2008, 10.

⁷¹ Siehe im Einzelnen <http://www.daten-speicherung.de/?p=605>.

⁷² Bevollmächtigter der Bundesregierung, Schriftsatz vom 17.03.2008, 15.

schon darauf hingewiesen worden, dass die durchschnittliche Aufklärungsquote von 55,4%⁷³ im Bereich des Internet seit jeher weit übertroffen wird: 2006 wurden 78,5% der registrierten Straftaten im Bereich der Verbreitung pornographischer Schriften via Internet, 86% der Fälle von Internetbetrug und 85,5% der Straftaten gegen Urheberrechtsbestimmungen im Internet aufgeklärt.⁷⁴ 2007 konnten diese Zahlen nochmals erheblich gesteigert werden, obwohl in diesem Zeitraum IP-Adressen allenfalls kurzzeitig gespeichert wurden: 2007 wurden 86,3% der registrierten Straftaten im Bereich der Verbreitung pornographischer Schriften via Internet, 84% der Fälle von Internetbetrug und 94,8% der Straftaten gegen Urheberrechtsbestimmungen im Internet aufgeklärt.⁷⁵

Eine Beleidigung im Internet ist schlichtweg ebenso häufig **ohne flächendeckende Protokollierung** aller Kontakte aufklärbar wie eine unmittelbar oder postalisch ausgesprochene Beleidigung. Ein via Internet begangener Betrug ist ohne flächendeckende Protokollierung der Nutzung von Internetzugängen ebenso häufig aufklärbar wie ein unmittelbar oder postalisch begangener Betrug. Die Verschaffung kinderpornografischer Darstellungen via Internet ist ohne flächendeckende Protokollierung aller Kontakte ebenso häufig aufklärbar wie die Verschaffung per persönlicher Übergabe oder Post. Den Strafverfolgungsbehörden stehen allgemein keine flächendeckenden Verhaltensprotokolle zur Verfügung. Es gibt keinen Grund, weshalb dies in der Informationsgesellschaft anders sein soll. Die Strafverfolgungsbehörden benötigen auch keine flächendeckenden Verhaltensprotokolle, um eine Aufklärungsquote zu erzielen, von der eine zum Rechtsgüterschutz hinreichende Abschreckungswirkung ausgeht. Denn sie können im Fall von Internetdelikten – wie sonst auch – mit einzelfallbezogenen Ermittlungen und anlassbezogener Überwachung Verdächtiger (z.B. mit V-Leuten, Hausdurchsuchungen usw.) arbeiten. Dass professionell agierende Straftäter die Entstehung identifizierbarer Verkehrsdaten ohnehin und trotz § 113a TKG zu vermeiden wissen, ist bekannt und wird nun auch vom Bevollmächtigten der Bundesregierung zugestanden.⁷⁶ Der Bevollmächtigte der Bundesregierung überschätzt die Bedeutung von Telekommunikationsprotokollen für die Strafverfolgung weit.

Im Übrigen machen sich die Beschwerdeführer die Einschätzung des **Präsidenten des Bundesgerichtshofs**, der mit der praktischen Anwendung des Strafrechts befasst ist, ausdrücklich zu Eigen:⁷⁷

Der Wertung, dass ohne die Möglichkeit der Speicherung und Erhebung der genannten Daten die Nutzung des Internets zu einem "rechtsfreien Raum" würde, könnte ich mich nicht anschließen. Einzelne Bereiche sozialen Verhaltens sind nicht deshalb rechtsfreie Räume, weil von ihrer präventiven Überwachung abgesehen wird.

Soweit der Bevollmächtigte der Bundesregierung eine „rasante Ausbreitung der **Kinderpornografie** im Internet“ behauptet,⁷⁸ wird mit Nichtwissen bestritten, dass die Nutzung des Internet zum Austausch solcher Darstellungen in größerem Maß zu nähme, als die Nutzung des Internet insgesamt, zumal die Ermittlung von Internetdelikten sehr viel häufiger gelingt als Ermittlungen in anderen Kommunikationskanälen. Im Übrigen schützt § 113a TKG kein Kind vor sexuellem Missbrauch. In Ländern mit Vorratsdatenspeicherung gibt es nicht weniger Missbrauch von Kindern als in Ländern ohne Vorratsdatenspeicherung. Die Vorratsdatenspeicherung ist kein

⁷³ Bundeskriminalamt, Polizeiliche Kriminalstatistik 2006, 65.

⁷⁴ Bundeskriminalamt, Polizeiliche Kriminalstatistik 2006, 243.

⁷⁵ Bundeskriminalamt, Polizeiliche Kriminalstatistik 2007, 243.

⁷⁶ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 49 und 63.

⁷⁷ Präsident des Bundesgerichtshofs, Stellungnahme vom 07.11.2008, 7.

⁷⁸ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 15.

taugliches Mittel zum Schutz von Kindern. Fahndungserfolge im Bereich des Austauschs kinderpornografischer Darstellungen wurden etwa in den Jahren 2006 und 2007 erzielt, ohne dass § 113a TKG für den Internetbereich in Kraft war. Dass in diesem Bereich schon vor Inkrafttreten des § 113a TKG eine überdurchschnittlich hohe Aufklärungsquote erzielt wurde, ist bereits belegt worden.

Der Bevollmächtigte der Bundesregierung behauptet, zur Identifizierung der Nutzer von **Internettelefonie** werde deren IP-Adresse benötigt.⁷⁹ Richtig ist demgegenüber, dass die Anbieter von Internettelefonie schon zu Abrechnungszwecken identifizierbare Kundendaten speichern. Die verwendete IP-Adresse können Straftäter leicht verschleiern und ist zur Identifizierung nicht erforderlich.

2.3 Erwiderung auf den Schriftsatz des Bevollmächtigten der Bundesregierung vom 28.11.2008

Auf die Ausführungen des Bevollmächtigten der Bundesregierung mit Schriftsatz vom 28.11.2008 wird wie folgt erwidert:

Der Bevollmächtigte der Bundesregierung behauptet, § 113a Abs. 6 TKG sei europarechtlich vorgegeben.⁸⁰ Das Gegenteil ist bereits vom Bundesverfassungsgericht anerkannt worden.⁸¹ **Anonymisierungsdienste** bieten weder Telefonie noch E-Mail oder Internetzugang an und sind nach der Richtlinie zur Vorratsdatenspeicherung deshalb nicht zur Speicherung verpflichtet.

Der Bevollmächtigte der Bundesregierung vertritt die Auffassung, Anonymisierungsdienste behielten ihre **Berechtigung**, weil die Kommunikation im Verhältnis zum Kommunikationspartner anonym bleibe.⁸² Indes sind Internetnutzer für ihre Kommunikationspartner auch ohne Anonymisierungsdienst nicht unmittelbar identifizierbar, weil es dazu der Mitwirkung des Internet-Zugangsanbieters bedarf. Wenn die Nutzung von Anonymisierungsdiensten also keinen Mehrwert bietet, warum sollte man einen deutschen Anonymisierungsdienst nutzen, der zur Vorratsdatenspeicherung verpflichtet ist? Schon mit Schriftsatz vom 17.03.2008 ist ausgeführt worden, dass die Vorratsdatenspeicherung die Existenz deutscher Anbieter von Anonymisierungsdiensten gefährdet.⁸³ Die Beschwerdeführerin zu 4 kann ihre Glaubwürdigkeit gegenwärtig nur dadurch einigermaßen aufrecht erhalten, dass sie mit ausländischen Anbietern zusammen arbeitet, die nicht zur Vorratsdatenspeicherung verpflichtet sind.

Der Bevollmächtigte der Bundesregierung behauptet, die Verpflichtung der Anbieter von E-Mail-Diensten zur Protokollierung der von ihren Nutzern verwendeten **IP-Adressen** sei in Art. 5 Abs. 1 Buchst. c Nr. 2 (i) vorgesehen.⁸⁴ Das ist falsch, weil diese Bestimmung eindeutig nur den „Internetzugangsdienst“ betrifft, während für den „Internet-E-Mail-Dienst oder Internet-Telefonie-Dienst“ nur Art. 5 Abs. 1 Buchst. c Nr. 2 (ii) RiL 2006/24/EG gilt. Diese Bestimmung fordert nur die Speicherung der „Benutzerkennung“, also der E-Mail-Adresse von Absender und Empfänger (Art. 5 Abs. 1 Buchst. a Nr. 2 und Buchst. b Nr. 2 RiL 2006/24/EG). Dass die Richtlinie mit „Benutzerkennung“ nicht die IP-Adresse meint, ergibt sich daraus, dass die Richtlinie den Begriff der „Internetprotokoll-Adresse“ kennt und nur in anderem Zusammenhang erwähnt (Art. 5 Abs. 1 Buchst. a Nr. 2 iii und Buchst. c Nr. 2 i RiL 2006/24/EG). Dementsprechend hatte auch der

⁷⁹ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 16.

⁸⁰ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 9 f.

⁸¹ Beschluss vom 11.03.2008, Abs. 136.

⁸² Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 10 f.

⁸³ Schriftsatz vom 17.03.2008, 11.

⁸⁴ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 11 f.

Referentenentwurf des Bundesjustizministeriums betreffend noch nicht vorgesehen, dass E-Mail-Anbieter die IP-Adressen der Teilnehmer speichern müssen (§ 110a Ref-E TKG). Durch Einbeziehung der IP-Adresse hebt § 113a Abs. 3 TKG die in § 111 Abs. 1 S. 3 TKG vorgesehene und auch in der Richtlinie vorausgesetzte Möglichkeit der anonymen Nutzung von E-Mail-Diensten wieder aus. Denn Internet-Zugangsanbieter müssen die Vergabe von IP-Adressen auf Vorrat protokollieren. Über die vorrattgespeicherte IP-Adresse kann die Person des E-Mail-Nutzers letztlich doch festgestellt werden. Dies gilt selbst dann, wenn Deutsche E-Mails über anonyme Dienste versenden, die von Drittstaaten aus angeboten werden. Denn die deutsche IP-Adresse ist auch in über Drittstaaten versandten E-Mails enthalten und kann über den Zugangsprovider zugeordnet werden. Insofern geht § 113a Abs. 3 TKG weit über die noch im Referentenentwurf vorgesehene Identifizierungspflicht für E-Mail-Nutzer (§ 111 Ref-E TKG) hinaus.

Der Bevollmächtigte der Bundesregierung führt an, **§ 113b TKG** könne nicht isoliert zum Gegenstand einer Verfassungsbeschwerde gemacht werden.⁸⁵ § 113b TKG ist indes nicht der einzige Gegenstand der vorliegenden Verfassungsbeschwerde. Vielmehr richtet sich die Beschwerde gegen § 113a TKG, ohne den auch § 113b TKG keinen Regelungsgegenstand mehr hat. Die beantragte Aufhebung des § 113b TKG ist daher die notwendige Konsequenz der Nichtigkeit des § 113a TKG.

Der Bevollmächtigte meint, im Fall der Beschwerdeführerin zu 4 sei die **Subsidiarität** der Verfassungsbeschwerde nicht gewahrt, weil die Beschwerdeführerin vor den Fachgerichten eine Entschädigung erstreiten könne.⁸⁶ Dieses Argument ist bereits mit Schriftsatz vom 17.03.2008 widerlegt worden.⁸⁷ § 113a TKG gefährdet die berufliche Existenz deutscher Anonymisierungsdienste, ohne dass eine Entschädigung für Umsetzungskosten daran etwas ändern würde. Ein Anonymisierungsdienst, der zur Protokollierung aller Zugriffe verpflichtet ist, ist kein Anonymisierungsdienst mehr und verliert seine Kunden an internationale Dienste, die nicht zur Vorratsdatenspeicherung verpflichtet sind und eine echte Anonymisierung bieten können.

Der Bevollmächtigte meint, in der Vorratsdatenspeicherung liege nur ein **mittelschwerer Eingriff**.⁸⁸ Demgegenüber ist in der Beschwerdeschrift umfassend ausgeführt worden, weshalb ein tiefgreifender Grundrechtseingriff vorliegt.⁸⁹ Ergänzend ist die zutreffende Stellungnahme des Bundesverwaltungsgerichts vom 04.06.2008 zu zitieren. Danach weise die Vorratsdatenspeicherung eine „immense Breitenwirkung“ auf.⁹⁰ Sie nähere sich einer „Ermittlung ins Blaue hinein“ an.⁹¹ Weiter heißt es:⁹²

Damit ist ein erhöhtes Missbrauchsrisiko gesetzt und der spezifische Gefährdungstatbestand geschaffen, der den Grundrechtsschutz aus Art. 10 Abs. 1 GG begründet. Die Vielzahl der von der Speicherung umfassten Telekommunikationsdaten und die Dauer der Speicherung für einen feststehenden, nicht nur kurzfristigen Zeitraum von sechs Monaten tragen zur Intensität der Grundrechtsbeeinträchtigung bei. [...] Die Vorratsdatenspeicherung nach § 113a TKG ist eine flächendeckende Dauermaßnahme, die weder an eine Einschreitschwelle noch an eine Tatsachenbasis gebunden ist. Sie erfolgt vielmehr in tatsächlicher und

⁸⁵ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 24 ff.

⁸⁶ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 33.

⁸⁷ Schriftsatz vom 17.03.2008, 11.

⁸⁸ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 39.

⁸⁹ Beschwerdeschrift vom 31.12.2007, 72 ff.

⁹⁰ BVerwG, Stellungnahme vom 04.06.2008, 10.

⁹¹ BVerwG, Stellungnahme vom 04.06.2008, 7.

⁹² BVerwG, Stellungnahme vom 04.06.2008, 4 f. und 8.

rechtlicher Hinsicht voraussetzungslos. [...]Die Speicherungspflicht des § 113a TKG ist sachlich weitreichend und umfasst Daten mit potentiell hoher Persönlichkeitsrelevanz.

Der Bevollmächtigte meint, die Eingriffstiefe der Vorratsdatenspeicherung sei **in dreierlei Hinsicht abgeschwächt**:⁹³ Erstens würden Telekommunikationsinhalte nicht gespeichert. Dem wird jedoch bereits in der Beschwerdeschrift entgegen gehalten, dass Verkehrsdaten nach Nutzbarkeit und Verwendungsmöglichkeit weiter gehende Grundrechtseingriffe ermöglichen als Telekommunikationsinhalte.⁹⁴ Zweitens führt der Bevollmächtigte an, dass eine staatliche Kenntnisnahme der Daten nur unter weiteren Voraussetzungen erfolge. Dem ist bereits mit Schriftsatz vom 13.08.2008 entgegen gehalten worden, dass Nachteile infolge einer staatlichen Kenntnisnahme nur einen kleinen Teil der schädlichen Auswirkungen der Vorratsdatenspeicherung ausmachen.⁹⁵ Sehr viel schädlicher ist die abschreckende Wirkung bereits der Gefahr eines legalen staatlichen Zugriffs, der Gefahr illegaler Zugriffe durch das speichernde Unternehmen, Mitarbeiter des Unternehmens, staatliche Stellen, Staatsbeamte oder Dritte sowie der Gefahr einer versehentlichen Offenlegung der Daten durch das speichernde Unternehmen, dessen Mitarbeiter, staatliche Stellen, deren Mitarbeiter oder Dritte. Die grundrechtsschädliche Wirkung der Vorratsdatenspeicherung hängt größtenteils nicht von der Nutzung der Daten ab, sondern liegt in der dauernden, latenten Gefahr einer Nutzung oder Offenlegung sensibelster Informationen über unser persönliches Kommunikations-, Informations- und Bewegungsverhalten begründet. Drittens führt der Bevollmächtigte an, dass die Speicherung nicht heimlich erfolgt. Das Wissen um die Protokollierung stellt allerdings keine Abschwächung des Grundrechtseingriffs dar, sondern begründet ihn gerade. Denn es ist gerade die Kenntnis von der Protokollierung des eigenen Kommunikations- und Bewegungsverhaltens, von welcher die schädlichen Wirkungen der Vorratsdatenspeicherung auf das Gebrauchmachen von zahlreichen Grundrechten in unserer Gesellschaft ausgeht.

Umgekehrt könnte die Vorratsdatenspeicherung als „**dreifach verschärfter Grundrechtseingriff**“ bezeichnet werden: Sie trifft erstens flächendeckend die gesamte Bevölkerung, obwohl es an jeder Nähe der Betroffenen zu einer Straftat oder Gefahr fehlt. Sie erfolgt zweitens ohne jeden Tatverdacht oder sonstigen Anlass. Sie hat drittens die privatesten vorstellbaren maschinenverarbeitbaren Daten zum Gegenstand, nämlich Informationen über unser tägliches Kommunikations-, Informations- und Bewegungsverhalten, über unser soziales Umfeld und unsere geschäftlichen, privaten, ehrenamtlichen, politischen und Vertrauensbeziehungen, vertrauliche Kontakte und Bewegungen.

Der Bevollmächtigte der Bundesregierung greift erneut den Mythos auf, wonach die Vorratsdatenspeicherung lediglich die **Flüchtigkeit elektronischer Kommunikationsspuren** kompensieren solle.⁹⁶ Demgegenüber ist bereits in der Beschwerdeschrift ausgeführt worden, dass Kommunikation allgemein keine Spuren bei Dritten hinterlässt und ihre Nachverfolgbarkeit anhand von Verkehrsdaten anormal ist.⁹⁷ Verkehrsdaten sind keine zufällig hinterlassenen Spuren wie DNA-Spuren, sondern absichtlich und aktiv aufgezeichnete Protokolle, derer es für Abwicklung und Abrechnung der Telekommunikation nicht bedürfte.⁹⁸ Die Nichtprotokollierung des Kommunikations-, Informations- und Bewegungsverhaltens stellt ebenso wenig eine „Vernichtung von Spuren“ dar, wie es die fehlende Videoaufzeichnung sonstigen Verhaltens tut.

⁹³ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 40.

⁹⁴ Beschwerdeschrift vom 31.12.2007, 80 ff.

⁹⁵ Schriftsatz vom 13.08.2008, 4 f.

⁹⁶ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 41.

⁹⁷ Beschwerdeschrift vom 31.12.2007, 126 f.

⁹⁸ Näher Schriftsatz vom 17.03.2008, 5.

Der Bevollmächtigte führt einen Fall an, in dem nach dem **Raub eines Handys** mit diesem telefoniert wurde, der Anbieter aber kein Verbindungsprotokoll erstellt hatte.⁹⁹ Es ist nicht ersichtlich, wie sich dieser Fall von der Verwendung eines beliebigen sonstigen Raubgutes unterscheiden soll. Die Verwendung gestohlener Gegenstände ist allgemein nicht nachvollziehbar. Im Fall von Mobiltelefonen braucht dies nicht anders sein.

Der Bevollmächtigte behauptet erneut, § 100g StPO verliere wegen **Fehlens von Verkehrsdaten** zunehmend an Bedeutung, ohne irgend einen aussagekräftigen Beleg dafür vorzulegen. Dem ist bereits mit Schriftsatz vom 17.03.2008 entgegen gehalten worden, dass der staatliche Zugriff auf unser Kommunikations- und Bewegungsverhalten und die von staatlichen Stellen daraus gewonnenen Informationen in Wahrheit exponentiell ansteigen und zunehmen.¹⁰⁰

Die Behauptung zunehmend fehlender Verkehrsdaten will der Bevollmächtigte mit **Fallbeispielen** untermauern.¹⁰¹ Er bleibt dabei aber einen Beleg dafür schuldig, dass die erwünschten Verkehrsdaten früher verfügbar gewesen wären. Davon abgesehen, dass es Mobiltelefone und Internet früher überhaupt nicht gab, ist auch im Festnetzbereich früher taktbezogen ohne Protokollierung von Verbindungen abgerechnet worden. Für den Internetbereich ist bereits mit Schriftsatz vom 17.03.2008 ausgeführt worden, dass die Protokollierung der zugewiesenen IP-Adresse durch einige Internet-Zugangsanbieter immer schon illegal gewesen ist und deswegen nicht zum Maßstab erhoben werden kann.¹⁰²

Im einzelnen ist zu dem geschilderten **Trickbetrugsfall** zu sagen, dass Identifikationsdaten auch dann nicht vorhanden gewesen wären, wenn der Trickbetrug an der Haustür oder per Post begangen worden wäre. Zu dem Fall der versuchten Nötigung einer 12-jährigen im Internet ist zu bemerken, dass Identifikationsdaten auch im Fall eines direkten oder postalischen Kontakts zwischen den beiden Personen nicht verfügbar gewesen wären. Zu dem Fall der Online-Überweisung unter falschem Namen ist zu bemerken, dass Spuren auch im Fall eines unmittelbaren oder postalischen Überweisungsauftrags oder eines Geldabhebens mit ec-Karte nicht vorhanden gewesen wären. Außerdem ist die Annahme leichtgläubig, dass der professionell agierende Täter nicht ein Internet-Café, einen öffentlichen WLAN-Internetzugang oder einen internationalen Anonymisierungsdienst genutzt habe, um seine Identifizierung anhand der IP-Adresse zu vereiteln. An anderer Stelle gesteht der Bevollmächtigte selbst ein, dass Straftäter „so gut wie immer“ Anschlüsse anderer Personen einsetzen,¹⁰³ so dass auch die Verfügbarkeit weiterer Verkehrsdaten höchstwahrscheinlich nicht zur Zielperson geführt hätte.

Der Bevollmächtigte behauptet, dass die Auswertung von Verkehrsdaten ein **unverzichtbares Ermittlungsinstrument** darstelle. Dem ist im Einklang mit dem Europäischen Gerichtshof für Menschenrechte entgegen zu halten, dass die Strafverfolgungsbehörden der EU-Staaten bis vor kurzem auch ohne Vorratsprotokollierung der gesamten gesellschaftlichen Telekommunikation ausgekommen sind und viele Staaten bis heute ohne sie auskommen.¹⁰⁴ Staaten mit Vorratsdatenspeicherung weisen weder eine erkennbar höhere Aufklärungs- noch eine niedrigere Kriminalitätsrate auf als Staaten ohne Vorratsdatenspeicherung. Auch innerhalb eines Staates bewirkt die Einführung einer Vorratsdatenspeicherung keine erkennbare Steigerung der Aufklärungsrate oder Rückgang der Kriminalitätsrate. Mit Schriftsatz vom 17.03.2008 ist anhand der Studie des Max-Planck-Instituts belegt worden, dass die Vorratsdatenspeicherung die

⁹⁹ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 41.

¹⁰⁰ Näher Schriftsatz vom 17.03.2008, 6 und 9 ff.

¹⁰¹ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 43 ff.

¹⁰² Schriftsatz vom 17.03.2008, 3.

¹⁰³ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 49.

¹⁰⁴ EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 115 f.

Aufklärungsquote bestenfalls um 0,002% steigern könnte.¹⁰⁵ Die Vorratsdatenspeicherung ist daher aus empirischer Sicht problemlos verzichtbar. Das Europaparlament als Gesetzgeber hat dies im Jahr 2005 verkannt, weil es auf eine empirische Untersuchung der Situation weitgehend verzichtet hat. Auch der deutsche Umsetzungsgesetzgeber hat den fehlenden Bedarf nach Vorratsdaten verkannt, weil die einschlägige Studie des Max-Planck-Instituts erst Anfang 2008 veröffentlicht worden ist.

Zu den weiter vom Bevollmächtigten angeführten **Einzelfällen** (StAen Traunstein, Osnabrück, Bielefeld, Frankfurt/Oder, Neuruppin, Dessau-Roßlau, Mainz, Konstanz, Stuttgart, Hamburg)¹⁰⁶ ist zu bemerken, dass in keinem Fall nachvollziehbar dargetan ist, dass Verkehrsdaten tatsächlich zu einer Verurteilung geführt hätten. Außerdem ereigneten sich die Fälle allesamt zu einer Zeit, zu der die Vorratsdatenspeicherung nicht in Kraft war. Sie taugen daher von vornherein nicht zum Beleg der Behauptung, dass § 113a TKG erforderlich sei.

Soweit der Bevollmächtigte aus der im vorliegenden Verfahren vorgelegten **Statistik der Bundesregierung** einen Beleg für die angebliche Erforderlichkeit des § 113a TKG herleiten will, ist bereits mit Schriftsatz vom 13.08.2008 ausgeführt worden, weshalb die vorgelegten Zahlen einen solchen Rückschluss nicht zulassen:¹⁰⁷ Die Statistik lässt nicht auf einen Bedarf nach Vorratsdaten schließen, weil Strafverfolgungsbehörden Vorratsdaten nicht erst anfordern, nachdem der Zugriff auf ohnehin gespeicherte Abrechnungsdaten erfolglos geblieben ist, und weil zweitens die Erheblichkeit der Vorratsdaten für den Verfahrensausgang nicht erfasst worden ist. Aussagekräftig ist einzig die im Februar 2008 vorgelegte Untersuchung des unabhängigen Max-Planck-Instituts, der zufolge den Strafverfolgern nur in 0,01% aller Ermittlungsverfahren Verbindungsdaten fehlten.

Der Bevollmächtigte kritisiert die Grenzen eines **Quick-Freeze-Verfahrens**¹⁰⁸, welches einzuführen die Bundesregierung bislang unter Verstoß gegen Art. 16 des Übereinkommens über Computerkriminalität¹⁰⁹ versäumt hat. Der Bevollmächtigte verkennt bei seiner Kritik an den Grenzen dieses Verfahrens, dass es eine ganze Palette milderer Mittel zu einer Vorratsdatenspeicherung gibt, wie sie mit Schriftsatz vom 13.08.2008 im Einzelnen dargestellt worden sind.¹¹⁰ Diese Mittel können die Beschränkungen des Quick-Freeze-Verfahrens weitgehend vermeiden, ohne eine pauschale und globale Sammlung des Kommunikations-, Informations- und Bewegungsverhaltens der gesamten Bevölkerung zu erfordern.

In der Beschwerdeschrift¹¹¹ und mit Schriftsatz vom 13.08.2008¹¹² ist dargestellt worden, dass und weshalb eine auch nur teilweise Aufrechterhaltung des § 113a TKG mit der **ständigen Rechtsprechung** des Hohen Gerichts brechen würde. Dem will der Bevollmächtigte der Bundesregierung entgegen halten, dass sich diese Entscheidungen auf Normen bezogen hätten, mit denen der Staat auf Daten zugreifen konnte.¹¹³ Dass sich die bisherigen Entscheidungen des Bundesverfassungsgerichts noch nicht auf die Vorratsdatenspeicherung bezogen haben, ist indes eine Selbstverständlichkeit, da sich das Gericht bisher nicht mit § 113a TKG befassen musste. Dies ändert aber nichts daran, dass das Hohe Gericht in ständiger

¹⁰⁵ Schriftsatz vom 17.03.2008, 1 f.

¹⁰⁶ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 45 ff.

¹⁰⁷ Schriftsatz vom 13.08.2008, 6 f.

¹⁰⁸ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 51.

¹⁰⁹ Übereinkommen vom 23.11.2001.

¹¹⁰ Schriftsatz vom 13.08.2008, 33 f.

¹¹¹ Beschwerdeschrift vom 31.12.2007, 12 f.

¹¹² Schriftsatz vom 13.08.2008, 34 f.

¹¹³ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 58.

Rechtsprechung Eingriffsgrenzen aus den Grundrechten abgeleitet hat, die über die entschiedenen Einzelfälle hinaus Geltung beanspruchen. Dazu gehört die Voraussetzung bestimmter Verdachts- oder Gefahrenstufen für Grundrechtseingriffe,¹¹⁴ das Gebot eines hinreichenden Anlasses für Eingriffe¹¹⁵ und das Erfordernis der hinreichenden Wahrscheinlichkeit einer Rechtsgutsverletzung¹¹⁶. § 113a TKG greift völlig losgelöst von jeder Nähe zu einer Straftat oder Gefahr ein und verletzt damit den grundrechtlich verbürgten Freiheitsanspruch jedes Menschen in Deutschland.

Im Übrigen ist es auch nicht richtig, dass die **bisherige Rechtsprechung** des Bundesverfassungsgerichts nur Fälle der staatlichen Kenntnisaufnahme von Daten zum Gegenstand gehabt hätte. Einen hinreichenden Anlass hat das Hohe Gericht etwa auch als Voraussetzung eines automatisierten Kfz-Massenabgleichs gefordert, selbst wenn der automatisierte Abgleich regelmäßig spurlos erfolgt und staatliche Stellen mithin keine Kenntnis von den gesichteten Kraftfahrzeugen erlangen. Was für automatisierte, maschinelle Eingriffe in die Privatsphäre ohne Kenntnisaufnahme durch einen Staatsbeamten gilt, muss erst Recht für staatlich veranlasste Eingriffe in die Privatsphäre durch Dritte gelten, deren Ziel es ist, staatliche Kenntnisaufnahmen zu einem späteren Zeitpunkt zu ermöglichen. Dass das bloße Outsourcing der Datenspeicherung an Private verfassungsrechtlich ohne Bedeutung ist, ist bereits in der Beschwerdeschrift erläutert worden.¹¹⁷

Absurd ist die Auffassung des Bevollmächtigten der Bundesregierung, im Vergleich zu einer Maßnahme, die „viele Personen ohne Rücksicht auf individuelles Verhalten betrifft“, sei die Anknüpfung des Gesetzgebers an ein **individuelles Verhalten** „regelmäßig dazu geeignet, die Eingriffsintensität zu verstärken“.¹¹⁸ Mit dieser Argumentation käme einem Massenmord an Unschuldigen eine geringere Eingriffsintensität zu als einem finalen Rettungsschuss.

Das Bundesverfassungsgericht berücksichtigt bei seinen Urteilen zu Recht nicht nur, wie einschneidend die Maßnahme für den einzelnen Betroffenen ist. Denn die Grundrechte haben eine gesamtgesellschaftliche Funktion und bringen eine objektive **Werteordnung** zum Ausdruck. Nur das Primat der Freiheit bewahrt Unschuldige ausreichend vor staatlichen Vor- und Fehlurteilen. Nur auf diese Weise kann die unbefangene Mitwirkung der Bürger an einer demokratischen Willensbildung gesichert werden. Wenn der Staat beginnt, mit individuell vielleicht nicht unmittelbar einschneidenden Maßnahmen rechtschaffene und anständige Bürger massenhaft zu erfassen und zu kontrollieren, geht damit eine grundlegende Machtverschiebung einher, die mittelbar das unbefangene Gebrauchsmachen von Grundrechten beeinträchtigt und dadurch die Funktionsfähigkeit einer lebendigen Demokratie einschränkt. Diese abschreckende Nebenwirkung von Massenerfassung und Massenüberwachung ist überaus grundrechtsrelevant und findet vor dem Hohen Gericht zu Recht Berücksichtigung. Diese Berücksichtigung ist auch kein Alleingang des Bundesverfassungsgerichts, sondern internationaler Standard. So hat der Europäische Gerichtshof für Menschenrechte bereits im Jahr 1978 ausgeführt:¹¹⁹

Gleichwohl unterstreicht der Gerichtshof, daß dies nicht bedeutet, die Vertragsstaaten hätten ein unbegrenztes Ermessen, Personen innerhalb ihres Hoheitsbereichs geheimer Überwachung zu unterwerfen. Im Bewußtsein der Gefahr, die ein solches Gesetz in sich birgt,

¹¹⁴ BVerfG, 1 BvR 518/02 vom 4.4.2006, Absatz-Nr. 88; BVerfG, 1 BvR 2074/05 vom 11.3.2008, Absatz-Nr. 168.

¹¹⁵ BVerfG, 1 BvR 2074/05 vom 11.3.2008, Absatz-Nr. 171 ff..

¹¹⁶ BVerfG, 1 BvR 518/02 vom 4.4.2006, Absatz-Nr. 136; BVerfG, 1 BvR 2074/05 vom 11.3.2008, Absatz-Nr. 169.

¹¹⁷ Beschwerdeschrift vom 31.12.2007, 41 ff.

¹¹⁸ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 60.

¹¹⁹ EGMR, NJW 1979, 1755 (1757) – Klass u.a.

nämlich die Demokratie mit der Begründung, sie zu verteidigen, zu untergraben oder sogar zu zerstören, bekräftigt der Gerichtshof, daß die Vertragsstaaten nicht im Namen des Kampfes gegen Spionage und Terrorismus zu jedweder Maßnahme greifen dürfen, die ihnen geeignet erscheint.

Auch der EGMR berücksichtigt in seiner Rechtsprechung also, dass man des Schutzes der Grundrechte willen nicht dieselben aufgeben darf oder – drastisch formuliert – dass man sich nicht aus Angst vor dem Tod selbst umbringen darf. Um dies zu verhindern, müssen die mittelbaren und **gesamtgesellschaftlichen Auswirkungen** eines Grundrechtseingriffs wie der Vorratsdatenspeicherung Berücksichtigung finden. Wie drastisch diese Auswirkungen sind, ist in sämtlichen Schriftsätzen und auch mit der vorgelegten Meinungsumfrage deutlich gemacht worden.

Der Bevollmächtigte der Bundesregierung meint, § 113a TKG sei verfassungsrechtlich nicht zu beanstanden, weil er hinsichtlich der **persönlichkeitsrelevanten Qualität** der zu speichernden Daten nicht über bestehende Regelungen – etwa § 100g StPO – hinaus gehe.¹²⁰ Dass die Aufdeckung des Kommunikations- und Bewegungsverhaltens eines Verdächtigen noch mit überwiegenden Interessen des Rechtsgüterschutzes zu rechtfertigen sein mag, bedeutet jedoch nicht, dass auch die anlass- und verdachtslose, flächendeckende und permanente Erfassung des Kommunikations-, Informations- und Bewegungsverhaltens der gesamten Bevölkerung zu rechtfertigen wäre.

Der Bevollmächtigte der Bundesregierung meint, die Eingriffsintensität der Vorratsdatenspeicherung werde dadurch gemindert, dass sie nicht **heimlich** erfolge.¹²¹ Das Kriterium der Heimlichkeit ist indes für einzelfallbezogene, gezielte Ermittlungsmaßnahmen geschaffen worden. Es lässt sich nicht übertragen auf eine permanente, flächendeckende, anlasslose Maßnahme. Mit der Auffassung des Bevollmächtigten der Bundesregierung wäre eine tägliche, anlasslose offene Hausdurchsuchung bei der gesamten Bevölkerung weniger eingriffsintensiv als die Gefahr einer geheimen Wohnungsdurchsuchung in einzelnen Verdachtsfällen. Dass dies nicht zutreffen kann, liegt auf der Hand.

Der Bevollmächtigte der Bundesregierung beruft sich auf Rechtsprechung, wonach die Überwachung auch von **Gesprächsinhalten** einen tiefergreifenden Grundrechtseingriff darstelle als die Aufdeckung des Kommunikationsverhaltens anhand der Kommunikationsumstände.¹²² Demgegenüber ist bereits in der Beschwerdeschrift ausführlich erläutert worden, dass die Einbeziehung von Kommunikationsinhalten nur eine quantitative Erhöhung des Informationsgehalts bewirkt,¹²³ wie sie etwa auch Folge der Abfrage von Verkehrsdaten über einen zeitlich längeren Zeitraum hinweg oder der Abfrage der Verkehrsdaten weiterer Personen ist. Beispielsweise ist das Abhören eines einzelnen belanglosen Telefongesprächs zwischen Nachbarn keineswegs eingriffsintensiver als die Ermittlung, mit welchen Freunden, Bekannten, Geschäftspartnern, Ärzten, Rechtsanwälten, Beratungsstellen usw. jemand in den letzten sechs Monaten in Kontakt hatte und wo er sich mit seinem Mobiltelefon in den letzten sechs Monaten aufgehalten hat. Die Erhebung von Inhalten stellt nicht per se einen qualitativen Sprung in der Eingriffstiefe dar. Kriminalisten räumen umgekehrt ein, dass – wenn sie wählen müssten – sich aus Verbindungs- und Standortdaten mehr und wichtigere Informationen gewinnen lassen als aus Kommunikationsinhalten, zumal Verkehrsdaten mühelos und in großer Menge maschinell kombiniert, analysiert und zusammen geführt werden können. Gerade die Nutzbarkeit und

¹²⁰ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 63.

¹²¹ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 63.

¹²² Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 63.

¹²³ Näher Beschwerdeschrift vom 31.12.2007, 80 ff.

Verwendungsmöglichkeiten der maßgeblichen Informationen ist nach der Rechtsprechung des Hohen Gerichts für die Verhältnismäßigkeitsprüfung entscheidend, nicht die Art der Informationen. In Anlehnung an das Volkszählungsurteil sind Verkehrsdaten keine per se „belangloseren“ Informationen als Kommunikationsinhalte.

Soweit sich der Bevollmächtigte der Bundesregierung auf Rechtsprechung zur strategischen, flüchtigen **Auslandsüberwachung** beruft, ist bereits in der Beschwerdeschrift dargelegt worden, weshalb diese nicht auf die Zulässigkeit der flächendeckenden Vorratsdatenspeicherung schließen lässt.¹²⁴

Soweit der Bevollmächtigte der Bundesregierung aus der vermeintlichen (tatsächlich ungeklärten) Zulässigkeit anderer **Aufbewahrungspflichten** auf die Zulässigkeit des § 113a TKG schließen will,¹²⁵ ist bereits in der Beschwerdeschrift ausgeführt worden: „Es handelt sich aber um jahresabschluss- und steuerrelevante Daten, die zu einem bestimmten Zweck – etwa der Steuerfestsetzung – tatsächlich benötigt werden und nur nicht im Hinblick auf denkbare zukünftige Zugriffswünsche der Eingriffsbehörden auf Vorrat gespeichert werden.“¹²⁶ Im Fall der §§ 257 HGB, 147 AO, 24c KWG ist also ein konkreter Bedarf und eine direkte Sachnähe der Betroffenen zum Ziel der Datenspeicherung gegeben, während im Fall der Vorratsdatenspeicherung fast nie ein Bedarf nach den Daten besteht und die Betroffenen in keinerlei Nähebeziehung zu einer Straftat oder Gefahr stehen. Außerdem macht es einen großen Unterschied, ob der Betroffene Aufzeichnungen über sein eigenes Geschäft führen muss oder ob sein Telekommunikationsanbieter Aufzeichnungen über ihn führt und er die Verwendung der Daten nicht kontrollieren kann und auch nicht zuverlässig davon erfährt. Schließlich sind Informationen über unser tägliches Kommunikations-, Informations- und Bewegungsverhalten auch inhaltlich weitaus persönlichkeitsrelevanter als Geschäftsbriefe und Finanztransaktionen.

Soweit der Bevollmächtigte der Bundesregierung auf die Entscheidung zur **Kontodatei** rekurriert, sind die grundlegenden Unterschiede zur Vorratsdatenspeicherung bereits in der Beschwerdeschrift dargestellt worden.¹²⁷

Der Bevollmächtigte der Bundesregierung meint, das Bundesverfassungsgericht halte die **flächendeckende Aufbewahrung** von Informationen in bestimmten Fällen für zulässig.¹²⁸ Richtig ist, dass das Hohe Gericht in keiner Entscheidung die flächendeckende Aufbewahrung von Informationen als zulässig bezeichnet hat, insbesondere nicht in der Entscheidung zur strategischen Auslandsüberwachung, in der nur eine zeitlich begrenzte, flüchtige Filterung des Fernmeldeverkehrs mit bestimmten Staaten in Rede stand.

Der Bevollmächtigte der Bundesregierung behauptet, „dass bestimmte Kommunikationsformen, in denen sich **schwere Kriminalität** abspielt, überhaupt nur durch den Rückgriff auf die hier erhobenen Verkehrsdaten oder auf die noch grundrechtssensibleren Gesprächsinhalte erfasst werden können“. Soweit damit behauptet werden soll, dass die Vorratsdatenspeicherung zur Aufklärung schwerer Kriminalität erforderlich sei, ist dem bereits umfassend entgegen gehalten worden, dass eine wirksame Strafverfolgung auch ohne Vorratsdatenspeicherung möglich ist¹²⁹

¹²⁴ Beschwerdeschrift vom 31.12.2007, 76 f.

¹²⁵ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 64 f.

¹²⁶ Beschwerdeschrift vom 31.12.2007, 75 f.

¹²⁷ Beschwerdeschrift vom 31.12.2007, 76.

¹²⁸ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 64.

¹²⁹ Schriftsatz vom 17.03.2008, 1 ff.

und diese sogar überwiegend kontraproduktive Wirkungen entfaltet.¹³⁰ Auch ist bereits ausgeführt worden, dass der Staat etwa zufällig aus betrieblichen Gründen vorhandene Verbindungsdaten keineswegs flächendeckend für die gesamte Bevölkerung ohne Anlass beanspruchen kann.¹³¹ Mit der gegenteiligen Ansicht des Bevollmächtigten der Bundesregierung, wonach die Verfügbarkeit von Spuren nicht von „**Zufälligkeiten der Preisbildung**“ abhängen dürfe,¹³² ließe sich etwa auch ein Zwang zur Abgabe des Fingerabdrucks bei Betreten eines Gebäudes oder ein allgemeiner Fahrtenbuchzwang rechtfertigen, denn auch bei Fingerabdrücken, Reifenspuren und sonstigen Spuren hängt es selbstverständlich vom Zufall ab, ob sie von einem Straftäter hinterlassen werden oder nicht. Das deutsche Recht kennt zu Recht keine anlasslose und flächendeckende Aufbewahrung von Spuren menschlichen Verhaltens allein zum Zweck der Erleichterung möglicher zukünftiger staatlicher Ermittlungen. Wenn der Staat jeden Bürger wie einen potenziellen Straftäter behandeln dürfte, wären die Grundrechte, das Erforderlichkeitsprinzip und das Verhältnismäßigkeitsgebot obsolet.

Soweit der Bevollmächtigte der Bundesregierung veränderte **Abrechnungsmodelle** (Flatrates) beklagt, ist bereits ausgeführt worden, dass in den letzten Jahren weder die Menge an verfügbaren Verkehrsdaten abgenommen hat, noch die Strafverfolgung erschwert worden ist.¹³³ Ohnehin wäre eine Abnahme der verfügbaren Datenmenge nicht geeignet, eine anlasslose und flächendeckende Vorratsdatenspeicherung zu rechtfertigen.¹³⁴

Der Bevollmächtigte der Bundesregierung meint, im Unterschied etwa zu DNA-Spuren und Fingerabdrücken auf einem **Brief** ließen sich Telekommunikationsspuren einfach vernichten¹³⁵. Dies ist unzutreffend. Ein Straftäter kann bei seinem Telekommunikationsanbieter vorgenommene Aufzeichnungen überhaupt nicht vernichten. Er kann zwar durch Wahl des Abrechnungsmodells, durch Nutzung anonymer Produkte und auf andere Weise die Entstehung identifizierbarer Spuren seiner elektronischen Kommunikation vermeiden. Dies ist aber auch bei DNA-Spuren und Fingerabdrücken auf einem Brief möglich. Im Übrigen können Briefe anonym versandt werden, was die Zuordnung zum Absender erschwert. Weiters können Strafverfolgungsbehörden Briefe regelmäßig nur bei dem Empfänger überhaupt erlangen, während Telekommunikationsspuren bei dem Vermittler anfallen und dort von staatlichen Behörden insgeheim erhoben werden können. Die Telekommunikation ist daher besonders anfällig für staatliche Überwachung und nicht besonders davor geschützt, wie der Bevollmächtigte der Bundesregierung Glauben machen will.

Der Bevollmächtigte schildert einen **Fall**, in dem eine „Verkehrsdatenabfrage zur Ermittlung eines vom Beschuldigten gegenüber seinem Gesprächspartner angekündigten neuen Mobilfunkanschlusses“ geführt habe.¹³⁶ Diese Argumentation ist allerdings nicht nachvollziehbar: Wenn der Beschuldigte den neuen Anschluss gegenüber seinem Gesprächspartner angekündigt hatte und dieses Gespräch offenbar abgehört wurde (§ 100a StPO), weshalb soll es dann noch der Vorratsdatenspeicherung bedürft haben, um die ohnehin schon bekannte Nummer zu ermitteln? Im Übrigen ist nicht ersichtlich, dass die Datenerhebung für den Verfahrensausgang von Bedeutung gewesen wäre.

¹³⁰ Schriftsatz vom 17.03.2008, 7.

¹³¹ Schriftsatz vom 17.03.2008, 4 f.

¹³² Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 64.

¹³³ Schriftsatz vom 13.08.2008, 26 ff.; Schriftsatz vom 17.03.2008, 3 ff.

¹³⁴ Näher Schriftsatz vom 13.08.2008, 29 f.

¹³⁵ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 66 f.

¹³⁶ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 67.

Der Bevollmächtigte der Bundesregierung meint, Telekommunikationsspuren seien besonders **flüchtig**.¹³⁷ Demgegenüber ist schon umfassend ausgeführt worden, dass bei anderen Kommunikationsformen (z.B. persönliche Treffen, postalische Kommunikation) regelmäßig überhaupt keine Spuren auf dem Übertragungsweg zurückbleiben. Auch ist oben schon dargestellt worden, dass Verkehrsdaten keine zufällig zurückbleibenden „Spuren“ darstellen, sondern bewusst erstellte und vorgehaltene Protokolle.

Der Bevollmächtigte der Bundesregierung bestreitet, dass von der Vorratsdatenspeicherung ein **Einschüchterungseffekt** ausgeht.¹³⁸ Diese Wirkung der Vorratsdatenspeicherung ist aber im einzelnen dargelegt¹³⁹ sowie anhand von Fallbeispielen¹⁴⁰ und einer repräsentativen Umfrage¹⁴¹ belegt worden. Der Bevollmächtigte behauptet, schon früher sei von der Verbindungsdatenspeicherung zu betrieblichen Zwecken keine Abschreckungswirkung ausgegangen. Diese Behauptung ist jedoch erstens bereits nicht belegt. Zweitens standen vor Einführung des § 113a TKG ausreichende Möglichkeiten auch für Normalbürger zur Verfügung, um eine Protokollierung ihrer Kontakte zu vermeiden (z.B. Flatrates, Guthabekarten). Von vermeidbaren Spuren geht eine vergleichbare Abschreckungswirkung natürlich nicht aus. Drittens hat der unersättliche staatliche Überwachungshunger im Allgemeinen und die ausufernde Überwachung der Nutzung von Telefon, Handy und E-Mail im Speziellen das Bewusstsein der Menschen für die Risiken von Kommunikationsspuren gestärkt.

Der Bevollmächtigte der Bundesregierung will eine abschreckende Wirkung von Grundrechtseingriffen nur berücksichtigen, wenn die Betroffenen ein **„zutreffendes Verständnis** des Inhalts der angegriffenen Regelungen“ haben.¹⁴² Diese Meinung wird dem Zweck der Grundrechte nicht gerecht. Unser demokratisches Staatswesen (Art. 20 Abs. 1 GG) ist auf die aktive und unbefangene Mitwirkung aller Bürger angewiesen,¹⁴³ und zwar unabhängig von ihrem Bildungsstand und ihrer Gesetzeskenntnis. Im Übrigen muss die überhebliche Auffassung bestritten werden, dass in der Bevölkerung ein unzutreffendes Verständnis der Vorratsdatenspeicherung vorherrsche. Der Bevollmächtigte der Bundesregierung hält die Menschen zu Unrecht für dumm. Es ist durchaus in Grundzügen allgemein bekannt, dass seit 2008 die näheren Umstände jeder Nutzung von Telefon, Handy, E-Mail und Internet protokolliert werden und der Staat etwa in Gestalt der Strafverfolgungsbehörden darauf unter bestimmten Voraussetzungen Zugriff nehmen kann. Wenn die Menschen wegen § 113a TKG die Gefahr eines falschen Verdachts, einer irtümlichen Veröffentlichung oder einer missbräuchlichen Offenlegung ihres global und pauschal aufgezeichneten Kommunikations- und Bewegungsverhaltens sehen, so sind diese Befürchtungen nicht unreal, sondern – wie gerade die zahlreichen im letzten Jahr bekannt gewordenen Skandale gezeigt haben – realistisch und begründet. Diesem Schriftsatz wird als

Anlage 1

eine Aufstellung einiger Fälle beigefügt, in denen es in der Vergangenheit zu Datenmissbrauch und falschem Verdacht gekommen ist.

¹³⁷ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 67.

¹³⁸ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 69.

¹³⁹ Beschwerdeschrift vom 31.12.2007, 95 ff.

¹⁴⁰ Schriftsatz vom 11.02.2008.

¹⁴¹ Anlage 1 zum Schriftsatz vom 13.08.2008.

¹⁴² Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 70.

¹⁴³ BVerfGE 65, 1 (43); BVerfGE 100, 313 (381).

Entgegen der Behauptung des Bevollmächtigten der Bundesregierung¹⁴⁴ suggeriert die Webseite www.vorratsdatenspeicherung.de nicht wahrheitswidrig, dass Vorratsdaten dem Staat ohne weiteres zur Verfügung stünden. Umgekehrt hat die Bundesjustizministerin im Vorfeld des Gesetzesbeschlusses mehrfach unzutreffende Verharmlosungen der Vorratsdatenspeicherung in der Öffentlichkeit vorgenommen. So hat die Bundesjustizministerin vor dem Bundestag wahrheitswidrig behauptet, bei der Vorratsdatenspeicherung gehe es um „schwerste Kriminalität“, ein Zugriff werde nur bei dem „Verdacht auf eine erhebliche Straftat“ zugelassen, nur „Daten, die für Abrechnungszwecke gebraucht werden, werden gespeichert“ oder die EU-Richtlinie zur Vorratsdatenspeicherung werde „in minimaler Weise“ umgesetzt.¹⁴⁵

Entgegen der Behauptung des Bevollmächtigten der Bundesregierung¹⁴⁶ hat das Bundesverfassungsgericht nicht entschieden, dass von der Vorratsdatenspeicherung selbst noch kein **Einschüchterungseffekt** ausgehen könne. Das Hohe Gericht hat lediglich entschieden, dass die einschüchternde Wirkung des § 113a TKG nicht so groß sei, dass die Aussetzung eines durch zwingendes Europarecht vorgegebenen Parlamentsgesetzes im Wege der einstweiligen Anordnung geboten sei.¹⁴⁷ Das Gericht hat indes bestätigt, dass „die in § 113a TKG angeordnete umfassende und anlasslose Bevorratung sensibler Daten über praktisch jedermann für staatliche Zwecke [...] einen erheblichen Einschüchterungseffekt bewirken“ kann.¹⁴⁸ Auch hat das Gericht „die durch §§ 113a und 113b TKG begründete Beeinträchtigung der allgemeinen Unbefangenheit des elektronischen Informations- und Gedankenaustauschs“ anerkannt.¹⁴⁹

Der Bevollmächtigte der Bundesregierung moniert, es fehle zu **Art. 14 GG** eine substantiierte Darlegung, dass technische Einrichtungen der Beschwerdeführer durch die Vorratsdatenspeicherung entwertet würden.¹⁵⁰ Demgegenüber sind die Beschwerdeführer der Auffassung, dass der bisherige Vortrag zu diesem Punkt jedenfalls für das Hauptsacheverfahren genügt. Im Übrigen hat auch das Verwaltungsgericht Berlin eine Vorlage nach Art. 100 GG wegen des Entschädigungsausschlusses durch § 110 TKG vorgenommen und das diesbezügliche Vorbringen des betroffenen Anbieters augenscheinlich für ausreichend erachtet.

Der Bevollmächtigte der Bundesregierung moniert, es fehle an Vortrag der Beschwerdeführer zu **Art. 12 GG**, wonach ihr Unternehmen wegen § 113a TKG nicht mehr profitabel zu betreiben sei.¹⁵¹ Demgegenüber ist mit Schriftsatz vom 13.08.2008 und der Anlage 2 dazu gerade zu dieser Frage im Einzelnen vorgetragen worden.

Der Bevollmächtigte der Bundesregierung meint, den von § 113a TKG betroffenen Unternehmen stehe regelmäßig die zur Vorratsdatenspeicherung **erforderliche Infrastruktur** ohnehin zur Verfügung. Diese Behauptung wird indes bereits in der Beschwerdeschrift widerlegt.¹⁵² Der Bevollmächtigte behauptet auch, die nach § 113a TKG zu speichernden Daten entstünden aus technischen Gründen ohnehin. Dass nach § 113a TKG nur ohnehin verarbeitete Daten zu speichern sind, bedeutet aber nicht, dass die Unternehmen auch auf eine Protokollierung und längerfristige Vorhaltung der normalerweise nur flüchtig verarbeiteten Daten vorbereitet wären. Unzutreffend ist die Behauptung des Bevollmächtigten, die zur Umsetzung des § 113a TKG

¹⁴⁴ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 70.

¹⁴⁵ BT-Prot. 16/124, 12994 ff.

¹⁴⁶ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 71.

¹⁴⁷ Beschluss vom 11.03.2008, Abs. 150.

¹⁴⁸ Beschluss vom 11.03.2008, Abs. 148.

¹⁴⁹ Beschluss vom 28.10.2008, Abs. 92.

¹⁵⁰ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 73.

¹⁵¹ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 73 f.

¹⁵² Näher Beschwerdeschrift vom 31.12.2007, 109 ff.

angeschafften Anlagen ließen sich auch betriebsintern nutzen. Richtig ist, dass § 113a TKG eine Nutzung der zu speichernden Daten zu eigenen Zwecken des Anbieters ausschließt.

Dem Hinweis des Bevollmächtigten, kleine Unternehmen würden durch die Anhebung der Grenze des § 3 Abs. 2 Nr. 5 **TKÜV** entlastet,¹⁵³ ist entgegen zu halten, dass diese Grenze für die Verpflichtung zur Vorratsdatenspeicherung gerade nicht gilt, dass vielmehr selbst kleinste Anbieter, die über Jahre hinweg keine Anfrage von Strafverfolgungsbehörden erhalten haben, die Kommunikation ihrer Kunden ohne Anlass protokollieren müssen.

Soweit sich der Bevollmächtigte der Bundesregierung gegen die zutreffende Rechtsmeinung des VG Berlin sowie der Verfassungsgerichte anderer Länder¹⁵⁴ stellt, wonach Nichtverantwortliche für ihre Inanspruchnahme im öffentlichen Interesse angemessen zu **entschädigen** sind, ist bereits in der Beschwerdeschrift eingehend dargelegt worden, dass zwar die vom Bundesverfassungsgericht entwickelten Anforderungen an Sonderabgaben nicht anzuwenden sind, dass eine entschädigungslose Inanspruchnahme Nichtverantwortlicher jedoch schon nach allgemeinen Maßstäben mit Art. 3 GG unvereinbar ist.¹⁵⁵

Der Bevollmächtigte der Bundesregierung behauptet zu Art. 3 GG, **organisierte Kriminalität** und andere Kriminalitätsformen seien durch unmittelbare Kommunikation allein nicht zu bewerkstelligen. Das Gegenteil belegen nicht nur historische Formen krimineller Vereinigungen, sondern auch moderne Formen wie das terroristische Netzwerk Al Quaida, das auf die Verwendung von Telekommunikation bewusst verzichtet. Der Bevollmächtigte der Bundesregierung meint ferner, kinderpornografische Darstellungen könnten nur über das Internet verbreitet werden. Die Praxis der Vergangenheit und der Gegenwart belegt indes das Gegenteil. Datenträger und Fotos lassen sich ohne weiteres auch unmittelbar oder per Post (etwa auch einer verschlüsselten CD-Rom) weitergeben.

Der Bevollmächtigte der Bundesregierung meint, **unmittelbare Kommunikation** gestatte eine Protokollierung nicht in gleicher Weise wie elektronische Kommunikation. Dem ist ausdrücklich zuzustimmen. Es ist aber bereits in der Beschwerdeschrift ausgeführt worden, weshalb die bloße technische Machbarkeit der Überwachung einer Kommunikationsform nicht ihre Ungleichbehandlung gegenüber anderen Kommunikationsformen rechtfertigt.¹⁵⁶

Der Bevollmächtigte der Bundesregierung vertritt die Auffassung, eine **Gleichbehandlung von unmittelbarer und elektronischer Kommunikation** würde entweder jegliche Speicherung elektronischer Daten, also beispielsweise auch diejenige von Bestandsdaten, ausschließen oder die Speicherung auch von Inhalten unmittelbarer Kommunikation gebieten.¹⁵⁷ Diese Auffassung ist nicht nachvollziehbar. Die Gleichbehandlung von unmittelbarer und elektronischer Kommunikation gebietet es, in beiden Fällen nur anlass- und verdachtsbezogen zu ermitteln, anstatt die gesamtgesellschaftlichen elektronischen Kommunikationsbeziehungen und Kundendaten (Bestandsdaten) flächendeckend protokollieren zu lassen. Im Fall unmittelbarer Kommunikation kann eine anlassbezogene Ermittlung etwa durch den Einsatz verdeckter Ermittler oder technischer Mittel (§ 100c StPO) erfolgen. Im Fall elektronischer Kommunikation kann eine anlassbezogene Ermittlung durch eine Abhör- oder Speicherungsanordnung erfolgen (§ 100g StPO).

¹⁵³ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 74.

¹⁵⁴ Beschwerdeschrift vom 31.12.2007, 148 m.w.N.

¹⁵⁵ Beschwerdeschrift vom 31.12.2007, 145 ff.

¹⁵⁶ Beschwerdeschrift vom 31.12.2007, 126 ff.

¹⁵⁷ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 80 f.

Der Bevollmächtigte der Bundesregierung behauptet, die **postalische Kommunikation** sei „spurenintensiver als elektronische Kommunikation“, namentlich wegen Schriftspuren und DNA-Spuren. Dies ist unzutreffend. Erstens lassen sich solche Spuren auf Postsendungen vermeiden. Zweitens ermöglichen etwaige Spuren auf Postsendungen keinen Rückschluss auf die Person des Täters, weil es kein Register aller Drucker oder aller DNA-Profile gibt. Im Übrigen fallen bei der elektronischen Kommunikation auch ohne Vorratsdatenspeicherung vergleichbare Spuren wie bei Briefen an. So lässt sich typischerweise der verwendete Browser oder die verwendete E-Mail-Software feststellen. Auch anhand der Schreibweise und des Tippverhaltens kann die moderne Kriminologie Täter identifizieren, ohne dass Verkehrsdaten benötigt würden.

Der Bevollmächtigte der Bundesregierung meint, die Post eigne sich wegen der **Postlaufzeiten** und mangels unmittelbarer Kommunikation weniger für strafbare Handlungen.¹⁵⁸ Dem ist bereits in der Beschwerdeschrift entgegen gehalten worden, dass die Post andere Vorteile aufweist, die ihre Nutzung zu strafbaren Zwecken begünstigen:¹⁵⁹ Weil bei dem postalischen Verkehr kein Absender angegeben werden muss, eröffnet die Post eine gute Möglichkeit des konspirativen Informationsaustausches zwischen Straftätern. Ebenso wie im Telekommunikationsbereich lässt sich auch beim postalischen Informationsaustausch jegliche Kontrolle von Inhalten unterbinden, indem man verschlüsselte Informationen versendet. Zudem kann der Staat den Inhalt von Postsendungen schon des hohen Aufwandes wegen nicht in nennenswertem Maße auf einschlägige Hinweise kontrollieren.

Der Bevollmächtigte der Bundesregierung meint, die Nutzer und Anbieter elektronischer Kommunikation würden im Vergleich zu sonstigen Leistungen nicht benachteiligt, weil eine „Speicherung von **Kontenstammdaten**“ erfolge.¹⁶⁰ Demgegenüber ist bereits in der Beschwerdeschrift dargelegt worden, weshalb der Abruf von Kontostammdaten nicht mit der Vorratsdatenspeicherung vergleichbar ist.¹⁶¹ Mit dem Abruf von Kontenstammdaten vergleichbar wäre allenfalls eine Befugnis zur Anfrage bei Kommunikationsanbietern, welche Anschlüsse eine Person bei ihnen unterhält. Eine solche Befugnis steht hier nicht in Rede.

Nach Auffassung des Bevollmächtigten der Bundesregierung würde der in der Beschwerdeschrift angelegte **Gleichheitsmaßstab** „im Ergebnis jede gesetzliche Typisierung und damit jegliche demokratische Gesetzgebung weitgehend verfassungsrechtlich ausschließen.“¹⁶² Dies ist unrichtig. Unter Art. 3 GG darf der Gesetzgeber weiterhin typisieren und Vergleichbares ungleich behandeln, solange dies gerechtfertigt ist. Allein im Fall der Vorratsdatenspeicherung fehlt es an einer Rechtfertigung dafür, gerade die elektronische Kommunikation der gesamten Bevölkerung ohne Anlass zu erfassen, obwohl die Kommunikation, Mediennutzung und das Bewegungsverhalten traditionell frei und anonym möglich sind.

Zu dem systematischen Missbrauch von Verbindungs- und Standortdaten durch die **Deutsche Telekom AG** führt der Bevollmächtigte der Bundesregierung aus, § 113a TKG erleichtere einen Missbrauch von Verkehrsdaten nicht, weil technisch versierte Mitarbeiter Verkehrsdaten ohnehin im Einzelfall aufzeichnen könnten.¹⁶³ In Wahrheit setzt § 113a TKG eine große Menge an sensibelsten Informationen Offenlegungs- und Missbrauchsrisiken aus, die andernfalls nur unter großem Aufwand, nur von wenigen besonders versierten Personen und nur in einzelnen Fällen missbräuchlich aufgezeichnet werden könnten.

¹⁵⁸ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 81.

¹⁵⁹ Beschwerdeschrift vom 31.12.2007, 132 f.

¹⁶⁰ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 81.

¹⁶¹ Beschwerdeschrift vom 31.12.2007, 76.

¹⁶² Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 82.

¹⁶³ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 88.

Der Bevollmächtigte der Bundesregierung behauptet, **im Jahr 2003** hätten sich mehr Verkehrsdaten bei den Unternehmen befunden als im Jahr 2007, weil seither die Nutzung von Pauschaltarifen zugenommen habe.¹⁶⁴ Demgegenüber ist bereits in den vergangenen Schriftsätzen nachgewiesen worden, dass die Menge der gespeicherten Verkehrsdaten und auch die Zahl der staatlichen Zugriffe hierauf von Jahr zu Jahr rapide zugenommen hat.¹⁶⁵

Vier einfache Abschriften anbei.

Meinhard Starostik
Rechtsanwalt

¹⁶⁴ Bevollmächtigter der Bundesregierung, Schriftsatz vom 28.11.2008, 95.

¹⁶⁵ Beschwerdeschrift vom 31.12.2007, 35 ff.; Schriftsatz vom 17.03.2008, 9 ff.; Schriftsatz vom 13.08.2008, 24.

Fälle von Datenmissbrauch und -irrtümern

Falscher Verdacht

Deutschland

- Die Harburger Polizei suchte 2003 mit einem falschen Fahndungsfoto nach einem Sparbuchdieb. Geliefert hatte das Bild eine Videüberwachungskamera – und der Student Marco Koch kam unschuldig in Haft. [21] [Quelle](#)
- Ein 67-jähriger Wiesbadener geriet unter Verdacht, sich Kinderpornografie beschafft zu haben, weil von seinem Bankkonto entsprechende Abbuchungen vorgenommen wurden. Tatsächlich hatten aber Unbekannte seine Kreditkartendaten missbraucht. Am 15. Dezember 2006 standen zwei Kriminalbeamte in seinem Büro in Wiesbaden. Einen Durchsuchungsbeschluss hatten sie dabei, demzufolge die Computer im Büro beschlagnahmt werden sollten, außerdem sämtliche Speichermedien wie externe Festplatten und CD-ROMs. Seine private Wohnung, das Geschäft und das Auto sollten durchsucht werden. Nur weil sich der Betroffene nachhaltig beschwerte und ihm seine Bank schnell Belege faxte, brachen die Ermittler die Durchsuchung ab. [22] [Quelle](#)
- Zu Unrecht ins Visier der Kriminalpolizei ist ein 63-jähriger Mann aus Nürnberg geraten. 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 „Internetspuren“ (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. [23] [Quelle](#)
- Jemand wollte einem Geschäftsmann eins auswaschen und teilte der Polizei mit, dieser sei Terrorist und Bombenbauer. Die Kripo überwachte ihn drei Monate lang und stürmte schließlich mit einem Sondereinsatzkommando seine Wohnung und Geschäftsräume. Die behandelnden Ärzte diagnostizierten eine „Traumatisierung durch den Polizeieinsatz“. Wenig später erhängte sich der Mann. In seinem Abschiedsbrief heißt es: „Ich habe durch die Ungerechtigkeit den Glauben an das Leben verloren.“ [24] [Quelle](#)
- Bei einem Banküberfall im Jahre 1991 hatte eine automatische Überwachungskamera mehrere Lichtbilder des Täters gefertigt, die später zur Festnahme und Verurteilung eines Hausmeisters führten. Der Verurteilte verbrachte mehr als fünf Jahre im Gefängnis. Erst nach seiner Haftentlassung wurde die Tat von dem wirklichen Täter gestanden. Der unschuldig Verurteilte erhielt 24.000 Euro Haftentschädigung und vom Gerichtsgutachter ein Schmerzensgeld in Höhe von 150.000 Euro. [25] [Quelle](#), [26] [Quelle](#)
- Die Wohnung eines deutschen Professors wurde durchsucht und seine Computer beschlagnahmt, weil er Kinderpornografie über das Internet verbreitet haben soll. Tatsächlich hatte sein Internet-Zugangsanbieter der Polizei eine falsche Auskunft erteilt. [27] [Quelle](#)
- Ein Polizeibeamter notierte im Jahr 2000 Gerüchte aus seiner Nachbarschaft, wonach ein Fliesenlegermeister Handgranaten und Feuerwaffen zuhause habe. Ein SEK-Sonderkommando zerschlug die Scheibe seines Wagens und riss ihn vom Steuer. Er erlitt dauerhafte psychische Belastungen – unschuldig. [28] [Quelle](#)

Europa

- Ein in Österreich lebender Nigerianer geriet ins Visier der Behörden, weil er viele Telefonkontakte hatte – Verdacht des Drogenhandels. Es stellte sich heraus, dass er nur ein gefragter Ratgeber war. [30] [Quelle](#)
- Ein junger Navy-General und 38 weitere Personen aus England nahmen sich das Leben, nachdem sie aufgrund von Datenspuren beschuldigt und teilweise verurteilt worden waren, sich Kinderpornografie beschafft zu haben. Der junge Navy-General war vom Dienst suspendiert worden, obwohl sich die Vorwürfe gegen ihn in den Ermittlungen zuvor nicht erhärtet hatten ([31] [Quelle](#)). Im April/Mai 2007 stellte sich heraus, dass ein großer Teil der 7.000 verdächtigen Briten Opfer von Kreditkartenbetrügnern waren, darunter wohl auch mehrere der Menschen, die sich das Leben genommen hatten. Ihre Kreditkartendaten waren „gephist“ und dann benutzt worden, um bestimmte Sites zu besuchen, unter denen auch Kinderporno-Sites waren. [32] [Quelle Teil 1](#), [33] [Teil 2](#), [34] [Quelle 2](#), [35] [Quelle 3](#), [36] [Quelle 4](#), [37] [Quelle 5](#), [38] [Quelle 6](#).
- In Großbritannien wurden ein Student und ein Universitätsmitarbeiter verhaftet, nachdem sie ein extremistisches Al-Qaeda-Handbuch aus dem Internet geladen und ausgedruckt hatten. Der Student schrieb lediglich an einer Dissertation über radikale islamistische Gruppen. [39] [Quelle](#)

Welt

- Zehntausende Flugpassagiere wurden fälschlicherweise als Terrorverdächtige gelistet und sahen sich deshalb mit Einschränkungen bei ihren Reisen konfrontiert ([41] [Quelle](#)). Darunter befanden sich sogar Persönlichkeiten wie der bekannte amerikanische Senator Edward Kennedy ([42] [Quelle](#)) und Nelson Mandela ([43] [Quelle](#)).
- Ein amerikanischer Feuerwehrmann wurde festgenommen wegen versuchter Brandstiftung. Er soll versucht haben, durch Anzünden seines Hauses seine Frau und Kinder zu töten. Hauptbeweismittel war, dass er Feueranzünder derjenigen Marke gekauft hatte, die bei der versuchten Brandstiftung zum Einsatz kam. Dieser Datensatz war gespeichert, weil der Feuerwehrmann die Anzünder mit seiner Kundenkarte bezahlt hatte. Er kam erst wieder frei, als eine andere Person die Tat gestand. [44] [Quelle](#)
- Die US-amerikanische Polizei durchsuchte die Wohnung eines Unschuldigen nach Kinderpornografie. Der Betroffene berichtet, dass eine militärisch auftretende Einsatztruppe vor seiner Tür stand und ihn mit einer Waffe bedrohte. Es seien Kameras, Computer, DVDs und VHS-Kassetten mitgenommen worden. Erst später stellte sich heraus, dass der Polizei die falsche IP-Adresse gegeben worden war. [45] [Quelle](#)

Pannen

Staat

- Die Hessische Polizei stellt versehentlich ein 13 Seiten langes Einsatzprotokoll von Verkehrskontrollen ins Netz. Darin finden sich Namen, Geburtsdaten, aktuelle Adressen der Kontrollierten, „eventuelle Vorstrafen“, Automarke, Kennzeichen sowie Gesetzesverstöße. Die Daten stehen seit Februar 2006, also fast ein Jahr, im Netz und auch als das Ganze zufällig einem Rechtsanwalt auffällt, sieht sich die Polizei tagelang außerstande, die Daten aus dem Netz zu nehmen. [48] [Quelle](#) [49] [Quelle](#)
- Das britische Amt für polizeiliche Führungszeugnisse (Criminal Records Bureau) hatte bei ca. 2.700 Personen fälschlicherweise Vorstrafen notiert. Einige bekamen aufgrund dieser Fehlinformationen keine Stelle. [50] [Quelle](#)

- Der britische Datenschutzbeauftragte verzeichnete innerhalb eines Jahres 277 geleumdete Fälle von Datenverlusten, darunter 28 bei der Regierung, 75 im Gesundheitswesen und 80 in der Privatwirtschaft. Er führt an, welche Auswirkungen der Verlust oder Missbrauch von Daten in der Vergangenheit hatte: So seien falsche Kreditkartentransaktionen erfolgt, Zeugen wurden der Gefahr von Verletzung oder Einschüchterung ausgesetzt, Straftäter der Gefahr von Selbstjustiz, Adressen von Bediensteten, Polizei- und Gefängnisbeamte wurden bekannt. In einigen Fällen bestehe Lebensgefahr. Beispielsweise habe Gefängnispersonal nach Bekanntwerden der Anschrift aus Sicherheitsgründen umgelegt werden müssen. [51] [Quelle](#)
- Stalkern gelingt es trotz eingetragener Auskunftssperre im Melderegister immer wieder, die aktuelle Anschrift ihres Opfers vom Einwohnermeldeamt zu erfahren – was etwa Bert Simon aus Hannover in Lebensgefahr gebracht hat. [52] [Quelle](#)
- In der französischen Polizeidatenbank STIC, in welcher die Hälfte aller Franzosen verzeichnet ist, sind 83% der Einträge fehlerhaft. Da bei 1 Mio. Arbeitsstellen Bewerber mit der Datenbank abgeglichen werden, sieht die Datenschutzbehörde die Gefahr, dass es zu einer Vielzahl irrtümlicher Ablehnungen von Bewerbungen gekommen sein kann. [53] [Quelle](#)

Wirtschaft

- Die Auskunft der Telekom schlampfte und gab die Adresse des Frauenhauses Tübingen heraus. Daraufhin musste die ganze Einrichtung schließen, weil die Sicherheit der Frauen nicht mehr gewährleistet war ([55] [Quelle](#)).
- Eine englische Kundin der britischen Großbank HBOS bekam nicht nur ihren eigenen Kontoauszug zugeschickt, sondern gleich fünf Briefe mit insgesamt rund 2.500 Seiten, die Angaben zu den Finanzverhältnissen von 75.000 Kunden enthielten. Ein Sprecher der Bank bedauerte diesen „Einzelfall“. ([56] [Quelle](#)).
- Der für Sicherheit an US-Flughäfen zuständigen Transportation Security Administration (TSA) ist eine externe Festplatte mit 100.000 Datensätzen über Mitarbeiter abhanden gekommen. Die Datensätze enthalten unter anderem die Namen, Sozialversicherungsnummern, Geburtsdaten, Gehaltsinformationen und Bankverbindungen von Mitarbeitern. [57] [Quelle](#), [58] [Quelle](#)
- Alcatel-Lucent verliert Datenträger mit sensiblen Mitarbeiterinformationen. Auf dem Datenträger befanden sich Gehaltsinformationen, Geburtsdaten und Sozialversicherungsnummern von zahlreichen Angestellten und ehemaligen Mitarbeitern. [59] [Quelle](#)
- Ein Internetnutzer sollte einer Anwaltskanzlei 3.500 Euro zahlen, weil er 287 Audiodateien via Tauschbörse zum Download anbiete. Als er mitteilte, er habe damit nichts zu tun, glaubte man ihm nicht. Erst später stellte sich heraus, dass der Anwaltskanzlei ein Zahlendreher unterlaufen und der Betroffene tatsächlich unschuldig war. [60] [Quelle](#) In einem weiteren Fall sollte ein Internetnutzer sogar Anwaltskosten in Höhe von mehreren zehntausend Euro tragen, wenn er die Gebührenforderung nicht zahlt. Auch in diesem Fall war der Internetnutzer aber wegen eines Zahlendrehers unschuldig in Verdacht geraten, 696 Musikdateien illegal in einer Tauschbörse angeboten zu haben. [61] [Quelle](#)
- Die Ehefrau des Amerikaners Leroy Greer reichte die Scheidung ein und zog aus, nachdem sie eine Affäre ihres Mannes entdeckt hatte. Greer ließ Blumen mit einer Liebesbotschaft an eine Geliebte schicken. Das Unternehmen sicherte ihm absolute Vertraulichkeit zu. Einige Monate nach der Blumenbestellung versöhnten sich die Eheleute, die ein gemeinsames Kind hatten, wieder und zogen wieder zusammen. Greer erhielt nun jedoch einen Brief von der Blumenfirma, in dem ihm für seine Bestellung gedankt wurde. Seine Ehefrau öffnete den Brief und forderte von der Firma einen Beleg für die Lieferung an. Der Beleg wurde ihr prompt gefaxt – mitsamt Greers Liebesbotschaft an seine damalige Geliebte. Die Ehefrau zog daraufhin aus, reichte einen neuen Scheidungsantrag ein und verlangte die Zahlung eines um 300.000 US-\$ höheren Ausgleichsbetrags. Greer verklagte das Blumenunternehmen auf Zahlung von 1 Mio. US-\$ Schadensersatz. [62] [Quelle](#)

Absichtliche Handlungen

Maßnahmen des Staates

Deutschland

- Brandstiftung in Schleswig-Holstein. Alle, deren Handy sich zur Tatzeit in der Nähe des Brandorts befand, wurden von der Polizei angeschrieben. Wer nicht antwortete, müsse mit weiteren Maßnahmen rechnen, so die Polizei ([66] [Quelle 1](#), [67] [Quelle 2](#)). Die Generalstaatsanwaltschaft stoppte die Fahndung als rechtswidrig. Der Täter wurde auf andere Weise gefasst. ([68] [Quelle](#))
- Die Staatsanwaltschaft Halle erhielt über ein Fernsehmagazin Hinweise auf eine Internetseite, auf der möglicherweise kinderpornografische Inhalte angeboten wurden. Die Inhalte konnten gegen Bezahlung mit Kreditkarte heruntergeladen werden. Die Staatsanwaltschaft nahm aus „allgemeiner kriminalistischer Erfahrung“ an, dass sich auch Deutsche unter den Nutzern der Seite befinden könnten. Ohne eine richterliche Entscheidung einzuholen, „bat“ sie sämtliche Kreditkartenabrechnungsunternehmen in Deutschland, ihr entsprechende Abbuchungen zu übermitteln. In dem Schreiben der Staatsanwaltschaft hieß es: „Vorsorglich muss ich Sie darauf hinweisen, dass Sie sich selbst der Gefahr strafrechtlicher Verfolgung aussetzen, falls Sie meine Bitte unberücksichtigt lassen.“ Daraufhin durchsuchten die Unternehmen die Abrechnungsdaten aller Deutschen und übermittelten über 300 „Treffer“. Es wurden etliche Konsumenten von Kinderpornografie gefunden, einige gerieten aber auch unter einen falschen Verdacht. Die Betreiber der ausländischen Internetseite oder Hintermänner wurden nicht gefunden. ([69] [Quelle](#))
- 32.000 Personen wurden nach einer Rasterung in eine bundesweite Datei „Schläfer“ aufgenommen. Dabei gab es nicht auch nur ansatzweise konkrete Anhaltspunkte dafür, dass es sich gerade bei ihnen um so genannte Schläfer handeln könnte oder sie mit solchen in Kontakt stehen würden ([70] [Quelle](#)). Aufgrund der Rasterfahndung wurden in Hamburg 140 ausländische Studenten von der Polizei zu „Gesprächen“ vorgeladen ([70] [Quelle](#)).
- Zur Aufklärung von Straftaten werden oft Massengentests durchgeführt. Wer nicht mitmacht, muss mit Befragung und Überwachung rechnen.
- Das Bundesamt für Verfassungsschutz beobachtete 38 Jahre lang den Bürgerrechtler und Rechtsanwalt Dr. Rolf Gössner. Er ist Präsident der Internationalen Liga für Menschenrechte, Autor mehrerer Polizei- und Geheimdienst-kritischer Bücher sowie Mitherausgeber verschiedener Bürgerrechtspublikationen. Der Verfassungsschutz wirft ihm vor, „extremistische Bestrebungen von Personenzusammenschlüssen nachdrücklich [zu] unterstützen“. Näher liegen dürfte allerdings der Verdacht, dass Gössner den Verfassungsschützern misslieblich ist. Er ist unter anderem Autor des Buches „Geheime Informanten. V-Leute des Verfassungsschutzes: Kriminelle im Dienst des Staates“. Erst als Gössner auf vollständige Information über die Datensammlung des Verfassungsschutzes klagte ([71] [Quelle](#)), erklärte das Amt vor Gericht, man habe die Überwachung nun eingestellt und werde die vorhandenen Unterlagen über Gössner vernichten.
- Weibliche, unverdächtige Besucher von Fußballspielen mussten sich vor den Augen der Polizei nackt ausziehen und eine umfassende Kontrolle dulden. Dies passierte unter anderem einer 17-jährigen Schülerin ([72] [Quelle](#)). Ein Gericht urteilte später, dass die Vorgehensweise unverhältnismäßig und rechtswidrig war ([73] [Quelle](#)).
- Gegner von Gentechnik in der Landwirtschaft sind im oberbayerischen Landkreis Ebersberg ins Visier des Staatsschutzes geraten. Der Sprecher der Polizeidirektion in Erding, Christoph Huber, weist Vorwürfe zurück. Es sei darum gegangen, „die Versammlung vor möglichen Störern zu schützen“. Die Staatsregierung teilt mit, dass bei Straftaten im Zusammenhang mit Gentechnologie von Staatsschutzdelikten ausgegangen werde. [74] [Quelle](#)

- Die Hamburger Ausländerbehörde hat zur Überprüfung, ob eine Scheinehe vorliegt, ohne rechtliche Grundlage einen Privatdetektiv damit beauftragt u.a. eine verdeckte Videoüberwachung des Eingangsbereichs der angegebenen ehelichen Wohnung durchzuführen, die Handynummer des Ehegatten verdeckt bei einem Familienangehörigen zu erfragen, an dessen PKW einen GPS-Peilsender anzubringen und eine neuntätige Bewegungsüberwachung vorzunehmen. Das OVG Hamburg hat diese Maßnahmen für rechtswidrig erklärt und die unmittelbare Verwertung der Erkenntnisse sowohl im weiteren Verwaltungsverfahren als auch im gerichtlichen Verfahren verboten ([75] [Quelle](#), [76] [Quelle](#)).
- Die Staatsanwaltschaft ließ die Wohnung eines G8-Gegners durchsuchen. In dem Durchsuchungsbefehl wird dem Betroffenen vorgeworfen, an einem vor wenigen Monaten verübten Brandanschlag auf das Berliner Unternehmen Dussmann beteiligt gewesen zu sein. Das Indiz für diese Annahme: Der Beschuldigte hatte im Internet nach „Dussmann“ recherchiert. Dussmann unterhält unter dem gleichen Namen eines der größten Bücherkaufhäuser der Stadt. [77] [Quelle](#)
- Mindestens zwei V-Leute des Verfassungsschutzes haben das sozialkritische Berliner Sozialforum beschattet. Im Rahmen der Bespitzelung wurden auch Daten über Professor Peter Grottian gesammelt. [78] [Quelle](#)
- Das Bundeskriminalamt speichert, wer Informationen der Behörde über bestimmte Straftaten durchliest, z.B. über die terroristische Vereinigung „militante gruppe“. Die Behörde lässt sich dann Name und Anschrift der Internet-Nutzerinnen und Nutzer mitteilen, um weitere Ermittlungen einleiten zu können. Auf diese Weise hofft man, den Tätern auf die Spur zu kommen. [79] [Quelle](#)
- Das sächsische Landesamt für Verfassungsschutz sammelte seit 2004 Daten über angebliche organisierte Straftäter, obwohl es dafür nicht zuständig war. Es war von einem „Sachsen-Sumpf“ die Rede, in den 200 hochrangige Politiker und Juristen verwickelt sein sollten. Viele in den Akten enthaltene Namen wurden bekannt und von der Presse in den Zusammenhang mit Korruption gerückt. Heute (2008) steht fest, dass nicht einmal 10 Vorfälle strafrechtlich relevant sind. Der Jurist Norbert Röger klagt, er sei durch die Aktensammlung des Verfassungsschutzes Opfer eines „beispiellosen Rufmordes“ geworden. [80] [Quelle](#)
- Ein 27-jähriger arbeitsloser Bankkaufmann wurde beschuldigt, 2003 einen Brand gelegt zu haben. Die Ermittler in Landau (Pfalz) hörten Telefonate des Beschuldigten mit seiner Verteidigerin ab, obwohl das verboten ist. Von dem Vorwurf der Brandstiftung wurde der Betroffene später freigesprochen. [81] [Quelle 1](#), [82] [Quelle 2](#)
- 2005-2008 hat der Bundesnachrichtendienst 2.000 E-Mails einer von der deutschen Entwicklungshilfeorganisation Welthungerhilfe geleiteten Hilfsorganisation in Afghanistan mitgelesen. [83] [Quelle](#)
- 2006 überwachte der Bundesnachrichtendienst über Monate hinweg E-Mails des afghanischen Handelsministers Amin Farhang (68), unter anderem auch solche mit der Spiegel-Journalistin Susanne Koelbl. Das Passwort zu dem E-Mail-Konto des Ministers bei Yahoo hatte der BND erhalten, indem er ein Spionageprogramm auf den Computer des Ministers eingespielt hatte. Mithilfe des Passworts konnte der BND direkt auf das E-Mail-Postfach zugreifen. [84] [Quelle](#)

Europa

- Die portugiesische Justiz soll 2005 die Telefonanschlüsse von mehr als 200 Politikern und Spitzenbeamten kontrolliert haben, darunter war auch der Apparat des Staatschefs Jorge Sampaio. Abgehört wurde auch das Telefon des früheren sozialistischen Ministerpräsidenten Antonio Guterres, genauso wie die Nummern von hohen Richtern und des portugiesischen Generalstaatsanwaltes. [86] [Quelle](#)
- Der slowenische Nachrichtendienst Sova soll 2004 Telefongespräche abgehört haben, die der kroatische Ministerpräsident Ivo Sanader mit dem damaligen konservativen Oppositionsführer und nunmehrigen slowenischen Ministerpräsidenten Janez Janša geführt hat. Unter Berufung auf nicht genannte Quellen des Nachrichtendienstes berichtete die slowenische Tageszeitung ‚Dnevnik‘, dass zahlreiche dieser Gespräche aufgezeichnet worden seien. [87] [Quelle](#)
- Der italienische Militärgesheimdienst SISMI sammelte 2001 bis 2006 nicht nur Daten über Journalisten und Politiker, sondern auch über kritische Richter und Staatsanwälte. Laut dem Obersten Richterrat (CSM) hat der SISMI intensiv von 2001 bis 2003 sowie teilweise bis 2006 vier Staatsanwaltschaften (Mailand, Turin, Rom, Palermo) sowie 203 Richter aus 12 Ländern, davon 47 Italiener, bespitzelt. Funktionäre des Militärgesheimdienstes hätten darüber hinaus mit Einschüchterungsaktionen Richter bedroht und ihre Glaubwürdigkeit in der Öffentlichkeit in Frage gestellt. Auch der Mailänder Staatsanwalt Armando Spataro wurde überwacht. Er ermittelte wegen der Verschleppung des Islamistenpredigers Hassan Mustafa Osama Nasr alias „Abu Omar“ gegen die Geheimdienstmitarbeiter Nicolò Pollari und Pio Pompa, die seine Überwachung durchführten. [88] [Quelle 1](#), [89] [Quelle 2](#), [90] [Quelle 3](#)
- In Großbritannien hörten die Behörden hunderte von Gesprächen zwischen Strafverteidigern und Gefängnisinsassen ab. Auch Gespräche zwischen einem Abgeordneten und einem Gefangenen wurden abgehört. Außerdem wurden die Taschen von Gefängnisbesuchern heimlich durchsucht, ihre Handys ausgewertet und ihre Dokumente kopiert. Nun wird befürchtet, dass Straftäter wegen der illegalen Praktiken freigesprochen werden müssen. [91] [Quelle 1](#), [92] [Quelle 2](#)

Welt

- Das US-amerikanische FBI führt über 700.000 Menschen als Terrorverdächtige; jeden Monat kommen weitere 20.000 Personen hinzu. Diese Personen haben bei der Einreise, bei Anträgen, bei Banken usw. mit größten Schwierigkeiten zu kämpfen. ([43] [Quelle](#))
- [94] [Totalüberwachung von Autofahrern in den Vereinigten Arabischen Emiraten](#): Der Golfstaat hat IBM mit dem Aufbau eines landesweiten Verkehrsleit- und Sicherheitssystems beauftragt. In jedes Fahrzeug wird künftig eine personalisierbare Black-Box eingebaut, die Standort und Geschwindigkeit an Regierungsbehörden übermittelt.
- Das amerikanische FBI hat ohne gerichtliche Genehmigung und illegal jahrelang Konto-, Telefon- und Kreditkartendaten von Bürgern erhoben. Binnen drei Jahren nach Erlass eines entsprechenden Gesetzes gab es 143 000 „Anti-Terror-Anfragen“, sie betrafen 52 000 Menschen. Nicht immer lag Terrorverdacht vor; nur selten führten sie auf eine heiße Spur. Eine Stichprobe ergab in rund einem Fünftel der Fälle Rechtsverstöße. [95] [Quelle](#)
- Die Sozialversicherungsnummern von rund 30.000 US-Bürgern, die beim Agriculture Department registriert sind, waren jahrelang über eine öffentliche Datenbank zugänglich. Die Social Security Number gilt in den USA als eine Art allgemeines Personenkennzeichen. Um Identitätsdiebstahl vorzubeugen, müsste sie eigentlich vertraulich behandelt werden. Vertreter des Agriculture Department wussten bis vor kurzem nicht von der ungewollten Veröffentlichung, bis eine Farmerin aus Illinois zufällig bei einer Google-Suche ihre eigenen Daten fand. Die Datenbank wird seit 26 Jahren gepflegt und von zahlreichen Behörden, Forschungsinstituten oder auch Journalisten eingesetzt. Angeblich existieren tausende Kopien der Datenbank. Nach Analysen des Agriculture Department müssen nun 105.000 bis sogar 150.000 Personen befürchten, dass Betrüger unter ihrem Namen und mit ihrer Social Security Number Konten eröffnen, Kreditkarten ausstellen lassen oder im Internet einkaufen. [96] [Quelle](#)
- Von 1956 bis 1971 ging das amerikanische FBI gegen angeblich „politisch radikale“ Gruppen vor. Meistens wurden die Gruppen infiltriert und ihre Mitglieder bespitzelt. Auch der Bürgerrechtler Martin Luther King wurde bespitzelt und belästigt. Senator Frank Church, der die Vorgänge später untersuchte, erklärte: „Das FBI führte eine ausgeklügelte, verdeckte Operation durch, die verhindern sollte, dass von den Grundrechten der Meinungs- und Versammlungsfreiheit Gebrauch gemacht wird.“ [97] [Quelle](#)
- Das amerikanische Verteidigungsministerium und das FBI [98] [beobachten](#) und infiltrieren friedliche Bürgerrechts-, Umwelt-, Friedens- und Glaubensgruppen (darunter ACLU, Greenpeace und 28 weitere Gruppen und Aktivisten). [99]

Quelle 2

- Mit dem weltweiten Telekommunikations-Überwachungssystem Echelon hören die USA, Australien und Großbritannien Telefone ab. Im Vorfeld des Irakkrieges wurden z.B. Telefonate der übrigen Mitglieder des Weltsicherheitsrates abgehört. Aber auch den UNO-Generalsekretär hörten sie ebenso ab wie den UNO-Waffeninspekteur Hans Blix, dessen Vorgänger Robert Butler und die damalige UNO-Menschenrechtsbeauftragte Mary Robinson. Die britische Geheimdienst-Mitarbeiterin, die die Abhöraffaire enthüllte, wurde inhaftiert. [100] [Quelle](#), [101] [Quelle](#), [102] [Quelle](#).
- An Kanadas Grenzen werden alle Personen zurückgewiesen, die in ihrem Leben einmal verurteilt worden sind, auch wegen leichter Vergehen. Betroffen waren beispielsweise ein Mann, der sieben Jahre zuvor wegen Trunkenheit am Steuer verurteilt worden ist, ein Mann, der eine Sondererlaubnis zum Konsum von Marihuana aus medizinischen Gründen hat, ein Mann, der 1975 wegen Besitz von Marihuana verurteilt wurde, ein Mann, der als Student etwas aus dem benachbarten Supermarkt mitgehen ließ – und zwar vor 20 Jahren. Hintergrund ist ein Abkommen zwischen Kanada und den USA, demzufolge jedes Land auf die Polizeidatenbanken des anderen Zugriff erhält. Ähnliche Abkommen mit Europa sind geplant. [103] [Quelle](#)
- Das US-Justizministerium hat festgestellt, dass das FBI die generell schon weitgehenden Regeln im US-Antiterrorpaket Patriot Act zur Durchleuchtung von Bürgern in zahlreichen Fällen verletzt oder eigenmächtig ausgedehnt hat. Insbesondere US-Bürger wurden in deutlich stärkerem Maße ausgespäht, als es der gesetzliche Rahmen eigentlich zulassen würde. [104] [Quelle](#) [105] [Quelle](#)
- Der deutsche Staatsbürger und gebürtige Syrer Majed Shehadeh, wird am 28.12.2006 bei der Einreise in die USA zwei Tage lang ohne Angabe von Gründen festgehalten und verhoert. Während dieser Zeit wurde ihm die Einnahme lebenswichtiger Herzmedikamente verweigert. Anschliessend wurde ihm die Einreise verweigert – Shehadeh wurde ausgewiesen, obwohl seine Frau Amerikanerin ist und er seit knapp 30 Jahren ein Haus in den USA besitzt. Weder die Einwanderungsbehörde noch das FBI nahmen bislang zu dem Fall Stellung. [106] [Quelle 1](#), [107] [Quelle 2](#)
 - Ausführlicher Video-Beitrag: [108] [Urlaub in der Einzelzelle – wie US-Behörden deutsche Touristen schikanieren \(22.02.2007\)](#). Die USA wollen sich mit verschärften Sicherheitsmaßnahmen vor Terroristen schützen. Doch die Folge sind häufig voreilige Verdächtigungen und Gefängnisaufenthalte völlig harmloser USA-Besucher.

Maßnahmen der Wirtschaft

Deutschland

- Tauschbörsennutzer bekamen im Dezember 2006 Abmahnungen: Sie hätten rechtswidrig eine Software heruntergeladen und müssten deswegen Schadenersatz und Gebühren zahlen. Einige der Betroffenen zahlten. Später stellte sich heraus, dass die Software kostenfrei weitergegeben werden durfte (Freeware); die Anwaltskanzlei zog ihre Abmahnungen zurück. Die Ermittlung der Betroffenen war nur dadurch möglich, dass deren Internet-Zugangsanbieter die zugewiesenen Kennungen auf Vorrat speicherten. [111] [Quelle](#)
- Die Deutsche Telekom AG wertete 2005 und 2006 über einen Zeitraum von insgesamt anderthalb Jahren missbräuchlich die Telefonverbindungsdaten von Journalisten sowie von Arbeitnehmer-Aufsichtsräten, Managern und [112] [Betriebsräten](#) des Unternehmens aus, um undichte Stellen im Unternehmen zu ermitteln. Die Auswertung der Festnetz- und Mobilfunk-Verbindungsdatensätze der wichtigsten über die Telekom berichtenden deutschen Journalisten und deren privaten Kontaktpersonen war beabsichtigt. [113] [Quelle](#) Ausgewertet wurden nicht weniger als 250.000 Telefonverbindungen ([114] [Quelle](#)). Anhand von Handy-Standortdaten wurden auch die Bewegungen der Betroffenen nachverfolgt ([115] [Quelle](#)). Überwacht wurden auch Personen, die mit der Telekom kaum oder garnicht zu tun hatten ([116] [Quelle](#)). Es besteht der Verdacht, dass Daten auch missbraucht wurden, um Vorteile in Arbeitskämpfen zu erzielen ([117] [Video-Bericht](#)).
- 1997 soll sich die Deutsche Telekom AG in Telefonleitungen eingeschaltet haben, um gegen vermeintliche „Hacker“ zu ermitteln. Später stellte sich heraus, dass der vermeintliche Hacker ein Mitarbeiter von T-Mobile war, der auftragsgemäß Arbeiten durchgeführt hatte. [118] [Quelle](#)
- eBay erteilte dem Zoll Auskunft über 3.000 Käufer von Kaffee in den Niederlanden. Der Zoll leitete gegen alle ein Strafverfahren ein: Sie hätten es versäumt, 2,19 Euro Kaffesteuer pro Kilogramm Röstkaffee zu zahlen ([119] [Quelle](#)). Wenn Ebay die Daten gelöscht oder gesperrt hätte, wozu es verpflichtet war, wäre es nicht zu den Strafverfahren gekommen.

Welt

- Der New Yorker Generalstaatsanwalt erhebt im März 2006 Anklage gegen Gratis Internet. Die Firma hatte über Webseiten wie [121] [FreePods.com](#), [122] [FreeCDs.com](#), [123] [FreeDVDs.com](#) und [124] [FreeVideoGames.com](#) die Adressdaten von Nutzern gesammelt. Diese hatten persönliche Daten angegeben, in der Hoffnung auf Gewinne von Test- oder Gratisprodukten. Entgegen einer eindeutigen Zusage, die Daten der Nutzer vertraulich zu behandeln, hat Gratis Internet Millionen von Datensätzen an mindestens drei E-Mail-Marketingfirmen verkauft. [125] [Quelle](#), [126] [Quelle](#)
- Die Forschungsabteilung von AOL in den USA hat im Sommer 2006 zu Forschungszwecken die Suchanfragen von 658.000 AOL-Mitgliedern auf einem frei zugänglichen Wiki veröffentlicht. Die Daten waren anonymisiert, aber in den Datensätzen befanden sich Informationen, die Rückschlüsse auf die Nutzer zuließen, etwa Namen und Adressen von Freunden oder Kollegen. In der Folge mussten einige AOL-Mitarbeiter gehen und Kunden erhoben eine Sammelklage auf Schadenersatz gegen AOL. Der Konzern hat sich bereits entschuldigt, aber sammelt derartige Daten weiter. [127] [Quelle](#)
- Der amerikanische Computerhersteller Hewlett-Packard ließ eigene Aufsichtsratsmitglieder, neun Journalisten und andere Personen von einem Privatdetektivunternehmen bespitzeln. Die Detektive erhielten durch Vortäuschung falscher Identität von Telefongesellschaften die Verbindungsdaten der Zielpersonen und konnte auf diese Weise ermitteln, mit wem sie telefoniert hatten. [128] [Quelle](#)
- Die Telekom Austria soll Kunden anderer Internet Service Provider benutzt haben, um diese mit cold calls zu einem Anbieterwechsel zur Telekom Austria zu bewegen. Ein solches Vorgehen verstößt gegen österreichisches Datenschutz- und Wettbewerbsrecht. [129] [Quelle](#)
- Vodafone Ungarn hat 2005 alle 15 Minuten den Standort aller ihrer Mitarbeiter anhand ihrer Handy-Daten aufgezeichnet und in eine Datenbank eingestellt. Erst nach Einschaltung der Gerichte musste sich Vodafone entschuldigen und die Daten löschen. [130] [Quelle](#)

Missbrauch durch Einzelpersonen

Deutschland

- Deutscher Polizeidirektor soll polizeiliche Informationssysteme benutzt haben, um Infos über Leute abzufragen, die eine Wohnung von ihm mieten wollten ([133] [Quelle](#)). Das Verfahren ist eingestellt worden ([134] [Quelle](#)).
- Lufthansamitarbeiterin gibt Daten über Bonusmeilen von Abgeordneten an die Presse heraus und löst Rücktritte aus. [135] [Quelle](#)
- Der bayerische Datenschutzbeauftragte hat 2005 stichprobenweise 53 Abfragen von Polizeibeamte im polizeilichen

Informationssystem überprüft. Bei 15 dieser Anfragen konnte eine dienstliche Notwendigkeit nicht festgestellt werden; 3 Abfragen waren sogar eindeutig dem privaten bzw. sozialen Umfeld der abfragenden Polizeibediensteten zuzurechnen. Hochgerechnet bedeutet dies, dass mindestens 5% der Datenabfragen von Polizeibeamten missbräuchlich erfolgen.

[136] [Quelle](#)

- Ein Mitarbeiter der GEZ, der gleichzeitig bei einer Autoversicherung tätig war, hatte Zugriff auf die Daten von Kunden, welche er offensichtlich dazu benutzte, um nicht angemeldete Autoradios auffindig zu machen. [137] [Quelle](#)
- Mitarbeiter des Bundeskriminalamts verkauften 2002 und 2003 geheime Informationen und Daten an die Presse. Die Verantwortlichen konnten noch immer nicht identifiziert werden. [138] [Quelle](#)
- Mitarbeiter des Pergamon-Museums benutzen für die Dauer eines Jahres eine Überwachungskamera, um das Wohnzimmer von Bundeskanzlerin Angela Merkel zu beobachten ([139] [Quelle](#)).
- Der Betreiber eines Kinderbordells in Dresden filmte Prominente heimlich bei dem Besuch seines Etablissements. Zu den Besuchern sollen Politiker, Richter und Staatsanwälte gehört haben. Der Bordellbetreiber behauptet, ihm sei eine geringere Strafe angeboten worden, wenn er keine Namen von Besuchern nennt. Zu den Videoaufnahmen sagt er: „Die sind meine Lebensversicherung.“ [140] [Quelle](#)
- Ein 47-jähriger Polizist aus Berlin wird verdächtigt, mit Menschenschleusern gemeinsame Sache gemacht zu haben. Der Oberkommissar soll Daten aus dem polizeilichen Computersystem Poliks weitergegeben haben. Das betraf vor allem Termine für Razzien, die der Mann verraten haben soll. [141] [Quelle](#)
- Ein in Berlin tätiger Mitarbeiter des Bundesnachrichtendienstes, der mit der Überwachung elektronischer Kommunikation betraut war, soll seine technischen Möglichkeiten auch privat genutzt haben. Er soll während seines Dienstes den Email-Verkehr eines Deutschen ausgespäht haben, weil dieser ein Verhältnis mit seiner Frau hatte. Die Staatsanwaltschaft ermittelt. [142] [Quelle](#)
- Ein Mannheimer Polizeibeamter hat rechtswidrig den Mitschnitt eines Notrufs weitergegeben. Inzwischen ist der Mitschnitt im Internet veröffentlicht und dort über 400.000mal abgerufen worden, einschließlich Namen und Anschrift der Anruferin. Die 42-jährige Anruferin ist wegen ihres Dialekts und der Mutmaßung des Polizeibeamten, sie habe ihr Gebiss nicht im Mund, zum Gespött der Öffentlichkeit geworden. [143] [Quelle](#) Das Verfahren gegen den Polizeibeamten wurde eingestellt. Inzwischen ist auch ein Anruf bei der Polizei in Hamm im Internet veröffentlicht worden, um sich über die Anruferin lustig zu machen. [143] [Quelle](#)
- Ein Polizist aus Koblenz hat den Polizeicomputer genutzt, um Informationen über den neuen Partner seiner Frau auszukundschaften (Quelle: OLG Koblenz, Az. 1 Ss 13/08 und Ostfriesischer Kurier vom 18.07.08).
- Für nur 850 Euro wurden der Verbraucherzentrale 6 Millionen Datensätze deutscher Bundesbürger mit Kundendetails wie Adresse, Geburtsdatum und auch Kontonummern und Bankverbindungen verkauft. Solche Daten werden beispielsweise von Call-Centern dazu benutzt, fingierte Kontoabbuchungen zu veranlassen. [144] [Quelle](#)
- Im Jahr 2006 verkaufte ein Mitarbeiter von T-Mobile die Daten der 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 liegen dem Spiegel vor und werden in kriminellen Kreisen auch anderen Personen angeboten. In den Daten finden sich nicht nur viele Prominente aus Kultur und Gesellschaft wie Hape Kerkeling, Günther Jauch und Til Schweiger, 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 Bedrohung ihrer Sicherheit darstellt (etwa Charlotte Knobloch, Präsidentin des Zentralrats der Juden). Das Bundeskriminalamt erstellt eine Gefährdungsanalyse, um Betroffene schützen zu können. [145] [Quelle](#) Zur Aufklärung des Datenlecks verletzte T-Mobile erneut das Fernmeldegeheimnis und überprüfte illegal Verbindungsdaten. [145] [Quelle](#)
- Im Jahr 2007 überwachte der Bundesnachrichtendienst Computer von Personen im Kongo mithilfe von Spionageprogrammen. Ein Mitarbeiter des Bundesnachrichtendienstes missbrauchte die Überwachung, um romantische Post seiner Partnerin an einen Bundeswehrangehörigen im Kongo abzufangen. Die intimen Mails machten die Runde im Bundesnachrichtendienst. [84] [Quelle](#)
- 2007 soll eine stellvertretende Leiterin in der Abteilung Verkehrsüberwachung der Kreisverwaltung München den Standort wertvoller Motorräder am Dienstcomputer abgefragt und ihrem Ehemann mitgeteilt haben. Dieser stahl die Motorräder und verkaufte sie nach Bosnien. [146] [Quelle](#)

Europa

- Polizisten sollen von einer norwegischen Boulevardzeitung erfolgreich bestochen worden sein, um an pikante Details aus Prinzessin Mette-Marits wildem Leben vor ihrer Ehe mit Kronprinz Haakon zu kommen. Mit viel Geld sei auch bei Recherchen über Freunde, Bekannte und frühere Liebhaber der jungen Frau verfahren worden. Selbst Kontoauszüge des Kronprinzenpaares druckte die Zeitung ab. Das Boulevard-Magazin verfügte offenkundig über ein breites Netzwerk von Informanten bei der Polizei und bei Banken. ([148] [Quelle](#))
- In Griechenland wurden zwischen Juli 2004 und März 2005 Telefonate hochrangiger Personen abgehört, und zwar von Unbekannten. Abgehört wurden die Telefone von Ministerpräsident Kostas Karamanlis, mehrere seiner Minister – darunter der Außen- und der Verteidigungsminister –, hohen Militärs, führenden Politikern der oppositionellen Sozialisten, Journalisten, sowie ausländischen, vorwiegend aus arabischen Ländern stammenden Geschäftsleuten. Handys von insgesamt 100 Personen wurden abgehört. Die Regierung vermutet Spionage im Auftrag des Auslands, möglicherweise der USA. [149] [Quelle](#), [150] [Quelle](#)
- In Großbritannien wurde 2006 das Telefon von Thronfolger Prinz Charles überwacht, und zwar für die Sensationspresse. Ein Reporter sagte, das Abhören von Telefonen für die Presse sei bei Prominenten nicht ungewöhnlich. [151] [Quelle](#)
- In der Slowakei hat 2003 der Geheimdienst SIS systematisch Journalisten bespitzelt. Ein anonymen Informant „aus Sicherheitskreisen“ sagte, das illegale Abhören von Journalisten sei alltägliche Praxis des Geheimdienstes. Sogar die Ermittler selbst sollen während ihrer Untersuchungen abgehört und damit massiv unter Druck gesetzt worden sein: So wurden beispielsweise Gespräche, die Ermittler im privaten Familienkreis geführt hatten, auf die Anrufbeantworter ihrer Verwandten und Bekannten gespielt, um ihnen zu zeigen, dass sie nie unbeobachtet sein können. [152] [Quelle](#)
- In Italien ließ der Sicherheitschef der Telekom von 1997 bis 2006 die Telefonate von mehr als hunderttausend Bürgern abhören, darunter einfache Angestellte, aber auch Großbankiers, Politiker, Unternehmer, Intellektuelle, Sportler, Schiedsrichter, Show-Größen. Dies war ihm möglich, weil er für die Durchführung von (legalen) Telefonüberwachungen zuständig war. Er schleuste gefälschte, gerichtliche Überwachungsanordnungen ein. Neben den Telefondaten gelangte der Spionagering auch an Email-Korrespondenzen, Bankverbindungen und andere Daten. Diese Informationen wurden gegen Bezahlung von etlichen Polizisten und Finanzpolizisten geliefert – elf sind verhaftet worden. Diese Beamten drangen in Dateien der Steuerbehörden und des Innenministeriums ein, um die illegalen Dossiers noch anzureichern. Mit den gewonnenen Informationen wurden Skandale im den Medien produziert oder Menschen erpresst. Der Sicherheitschef verdiente 20 Mio. Euro an den Informationen. [153] [Quelle](#), [154] [Quelle](#)
- In Italien wurden von Herbst 2005 bis Sommer 2006 die Steuerdaten zahlreicher Prominenter illegal abgefragt, unter anderem von Premierminister Prodi und Oppositionsführer Berlusconi. Auch etwa Fußballstars wie Francesco Totti und Alessandro del Piero sind betroffen. Begünstigt wurde die Spionage durch die Tatsache, dass es in Italien eine zentrale Steuerdatei gibt, in der sämtliche steuerrelevante Daten über 40 Mio. Italiener gespeichert sind (z.B. über Einkommen, Grundbesitz, Firmenbeteiligungen). [155] [Quelle](#)
- Die britische Premierministerin Margaret Thatcher ließ einen Minister aus ihrer Regierung vom kanadischen Geheimdienst überwachen. [156] [Quelle](#)
- Ein irischer Beamte nutzte seinen Dienstcomputer, um für seinen kriminellen Bruder Einkommensdaten von potenziellen

Opfern herauszusuchen. Der Bruder nutzte die Daten für einen Einbruchsdiebstahl und um drei Geschäftsleute zu erpressen. Gegenüber der Polizei erklärte der inzwischen entlassene Sozialamtsmitarbeiter, es sei „üblich“, dass Mitarbeiter finanzielle Informationen über Freunde, Familienmitglieder, Arbeitskollegen und Bekannte abrufen. [157] [Quelle](#)

Welt

- AOL-Mitarbeiter verkauft für 28.000 US-Dollar eine Liste mit 92 Millionen Namen von amerikanischen AOL-Nutzern einschließlich E-Mail-Adresse und teilweise weiteren persönlichen Daten wie Telefonnummer, Wohnort oder Kreditkartendaten an einen Spammer. [159] [Quelle](#)
- 2005 verschaffte sich ein Cracker Zugang zu sensiblen Daten von 40 Mio. Kreditkartenkunden. Daraufhin tauchten auf den Abrechnungen einiger Kunden Belastungen auf, die nicht von ihnen stammten. [160] [Quelle](#), [161] [Quelle](#)
- Datendiebstahl ist ein großes Problem. Der amerikanischen Handelskommission zufolge erlitten allein im Jahr 2002 10 Mio. Amerikaner oder 5% der erwachsenen Bevölkerung Nachteile infolge von Datendiebstahl. Datendiebstahl führt für die Betroffenen zu finanziellen Verlusten, zu Kreditkündigungen, dem Verlust von Arbeitsplätzen, in manchen Fällen sogar zur Festnahme Unschuldiger, deren Daten von Kriminellen benutzt worden waren. In den meisten Fällen dauert es lange, die Folgen eines Datendiebstahls zu beseitigen. [162] [Quelle](#)
 - ChoicePoint, einer der größten Datenhändler der Welt, gab zwischen 2001 und 2005 sensible Daten über 163.000 Menschen an Kriminelle heraus. Dies führte in mindestens 800 Fällen zum Missbrauch der Daten. Das Unternehmen musste als Strafe 15 Mio. US-\$ zahlen, davon mindestens 5 Mio. US-\$ an die betroffenen Verbraucher. [163] [Quelle](#)
 - Der Bank of America kamen 2005 Kontodaten von 1,2 Mio. Bundesbediensteten abhandeln. [162] [Quelle](#)
 - Der Datenhändler Lexis-Nexis verlor 32.000 Datensätze über Amerikaner an Hacker. [162] [Quelle](#)
 - Jeden Monat gelangen 6 Millionen persönliche Daten (Sozialversicherungs- oder Kreditkartennummern, medizinische Daten, Adressen etc.), die rechtmäßig gesammelt wurden, in den USA in die falschen Hände, ergab die Auswertung eines amerikanischen Professors. Grundlage für die Schätzung sind Berichte in großen Medien über Vorfälle, bei denen der Datenschutz zwischen 1980 und 2006 verletzt wurde. Dabei kam er auf 1,9 Milliarden Datensätze oder neun Datensätze pro erwachsenem Amerikaner. Von den 550 bestätigten Vorfällen gingen 31 Prozent auf Cracker, 60 Prozent aber seien auf Nachlässigkeiten der Unternehmen oder Organisationen zurückzuführen, beispielsweise auf Hardware, die gestohlen oder verloren wurde. Jetzt würden vor allem aus Nachlässigkeit der Unternehmen, nicht aufgrund von kriminellen oder anderen Hackern, monatlich 6 Millionen persönliche Daten kompromittiert werden. [164] [Quelle](#)
- 1999 bezahlte der Stalker Liam Youens einer Detektei 150 US-\$ für die Information, wo Amy Boyer arbeitete. Er war lange von ihr besessen gewesen und hatte auf einer Internetseite beschrieben, wie er sie „vernichten“ wollte. Mithilfe der Daten gelang es Youens, sich vor dem Bürogebäude seines Opfers zu verstecken und sie zu erschießen. [97] [Quelle](#)
- Bei dem US-amerikanischen Forensik-Unternehmen Guidance wurde im Dezember 2005 ein Server geknackt und Namen, Adressen und Kreditkartendaten von rund 3800 Kunden kopiert. Der anschließende Mißbrauch der Kundendaten zu Betrugszwecken war nur möglich, weil Guidance verbotenerweise auch die Prüfnummern der Karten gespeichert hatte. Die Firma wurde von der U.S. Federal Trade Commission (FTC) zu schärferen Sicherheitsmaßnahmen verdonnert und muss der FTC über einen Zeitraum von 10 Jahren regelmäßig Bericht über Fortschritte erstatten. [165] [Quelle](#)
- Die Leiterin eines Escort-Dienstes in der US-amerikanischen Hauptstadt Washington DC drohte 2007, eine Liste mit allen Telefon-Verbindungsdaten zu ihrer Geschäftsnummer in den Jahren 2002-2006 meistbietend zu verkaufen ([166] [Quelle](#)). Auf den Listen befanden sich 10.000-15.000 Rufnummern von Kunden ([167] [Quelle](#)). Die Verbindungsdaten von vier Jahren gab sie schließlich an den Fernsehsender ABC News weiter ([168] [Quelle](#)). Der stellvertretende Außenminister der USA, der sich in seinem Amt für Abstinenz und gegen den Einsatz von Verhütungsmitteln einsetzte, trat zurück, nachdem bekannt wurde, dass er ein Kunde des Escort-Dienstes war ([167] [Quelle 1](#), [167] [Quelle 2](#)). Ein verheirateter konservativer Senator, der sich für moralisches Sexualverhalten und gegen gleichgeschlechtliche Lebensgemeinschaften aussprach, musste sich für die Inanspruchnahme des Escort-Dienstes entschuldigen ([169] [Quelle 1](#), [170] [Quelle 2](#)). Auf den Listen befanden sich auch prominente Vorstandsvorsitzende, Mitarbeiter der Weltbank und des IMF und eine Reihe von Lobbyisten ([168] [Quelle](#)).

Artikel ausgedruckt von Daten-Speicherung.de – minimum data, maximum privacy: <http://www.daten-speicherung.de>

Adresse zum Artikel: <http://www.daten-speicherung.de/index.php/faelle-von-datenmissbrauch-und-irrtuemern/>

Adressen in diesem Beitrag:

[21] Quelle: http://www.welt.de/politik/article787147/Kaufhaeuser_machen_Anti-Terror-Datei_Konkurrenz.html

[22] Quelle:

<http://www.faz.net/s/RubCD175863466D41BB9A6A93D460B81174/Doc%7EE213402745D034DD2985EC4BEB52EEB38%7EATpl%7EEcommon%7EScontent.html>

[23] Quelle: http://www.presseportal.de/polizeipresse/p_story.htx?nr=920697

[24] Quelle: <http://www.sek-team.net/index.php?area=1&p=news&newsid=266>

[25] Quelle: http://www.olg-frankfurt.justiz.hessen.de/irj/OLG_Frankfurt_am_Main_Internet?rid=HMdJ_15/OLG_Frankfurt_am_Main_Internet/sub/0a7/0a705485-f3b4-511a-eb6d-f144e9169fcc,,11111111-2222-3333-4444-100000005003%26overview=true.htm

[26] Quelle: http://www.hr-online.de/website/rubriken/nachrichten/index.jsp?rubrik=15662&key=standard_document_33184662

[27] Quelle: <http://www.lawblog.de/index.php/archives/2008/03/11/provider-liefert-falsche-daten-ans-bka/>

[28] Quelle: http://www.wdr.de/themen/panorama/25/sek_skandal/081030.jhtml

[29] bearbeiten:

http://www.daten-speicherung.de/wiki/index.php?title=F%C3%A4lle_von_Datenmissbrauch_und_irrt%C3%BCmern&action=edit§ion=3

[30] Quelle: <http://www.heise.de/tp/deutsch/inhalt/te/13870/1.html>

[31] Quelle: <http://www.heise.de/newsticker/meldung/64537>

[32] Quelle Teil 1: <http://oraclesyndicate.twoday.net/stories/4122817/>

[33] Teil 2: <http://oraclesyndicate.twoday.net/stories/4125469/>

[34] Quelle 2: http://news.bbc.co.uk/2/hi/uk_news/6641321.stm

[35] Quelle 3: <http://www.guardian.co.uk/crime/article/0,,2059880,00.html>

[36] Quelle 4: http://www.dailymail.co.uk/pages/live/articles/news/news.html?in_article_id=453950&in_page_id=1770&in_page_id=1770&expand=true

[37] Quelle 5: <http://thescotsmen.scotsmen.com/ViewArticle.aspx?articleid=2665674>

[38] Quelle 6: <http://www.pcpro.co.uk/news/news/112514>

[39] Quelle: <http://www.timeshighereducation.co.uk/story.asp?sectioncode=26&storycode=402125&c=2>

[40] bearbeiten:
http://www.daten-speicherung.de/wiki/index.php?title=F%C3%A4lle_von_Datenmissbrauch_und_-irrt%C3%BCmern&action=edit§ion=4

[41] Quelle: <http://www.heise.de/newsticker/meldung/67083>

[42] Quelle: <http://www.sueddeutsche.de/ausland/artikel/615/37578/print.html>

[43] Quelle: <http://www.aclu.org/privacy/spying/watchlistcounter.html>

[44] Quelle: <http://yro.slashdot.org/yro/05/01/29/030223.shtml?tid=158&tid=187>

[45] Quelle: <http://www.foxnews.com/wires/2006Oct25/0,4670,PeopleShaqBotchedRaid,00.html>

[46] bearbeiten:
http://www.daten-speicherung.de/wiki/index.php?title=F%C3%A4lle_von_Datenmissbrauch_und_-irrt%C3%BCmern&action=edit§ion=5

[47] bearbeiten:
http://www.daten-speicherung.de/wiki/index.php?title=F%C3%A4lle_von_Datenmissbrauch_und_-irrt%C3%BCmern&action=edit§ion=6

[48] Quelle: <http://www.heise.de/newsticker/meldung/83767>

[49] Quelle: <http://www.welt.de/data/2007/01/16/1178944.html>

[50] Quelle: http://www.privacyconference2006.co.uk/files/discussion_ger.pdf

[51] Quelle: http://www.ico.gov.uk/upload/documents/pressreleases/2008/rsa_speech_oct08_final.pdf

[52] Quelle: <http://www.swr.de/report/-/id=233454/nid=233454/did=4124466/u9go2v/index.html>

[53] Quelle: http://www.cnil.fr/fileadmin/documents/approfondir/dossier/Controles_Sanctions/CNIL-Conclusions_des_controls_STIC.pdf

[54] bearbeiten:
http://www.daten-speicherung.de/wiki/index.php?title=F%C3%A4lle_von_Datenmissbrauch_und_-irrt%C3%BCmern&action=edit§ion=7

[55] Quelle: <http://www.heise.de/tp/r4/artikel/13/13211/1.html>

[56] Quelle: <http://www.spiegel.de/wirtschaft/0,1518,463227,00.html>

[57] Quelle: http://www.tsa.gov/press/happenings/050407_statement.shtm

[58] Quelle: <http://www.heise.de/newsticker/meldung/89456>

[59] Quelle: <http://www.heise.de/newsticker/meldung/89917>

[60] Quelle: <http://www.heise.de/newsticker/meldung/97304>

[61] Quelle: <http://www.sueddeutsche.de/computer/artikel/231/148875/>

[62] Quelle: http://www.courtvt.com/news/2007/0809/flowers_ctv.html

[63] bearbeiten:
http://www.daten-speicherung.de/wiki/index.php?title=F%C3%A4lle_von_Datenmissbrauch_und_-irrt%C3%BCmern&action=edit§ion=8

[64] bearbeiten:
http://www.daten-speicherung.de/wiki/index.php?title=F%C3%A4lle_von_Datenmissbrauch_und_-irrt%C3%BCmern&action=edit§ion=9

[65] bearbeiten:
http://www.daten-speicherung.de/wiki/index.php?title=F%C3%A4lle_von_Datenmissbrauch_und_-irrt%C3%BCmern&action=edit§ion=10

[66] Quelle 1: <http://www.kn-online.de/artikel/1688548>

[67] Quelle 2: <http://bigbrotherawards.de/2005/.comm/>

[68] Quelle: <http://www.zdf.de/ZDFde/inhalt/20/0,1872,5274324,00.html>

[69] Quelle: <http://www.lawblog.de/index.php?s=mikado&submit=Suchen>

[70] Quelle: http://www.bundesverfassungsgericht.de/entscheidungen/rs20060404_1bvr051802.html

[71] Quelle: <http://www.rolf-goessner.de/BfV-FR22-2-06.htm>

[72] Quelle: <http://www.lawblog.de/index.php/archives/2006/06/06/die-welt-nackt-zu-gast-bei-freunden>

[73] Quelle: http://www.juris.de/jportal/portal/page/home.psml/js_peid/012122;jsessionid=D2AD496D1BE496CE44EFABEFB26D95B2.jpe?id=jnachr-JUNA071203426&action=controls.Maximize

[74] Quelle: http://www.zivilcourage.ro/pdf/Gentechgegner_als_Staatsfeinde.pdf

[75] Quelle: <http://fhh.hamburg.de/stadt/Aktuell/justiz/gerichte/oberverwaltungsgericht/aktuelles/presseerklarungen/pressemeldung-2007-04-25-ovg-02.html>

[76] Quelle: <http://fhh.hamburg.de/stadt/Aktuell/justiz/gerichte/oberverwaltungsgericht/aktuelles/aktuelle-entscheidungen/entscheidungsarchiv-2007/3bs396-05-pdf.property=source.pdf>

[77] Quelle: <http://www.taz.de/dx/2007/05/15/a0059.1/text>

[78] Quelle: <http://www.spiegel.de/unispiegel/studium/0,1518,420625,00.html>

[79] Quelle: <http://www.tagesspiegel.de/politik/deutschland/BKA-Datenschutz;art122,2390884>

[80] Quelle: <http://www.sueddeutsche.de/deutschland/artikel/434/173917/>

[81] Quelle 1: <http://www.rheinpfalz.de/cgi-bin/cms2/cms.pl?cmd=showMsg&tpl=rhpMsg.html&path=/rhp/lokal&id=4396249>

[82] Quelle 2: <http://www.rheinpfalz.de/cgi-bin/cms2/cms.pl?cmd=showMsg&tpl=rhpMsg.html&path=/rhp/lokal&id=4408749>

[83] Quelle: <http://www.heise.de/newsticker/Deutsche-Entwicklungshelfer-vom-BND-ausgespaehet--/meldung/120021>

[84] Quelle: <http://wissen.spiegel.de/wissen/dokument/82/36/dokument.html?titel=Au%C3%9Fer+Kontrolle&id=56756328&top=SPIEGEL&suchbegriff=&quellen=&vl=0>

[85] bearbeiten:
http://www.daten-speicherung.de/wiki/index.php?title=F%C3%A4lle_von_Datenmissbrauch_und_-irrt%C3%BCmern&action=edit§ion=11

[86] Quelle: <http://archiv.tagesspiegel.de/archiv/19.01.2006/2298869.asp>
[87] Quelle: <http://derstandard.at/?url=?id=2927363>
[88] Quelle 1: <http://www.heise.de/tp/r4/artikel/25/25685/1.html>
[89] Quelle 2: <http://derstandard.at/?url=?id=2952445>
[90] Quelle 3: http://www.nzz.ch/nachrichten/international/schnueffelei_unter_der_regierung_berlusconi_1.522874.htm
|

[91] Quelle 1: <http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2008/02/11/nbug111.xml>
[92] Quelle 2: <http://business.timesonline.co.uk/tol/business/law/article3341761.ece>
[93] bearbeiten:
http://www.daten-speicherung.de/wiki/index.php?title=F%C3%A4lle_von_Datenmissbrauch_und_-irrt%C3%BCmern&action=edit§ion=12

[94] Totalüberwachung von Autofahrern in den Vereinigten Arabischen Emiraten: <http://www.heise.de/newsticker/meldung/58623>
[95] Quelle: http://www.fr-online.de/in_und_ausland/politik/aktuell/?em_cnt=1092540&
[96] Quelle: <http://www.heise.de/newsticker/meldung/88609>
[97] Quelle: http://www.wired.com/news/politics/privacy/0,71622-1.html?tw=wn_story_page_next1
[98] beobachten: <http://www.aclu.org/safefree/spyfiles/>
[99] Quelle 2: <http://www.commondreams.org/headlines06/0327-04.htm>
[100] Quelle: http://www.businessweek.com/magazine/content/05_32/b3946010_mz001.htm
[101] Quelle: <http://www.sueddeutsche.de/ausland/artikel/452/27425/>
[102] Quelle: http://www.wdr.de/tv/monitor/pdf/040304d_Abh%F6raff%E4re.pdf
[103] Quelle: <http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2007/02/23/NEVIUS.TMP>
[104] Quelle: <http://www.heise.de/newsticker/meldung/86526>
[105] Quelle: <http://www.usdoj.gov/oig/special/s0703b/final.pdf>
[106] Quelle 1: <http://www.spiegel.de/panorama/0,1518,457627,00.html>
[107] Quelle 2: <http://www.main-netz.de/nachrichten/politik/berichte/art4207,507814>
[108] Urlaub in der Einzelzelle – wie US-Behörden deutsche Touristen schikanieren (22.02.2007):
http://daserste.ndr.de/panorama/archiv/2007/t_cid-3710902_mid-3718350_.html
[109] bearbeiten:
http://www.daten-speicherung.de/wiki/index.php?title=F%C3%A4lle_von_Datenmissbrauch_und_-irrt%C3%BCmern&action=edit§ion=13

[110] bearbeiten:
http://www.daten-speicherung.de/wiki/index.php?title=F%C3%A4lle_von_Datenmissbrauch_und_-irrt%C3%BCmern&action=edit§ion=14

[111] Quelle: <http://www.heise.de/newsticker/meldung/83511>
[112] Betriebsräten: <http://de.reuters.com/article/deEuroRpt/idDELB42297420081111>
[113] Quelle: <http://www.spiegel.de/wirtschaft/0,1518,555162,00.html>
[114] Quelle: <http://www.spiegel.de/wirtschaft/0,1518,556398,00.html>
[115] Quelle: <http://www.handelsblatt.com/News/default.aspx?p=201197&t=ft&b=1436894>
[116] Quelle: <http://www.spiegel.de/wirtschaft/0,1518,591374,00.html>
[117] Video-Bericht:
<http://www.swr.de/report/-/id=233454/did=4196196/pv=video/gp1=4340300/nid=233454/16mqp0q/index.html>
[118] Quelle: <http://www.spiegel.de/wirtschaft/0,1518,561076,00.html>
[119] Quelle: http://www.welt.de/webwelt/article96370/Hunderte_Ebay_Nutzer_zeigen_sich_selbst_an.html
[120] bearbeiten:
http://www.daten-speicherung.de/wiki/index.php?title=F%C3%A4lle_von_Datenmissbrauch_und_-irrt%C3%BCmern&action=edit§ion=15

[121] FreeiPods.com: <http://FreeiPods.com>
[122] FreeCDs.com: <http://FreeCDs.com>
[123] FreeDVDs.com: <http://FreeDVDs.com>
[124] FreeVideoGames.com: <http://FreeVideoGames.com>
[125] Quelle: <http://www.heise.de/newsticker/meldung/71266>
[126] Quelle: http://www.consumeraffairs.com/news04/2006/03/ny_gratis.html
[127] Quelle: <http://www.heise.de/newsticker/meldung/78668>
[128] Quelle: <http://www.heise.de/newsticker/meldung/78339>
[129] Quelle: <http://www.ispa.at/www/getFile.php?id=874>
[130] Quelle: <http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559531>
[131] bearbeiten:
http://www.daten-speicherung.de/wiki/index.php?title=F%C3%A4lle_von_Datenmissbrauch_und_-irrt%C3%BCmern&action=edit§ion=16

[132] bearbeiten:
http://www.daten-speicherung.de/wiki/index.php?title=F%C3%A4lle_von_Datenmissbrauch_und_-irrt%C3%BCmern&action=edit§ion=17

[133] Quelle: <http://www.wz-newsline.de/sro.php?redid=96691>
[134] Quelle: <http://www.lawblog.de/index.php/archives/2006/05/19/nichts-gegen-zu-wehren/>
[135] Quelle: <http://de.wikipedia.org/wiki/Bonusmeilen-Aff%C3%A4re>
[136] Quelle: <http://www.datenschutz-bayern.de/tbs/tb22/k3.html>
[137] Quelle: <http://www.gez-abschaffen.de/Faelle/versicherung/gez-versicherung.htm>
[138] Quelle: <http://www.sueddeutsche.de/tt2m4/deutschland/artikel/112/109003/>
[139] Quelle: <http://www.spiegel.de/politik/deutschland/0,1518,408015,00.html>
[140] Quelle: http://www.berlinonline.de/berliner-zeitung/print/seite_3/662069.html
[141] Quelle: <http://www.berlinonline.de/berliner-zeitung/print/berlin/665273.html>
[142] Quelle: <http://www.heise.de/newsticker/meldung/95338>
[143] Quelle: <http://satundkabel.magnus.de/artikel/datenschutz-notruf-bei-youtube-bringt-polizei-in-bedraengnis.html>

[144] Quelle: http://www.vzbv.de/start/index.php?page=presse&bereichs_id=&themen_id=&mit_id=1045&ask=mit

[145] Quelle: <http://www.spiegel.de/wirtschaft/0,1518,581938,00.html>
[146] Quelle: <http://www.sueddeutsche.de/muenchen/275/454955/text/>

[147] bearbeiten:

http://www.daten-speicherung.de/wiki/index.php?title=F%C3%A4lle_von_Datenmissbrauch_und_-irrt%C3%BCmern&action=edit§ion=18

[148] Quelle:

<http://www.faz.net/s/RubCD175863466D41BB9A6A93D460B81174/Doc%7EE51BB469724104316B960CDC73B732A1C%7EATpl%7EEcommon%7EScontent.html>

[149] Quelle: http://www.handelsblatt.com/news/Default.aspx?_p=200051&_t=ft&_b=1028595

[150] Quelle:

<http://www.faz.net/s/RubDDBDABB9457A437BAA85A49C26FB23A0/Doc%7EED08AFC2191C240BD926F029D06327396%7EATpl%7EEcommon%7EScontent.html>

[151] Quelle: <http://www.abendblatt.de/daten/2006/08/10/596277.html>

[152] Quelle: http://www.kas.de/publikationen/2003/2089_dokument.html

[153] Quelle: <http://www.spiegel.de/panorama/justiz/0,1518,438499,00.html>

[154] Quelle: <http://diepresse.com/home/wirtschaft/economist/74341/index.do>

[155] Quelle: <http://www.ftdeutschland.de/politik/europa/125988.html>

[156] Quelle: <http://www.cl.cam.ac.uk/%7Erja14/Papers/SE-21.pdf>

[157] Quelle: <http://www.independent.ie/national-news/civil-servant-mole-leaked-intelligence-to-criminal-1166835.html>

[158] bearbeiten:

http://www.daten-speicherung.de/wiki/index.php?title=F%C3%A4lle_von_Datenmissbrauch_und_-irrt%C3%BCmern&action=edit§ion=19

[159] Quelle: <http://www.heise.de/newsticker/search.shtml?T=aol+spammer&button=los%21>

[160] Quelle: <http://www.sueddeutsche.de/wirtschaft/artikel/182/55127/>

[161] Quelle: <http://www.sueddeutsche.de/computer/artikel/268/55213/>

[162] Quelle: <http://www.aclu.org/privacy/consumer/15301leg20050310.html>

[163] Quelle: <http://www.wired.com/news/politics/privacy/0,71622-0.html>

[164] Quelle: <http://www.heise.de/newsticker/meldung/86982>

[165] Quelle: <http://www.heise.de/newsticker/meldung/81196>

[166] Quelle: http://www.washingtonpost.com/wp-dyn/content/article/2007/03/01/AR2007030101725_pf.html

[167] Quelle: http://www.washingtonpost.com/wp-dyn/content/article/2007/04/27/AR2007042702497_pf.html

[168] Quelle: <http://abcnews.go.com/print?id=3141213>

[169] Quelle 1: <http://www.nytimes.com/2007/07/11/us/11vitter.html>

[170] Quelle 2: <http://edition.cnn.com/2007/POLITICS/07/10/vitter.madam/index.html#cnnSTCText>

[171] Diese Seite im Wiki editieren:

http://www.daten-speicherung.de/wiki/index.php/F%C3%A4lle_von_Datenmissbrauch_und_-irrt%C3%BCmern

Quelle: Daten-Speicherung.de - minimum data, maximum privacy. Freigegeben unter der CreativeCommons-Lizenz Namensnennung 2.0 Deutschland.