Antworten auf den Fragebogen der Europäischen Kommission vom 30.09.2009 zur Vorratsdatenspeicherung

Die Europäische Kommission hat unter anderem den Arbeitskreis Vorratsdatenspeicherung gebeten, bis zum 15.11.2009 einige Fragen zur Vorratsspeicherung von Verkehrsdaten und zur möglichen Einführung eines europäischen Identifizierungszwangs für Telekommunikationsnutzer zu beantworten.

Inhaltsverzeichnis

A. Vorratsdatenspeicherung

1. Auswirkungen der Vorratsdatenspeicherung auf die Bürger

> *„2.A.1. Which has been the effect, if any, on civil liberties of the use by law enforcement authorities of data retained under the Directive? Please provide examples of these effects as well as indications of the size of their impact.*"

Die Richtlinie zur Vorratsdatenspeicherung hat **katastrophale Auswirkungen** auf die Bürger und Verbraucher.

Wegen der Kosten der Vorratsdatenspeicherung, die sich wegen der hohen Investitions- und Fixkosten bei kleinen Anbietern überproportional bemerkbar machen, sind **kommerzielle Dienste teurer geworden**, was für die Verbraucher ein Nachteil ist. Eine Quantifizierung ist uns nicht möglich.

Wegen der hohen Kosten der Vorratsdatenspeicherung, von denen in Deutschland weder die Investitions- noch die Vorhaltekosten ersetzt werden, sind kleinere Anbieter vom Markt verdrängt oder von Wettbewerbern aufgekauft worden. Für Verbraucher bedeutet dies **weniger Wettbewerb** und dadurch auch mittelbar schlechtere Leistungen.

Die Vorratsdatenspeicherung bedeutet für Verbraucher vor allem **weniger Freiheit**. Wegen der Vorratsdatenspeicherung können sie Kontakte, die absolut vertraulich bleiben müssen, schlichtweg nicht mehr über Telefon, Handy, E-Mail oder Internet abwickeln. Damit ist das Medium der Telekommunikation nur noch eingeschränkt einsetzbar.

Eine nicht repräsentative **Umfrage**, die wir nach Inkrafttreten der Vorratsdatenspeicherung in Deutschland Anfang 2008 durchgeführt haben hat ergeben:

- Ein Teil der Bürger nutzt ihr **Handy** nicht mehr, seit bei jedem Kontakt der Standort festgehalten wird.
- **Online-Foren beispielsweise für Opfer sexuellen Missbrauchs** oder für politische Bewegungen sterben aus, seit jeder Teilnehmer anhand seiner IP-Adresse sechs Monate lang identifizierbar ist.
- Viele **Journalisten** haben berichtet, dass wichtige Informanten - beispielsweise aus Polizei, Feuerwehr, Unternehmen - mit Inkrafttreten der Vorratsdatenspeicherung ihren Kontakt abgebrochen haben oder nur noch persönliche Treffen wünschen.
- **Steuerberater, Rechtsanwälte und Notare** berichten, Mandanten wünschten keine elektronische Kontaktaufnahme mehr. In vielen Fällen scheitere eine Beratung daran überhaupt. Ein Steuerberater fürchtet, dass sich seine Mandanten strafbar machen könnten, wenn sie ihn nicht mehr telefonisch um Rat bitten können, was steuerliche Angaben gegenüber staatlichen Behörden angeht. Früher sei es ihm bei kurzen telefonischen Anfragen von Mandanten gelungen, diese „auf den rechten Weg" zu bringen. Unterblieben

solche Anrufe, sei ihm dies – zum Nachteil der Allgemeinheit – nicht mehr möglich.

- **Geschäftsleute** berichten, dass Kunden nicht mehr damit einverstanden sind, Geschäftsinformationen (z.B. Pläne und Zeichnungen) per E-Mail oder Fax zu übermitteln. Dass diese nun abgeholt werden müssten, erschwere Geschäftskontakte teils und mache sie in anderen Fällen - z.B. aus Zeitmangel - unmöglich.
- **Psychotherapeuten, Drogenberater und Telefonberatungen** berichten, dass weniger Menschen elektronisch Kontakt zu ihnen aufnehmen und oft nicht mehr bereit seien, offen zu sprechen. Da eine persönliche Beratung oft nicht möglich sei, könne psychisch kranken Menschen, Drogenabhängigen, gewaltbereiten Menschen usw. teils nicht mehr geholfen werden, was Gesundheits- und Lebensgefahr - auch für Dritte - nach sich ziehen kann.

Die **vollständigen Berichte** über die Auswirkungen finden sich im Internet.[1]

Vor dem Hintergrund dieser Ergebnisse, haben der Arbeitskreis Vorratsdatenspeicherung und andere Verbände eine **repräsentative Umfrage des renommierten Meinungsforschungsinstituts Forsa** in Auftrag gegeben. Dieses befragte 1.002 Bundesbürgern am 27./28. Mai 2008. Ergebnisse der Umfrage waren:

- Sieben von zehn Befragten war **bekannt**, dass seit Beginn des Jahres 2008 alle Verbindungsdaten jedes Bürgers in Deutschland sechs Monate lang gespeichert werden müssen (731 der Befragten).
- Die Mehrheit der Befragten **würde wegen der Vorratsdatenspeicherung davon absehen**, per Telefon, E-Mail oder Handy Kontakt zu einer Eheberatungsstelle, einem Psychotherapeuten oder einer Drogenberatungsstelle aufzunehmen, wenn sie deren Rat benötigten (517 der Befragten). Hochgerechnet entspricht dies über 43 Mio. Deutschen.
- Jede dreizehnte Person hat wegen der Verbindungsdatenspeicherung **bereits mindestens einmal darauf verzichtet**, Telefon, Handy oder E-Mail zu benutzen (79 der Befragten). Hochgerechnet entspricht dies 6,5 Mio. Deutschen. Jede sechzehnte Person hat den Eindruck, dass andere Menschen seit Beginn der Vorratsdatenspeicherung seltener per Telefon, Handy oder E-Mail Kontakt mit ihr aufnehmen (62 der Befragten). Hochgerechnet entspricht dies 5 Mio. Deutschen. Besonders stark ist die Veränderung des Kommunikationsverhaltens unter Menschen mit geringem Bildungsniveau (Haupt- oder Grundschulabschluss).
- Nahezu jeder zweite Bundesbürger sieht in der Vorratsdatenspeicherung einen **unverhältnismäßigen und unnötigen Eingriff** in seine Freiheitsrechte (465 der Befragten). Hochgerechnet entspricht dies 43 Mio. Deutschen, die sich gegen die Verbindungsdatenspeicherung aussprechen.

Die **vollständigen Umfrageergebnisse** finden sich im Internet.[2]

Im weiteren Verlauf des Jahres 2008 stellte sich heraus, dass die Deutsche Telekom AG als größter Anbieter von Telekommunikationsdiensten in Deutschland in

1 Schriftsatz der Beschwerdeführer an das Bundesverfassungsgericht vom 11.02.2008, http://www.vorratsdatenspeicherung.de/images/schriftsatz_2008-02-11_anon.pdf.
2 http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf.

den Jahren 2005 und 2006 über einen Zeitraum von insgesamt anderthalb Jahren **missbräuchlich die Telefonverbindungsdaten von Journalisten** sowie von Arbeitnehmer-Aufsichtsräten und Managern des Unternehmens ausgewertet hat, um undichte Stellen im Unternehmen aufzudecken.[3] Ziel der Operation war die Auswertung der Festnetz- und Mobilfunk-Verbindungsdatensätze der wichtigsten über die Telekom berichtenden deutschen Journalisten und deren privater Kontaktpersonen.[4] Ausgewertet wurden nicht weniger als 250.000 Verbindungen.[5] Anhand von Handy-Standortdaten wurden selbst die Bewegungen der Betroffenen nachverfolgt, um mögliche Zusammentreffen zu ermitteln.[6] Überwacht wurden auch Personen, die mit der Telekom kaum oder nicht zu tun hatten.[7] Es besteht der Verdacht, dass Daten auch missbraucht wurden, um Vorteile in Arbeitskämpfen zu erzielen.[8]

Wenngleich diese missbräuchlichen Nutzungen gespeicherter Kommunikationsdaten **vor Inkrafttreten der Vorratsdatenspeicherung** erfolgten, waren zum damaligen Zeitpunkt doch zumindest all diejenigen Personen vor einer missbräuchlichen Aufdeckung ihres Kommunikationsverhaltens geschützt, die einen Pauschaltarif („Flatrate“) nutzten oder eine Löschung oder Verkürzung ihrer Verbindungsdaten verlangt hatten. Standortdaten waren damals dadurch vor einer rückwirkenden Aufdeckung geschützt, dass sie nicht gespeichert werden durften. Die Deutsche Telekom AG konnte in diesen Fällen allenfalls für die Zukunft Verkehrsdaten missbräuchlich aufzeichnen.

Einem **heute stattfindenden Missbrauch** von Kommunikationsdaten würden wegen der Vorratsdatenspeicherung 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 sind mit der Vorratsdatenspeicherung entfallen. Spätestens seit 2009 ist zusätzlich der gesamte E-Mail-Verkehr einer missbräuchlichen Auswertung ausgesetzt.

Eine **Beschränkung der staatlichen Zugriffsrechte** ist von vornherein nicht geeignet, derartigen Missbrauch zu verhindern.[9] Dies zeigt sich bereits daran, dass das Vorgehen der Deutschen Telekom AG gegen Telekommunikationsgesetz und Strafgesetzbuch verstieß und dennoch stattgefunden hat. Nach Auskunft der Bundesregierung sind bei Kontrollen der Deutschen Telekom AG durch die Aufsichtsbehörden keine Auffälligkeiten festgestellt worden; das Sicherheitskonzept war nicht zu beanstanden.[10] Dies zeigt, dass Sicherungsvorkehrungen auch in Zukunft weitere Fälle von Datenmissbrauch nicht werden verhindern können.

Einen wirksamen Schutz vor Missbrauch ermöglicht somit alleine die Unterbindung der Protokollierung des Verhaltens selbst entsprechend dem Gebot der Datensparsamkeit.[11] **Nur nicht gespeicherte Daten sind sichere Daten.**

---

3 Spiegel Online vom 24.05.2008, http://www.spiegel.de/wirtschaft/0,1518,555162,00.html.
4 a.a.O.
5 Spiegel Online vom 29.05.2008, http://www.spiegel.de/wirtschaft/0,1518,556398,00.html.
6 Handelsblatt vom 30.05.2008, http://www.handelsblatt.com/News/default.aspx?_p=201197&_t=ft&_b=1436894.
7 Spiegel Online vom 19.11.2008, http://www.spiegel.de/wirtschaft/0,1518,591374,00.html.
8 http://www.swr.de/report/-/id=233454/did=4196196/pv=video/gp1=4340300/nid=233454/16mqp0q/index.html.
9 Gola/Klug/Reif, Datenschutz- und presserechtliche Bewertung der „Vorratsdatenspeicherung“ (2007), 38.
10 Bundesregierung, BT-Drs. 16/9894, 3.
11 Gola/Klug/Reif, Datenschutz- und presserechtliche Bewertung der „Vorratsdatenspeicherung“

Die von der Richtlinie in Blick genommene Datennutzung zu Strafverfolgungszwecken – die nicht selten aufgrund eines falschen Verdachts, mitunter auch missbräuchlich erfolgt – stellt nur einen kleinen Ausschnitt aus den insgesamt **durch die Kommunikationsdatenerfassung drohenden Gefahren** dar. Bloße Beschränkungen der Datennutzung durch die staatlichen Stellen lassen die Bürger ungeschützt vor

1. illegalen Zugriffen des speichernden Unternehmens
2. illegalen Zugriffen einzelner Mitarbeiter des speichernden Unternehmens
3. illegalen Zugriffen staatlicher Stellen
4. illegalen Zugriffen einzelner Mitarbeiter staatlicher Stellen
5. illegalen Zugriffen Dritter wie etwa Hacker
6. versehentlicher Offenlegung durch das speichernde Unternehmen
7. versehentlicher Offenlegung durch einzelne Mitarbeiter des speichernden Unternehmens
8. versehentlicher Offenlegung durch staatliche Stellen
9. versehentlicher Offenlegung durch einzelne Mitarbeiter staatlicher Stellen.

Die **Vorfälle bei der Telekom** beweisen, dass Beschränkungen von Zugriffsrechten und -möglichkeiten vor irreparablen Nachteilen aufgrund der Aufzeichnung von Kommunikationsdaten nicht wirksam schützen können.

Ausweislich einer am 02. Juni 2008 vom Meinungsforschungsinstitut Emnid unter 1.000 Bundesbürgern durchgeführten Umfrage sind acht von zehn Bürgern überzeugt, dass es sich bei den Vorgängen bei der Telekom **nicht um einen Einzelfall** handelt, sondern dass derartige Vorgänge an der Tagesordnung sind.[12] Diese durchaus realistische Einschätzung zeigt, dass die Vorgänge bei der Telekom das Vertrauen der Bürger in die Vertraulichkeit der Telekommunikation weiter zerstört haben. Die Mehrheit der befragten Bürger forderte als Konsequenz aus den Vorgängen einen verbesserten Datenschutz.[13] Aus den genannten Gründen kann eine solche Verbesserung einzig in der Beendigung der Vorratsdatenspeicherung selbst liegen. Allein dies bietet einen effektiven Schutz vor Missbräuchen.

Eine Umfrage des Instituts für Demoskopie Allensbach im Januar 2009[14] ergab, dass **nur 8% der Bundesbürger Unternehmen, wie sie mit gespeicherten Daten umgehen, vertrauen**. 82% misstrauen den Unternehmen da eher. Nur 16% der Bundesbürger vertrauen dem Staat, wie er mit gespeicherten Daten umgeht. 72% misstrauen dem Staat da eher. 61% der Befragten machen sich Sorgen, dass ihre eigenen Daten nicht ausreichend geschützt sind. 52% sind in letzter Zeit vorsichtiger geworden, wenn sie irgendwo ihre persönlichen Daten angeben mussten. Weitere 24% waren schon immer vorsichtig, wenn sie irgendwo ihre persönlichen Daten angeben mussten.

Neben dem Risiko von Datenverlust und -missbrauch bei den speichernden Stellen ist aber auch die Gefahr von Nachteilen infolge von Fehlern oder Irrtümern staatlicher Stellen bekannt. Telekommunikationsdaten führen regelmäßig dazu, dass **Unschuldige überwacht, durchsucht oder sogar verhaftet** werden. Sie weisen nämlich nur auf einen Anschluss hin, nicht aber auf die Person des Nutzers. Es kommt

(2007), 38; Rusteberg, VBlBW 2007, 171 (175).

12 Pressemitteilung von N24 vom 04.06.2008, http://www.presseportal.de/pm/13399/1204206/n24.

13 a.a.O.

14 http://www.ifd-allensbach.de/pdf/prd_0906.pdf.

häufig zu Falschverdächtigungen, etwa weil Personen ein offenes WLAN-Netz anbieten.

Zu Unrecht ins Visier der Kriminalpolizei ist etwa 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. Erst später stellte sich heraus, dass der eigentliche Täter den Internetzugang des zu Unrecht Verdächtigten über Funknetz (WLAN) genutzt hatte.[15]

Auch 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 bloß eine falsche Auskunft erteilt.[16]

Insgesamt zeigt sich, dass die Vorratsdatenspeicherung zu einem hohen Maß an Verunsicherung unter Bürgern und Verbrauchern führt, die - mit Recht - um die Sicherheit ihrer sensiblen Verbindungs-, Standort- und Internetzugangsinformationen fürchten müssen, daneben aber auch mit der jederzeitigen (legalen) staatlichen Nachverfolgbarkeit ihrer Kommunikationsbeziehungen nicht einverstanden sind. Dieser Vertrauensverlust behindert oder verhindert die Nutzung der neuen Medien teilweise, was **verheerende Auswirkungen auf die Betroffenen, die Gesellschaft, aber auch die Wirtschaft** hat.

2. Maßnahmen zur Begrenzung der nachteiligen Auswirkungen

> *„2.A.2. What additional measures (administrative, technical, legal, or other) would be appropriate for the offset of any negative impact(s) which has been identified?“*

a) Aufhebung der Richtlinie

Da nur nicht gespeicherte Daten sichere Daten sind, sollte die Richtlinie zur Vorratsdatenspeicherung in erster Linie als **Irrweg** aufgehoben werden. So hat sie keines ihrer Ziele erreicht, weder eine Harmonisierung der Datenspeicherung, noch eine messbare Verbesserung der Sicherheit der Bürger.

Von der ursprünglichen Zielsetzung der Richtlinie, die Speicherung von Telekommunikationsdaten in Europa zu **vereinheitlichen**, ist nichts übrig geblieben. Die Richtlinie schreibt lediglich Mindeststandards vor. Den EU-Mitgliedstaaten bleibt es unbenommen, die Daten länger speichern zu lassen (Art. 12 Abs. 1 RiL 2006/24/EG), weitere Datentypen aufzeichnen zu lassen (Art. 15 RiL 2002/58/EG) oder Zugriffe zu anderen Zwecken als zur Verfolgung schwerer Straftaten zuzulassen. Während die Telekommunikationsbranche vor Inkrafttreten der Richtlinie in einigen Mitgliedsstaaten unterschiedlichen Anforderungen zur Vorratsdatenspeicherung ausgesetzt war, ist sie nun in sämtlichen Mitgliedsstaaten unterschiedlichen Anforderungen zur Vorratsdatenspeicherung ausgesetzt. Die Richtlinie hat also das Gegenteil ihres Ziels erreicht.

---

15 http://www.presseportal.de/polizeipresse/p_story.htx?nr=920697.
16 http://www.lawblog.de/index.php/archives/2008/03/11/provider-liefert-falsche-daten-ans-bka/.

Ferner ist für keinen Staat ersichtlich, dass - und sei es auch nur im Bereich der Netzkriminalität - mit Vorratsdatenspeicherung die **Kriminalitätsrate** geringer oder die Aufklärungsrate höher wäre als ohne. Die Richtlinie hat folglich auch dieses Ziel nicht erreicht.

Dass die Vorratsdatenspeicherung demgegenüber das Grundrecht auf Achtung der Privatsphäre (Art. 8 EMRK) verletzt, ergibt sich inzwischen aus dem **Urteil der Großen Kammer des Europäischen Gerichtshofs für Menschenrechte vom 04.12.2008**.[17] Darin hat der Gerichtshof ausgeführt:[18]

> *„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:

1. 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 verworfenen Befugnis betroffen. Von der Richtlinie zur Vorratsdatenspeicherung sind demgegenüber praktisch alle 365 Mio. Europäer betroffen.
2. 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:

1. 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

17 EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 112.
18 EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 116.

Krankheiten. Die unter der Vorratsdatenspeicherung gesammelten Informationen betreffen zwar auch unsere Identität und erlauben die Identifizierung von Gesprächsteilnehmern (Name und Anschrift). Sie betreffen vor allem aber unser tägliches Kommunikations-, Informations- und Bewegungsverhalten (Verbindungs-, Internetzugangs- und Standortdaten). 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.

2. 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 **Verhältnismäßigkeitsverbot**, 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.[19] Dieser Behauptung hat der Gerichtshof erstens entgegen gehalten, dass England die Maßnahme selbst erst 2001 eingeführt habe.[20] Zweitens hat er darauf hingewiesen, dass die Strafverfolgungsbehörden anderer Staaten auch ohne eine solche Maßnahme auskommen.[21] Nichts anderes gilt auch für die Vorratsspeicherung von Telekommunikationsdaten.

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 viele Fällen ein erfolgreicher Abruf auch tatsächlich zur Verurteilung eines Straftäters geführt habe.[22] Auch sei nicht dargelegt, in wie vielen Fällen hierfür gerade die Vorratsspeicherung der Daten Nichtverurteilter erforderlich gewesen sei.[23] Die meisten der von der Regierung genannten erfolgreichen Abrufe wären auch ohne die beanstandete Vorratsspeicherung möglich gewesen.[24] Wenngleich der Gerichtshof im Ergebnis davon ausging, dass die Vorratsspeicherung biometrischer

19 EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 115.
20 EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 115.
21 EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 112.
22 EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 116.
23 EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 116.
24 EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 116.

Daten einen gewissen Beitrag zur Strafverfolgung leistete,[25] 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.[26] 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.[27] 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 Ungleichem liege eine Stigmatisierung der Betroffenen.[28] – 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.[29] Gleiches gilt im Fall der Vorratsdatenspeicherung insbesondere im Hinblick auf besondere Vertrauensverhältnisse.

Empfehlung: Der Europäischen Kommission ist zu raten, einer Aufhebung der Richtlinie zur Vorratsdatenspeicherung durch die Gerichte zu entgehen, indem sie die Richtlinie freiwillig aufhebt.

b) Sonst: Einführung eines Opt-out-Rechts der Mitgliedsstaaten

Sollte die Kommission eine Aufhebung der Richtlinie nicht vorschlagen, so fordern wir, die Richtlinie dahin zu ändern, dass **jeder Mitgliedsstaat selbst entscheidet**, ob er eine verdachtslose Erfassung von Telekommunikationsdaten anordnen will und - nach seinem nationalen Verfassungsrecht - darf. Dazu könnte an Artikel 1 der Richtlinie 2006/24/EG beispielsweise folgender Absatz 3 angefügt werden:

> „*Diese Richtlinie gilt **nur für diejenigen Mitgliedsstaaten**, nach deren nationalem Recht abweichend von den Artikeln 5, 6 und 9 der Richtlinie 2002/58/EG Daten, soweit sie im Rahmen ihrer Zuständigkeit im Zuge der Bereitstellung der betreffenden Kommunikationsdienste von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes erzeugt oder verarbeitet werden, auf Vorrat zu speichern sind.*"

Wenn man die Richtlinie auf ihre eigentliche Grundlage - die Beseitigung von Wettbewerbshindernissen durch unterschiedliche Anforderungen an Wirtschaftsunternehmen - zurück führt, ist bei Lichte betrachtet eine Harmonisierung der Vorrats-

25 EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 117.
26 EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 121.
27 EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 121.
28 EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 122.
29 EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 124.

datenspeicherung nämlich nur in denjenigen Staaten erforderlich, die überhaupt eine Vorratsdatenspeicherung wollen. Vor allem ist eine verpflichtende Vorratsdatenspeicherung mit den **Grundrechten der Bürger** nicht vereinbar. Insoweit wird auf das grundlegende Urteil des Europäischen Menschenrechtsgerichtshofes in Sachen S. und Marper vom 04.12.2008 Bezug genommen.[30]

Bei mehreren **Verfassungsgerichten der Mitgliedsstaaten** sind Beschwerden gegen die Umsetzung der Richtlinie anhängig, unter anderem bei dem deutschen Bundesverfassungsgericht. Das rumänische Verfassungsgericht hat das rumänische Umsetzungsgesetz bereits für verfassungswidrig erklärt.[31]

Empfehlung: Wenn die Richtlinie 2006/24/EG schon nicht aufgehoben wird, muss sie es wenigstens den Mitgliedsstaaten überlassen, ob ihre Rechtsordnung weiterhin eine verdachtslose, flächendeckende Erfassung der Kommunikationsbeziehungen und Bewegungen ihrer Bürger zulassen soll und darf.

c) Klare Ausnahme nicht-kommerzieller Dienste

In Deutschland wird bestritten, dass die Pflicht zur Vorratsdatenspeicherung nach der Richtlinie 2006/24/EG **nur für kommerzielle Dienste gilt**, wie es die Kommission ausgehend von Art. 95 EG zutreffend erläutert hat.[32] Ursache sind die insoweit divergierenden Sprachfassungen der Richtlinie 2002/21/EG, auf deren Definitionen die RiL 2006/24/EG Bezug nimmt.

In der englischen Fassung der RiL 2002/21/EG lautet Art. 2 Buchst. c: "'*electronic communications service' means* ***a service normally provided for remuneration*** *[…]*". Auch in der französischen Fassung definiert Art. 2 Buchst. c "*service de communications électroniques*" als "*le service fourni normalement contre rémunération […]*".

Nur die deutsche Fassung verursacht Verwirrung, weil "*elektronische Kommunikationsdienste*" im Plural als "*gewöhnlich gegen Entgelt erbrachte Dienste*" definiert werden. Dies wird nun von der **Bundesregierung** und der Bundesnetzagentur so ausgelegt, dass selbst unentgeltliche WLAN-Zugänge, E-Mail-Dienste o.ä. zur Vorratsdatenspeicherung verpflichtet seien, weil WLAN-Zugänge und E-Mail-Dienste gewöhnlich gegen Entgelt erbracht würden.[33] Richtigerweise ist aber maßgeblich, ob das jeweilige Angebot des einzelnen Anbieters gewöhnlich gegen Entgelt erbracht wird oder nicht.

Es macht inhaltlich einen **Unterschied**, ob *„Dienste [einer Art] gewöhnlich gegen Entgelt*“ erbracht werden oder ob *„ein Dienst gewöhnlich gegen Entgelt*“ erbracht wird.

Daher muss die **deutsche Definition in Art. 2 Buchst. c RiL 2002/21/EG** entsprechend der französischen und englischen Fassung formuliert werden:

> *c) "elektronischer Kommunikationsdienst":* ***ein gewöhnlich gegen Entgelt erbrachter Dienst****, der ganz oder überwiegend in der Übertragung von Signalen*

30 EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04.
31 Aktenzeichen 788 D / 2009.
32 Antworten E-0969/2009 und E-4374/09 auf Anfragen des Abgeordneten Alexander Alvaro.
33 Bundesjustizministerium, Stellungnahme vom 02.06.2009 gegenüber dem Bundesverfassungsgericht, http://www.vorratsdatenspeicherung.de/images/StN_BMJ_2009-06-02.pdf, S. 21 ff.

über elektronische Kommunikationsnetze besteht, einschließlich Telekommunikations- und Übertragungsdienste in Rundfunknetzen, jedoch ausgenommen Dienste, die Inhalte über elektronische Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben; nicht dazu gehören die Dienste der Informationsgesellschaft im Sinne von Artikel 1 der Richtlinie 98/34/EG, die nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen;

Empfehlung: Wir fordern die Kommission auf, auf eine entsprechende Berichtigung der deutschen Sprachfassung des Art. 2 Buchst. c RiL 2002/21/EG hinzuwirken.

d) Volle Kostenerstattung für die verpflichteten Unternehmen

Viertens fordern wir, die bereits ursprünglich von der Kommission vorgeschlagene **Kostenerstattungspflicht** in die Richtlinie aufzunehmen, wobei die erforderlichen Investitions-, Vorhalte- und Auskunftskosten der zur Speicherung Verpflichteten voll zu erstatten sind.

Die **wirtschaftlichen Auswirkungen** einer Vorratsspeicherungspflicht sind enorm. Diese Zusatzkosten könnten 15-20% der Kosten von Telekommunikationsdienstleistungen ausmachen[34] und zur Einstellung bisher kostenloser Angebote führen. Ausnahmen für kleinere Anbieter sind nicht vorgesehen. Die vorgeschriebene Datenspeicherung können kleine Anbieter nicht leisten; die dazu erforderlichen Einrichtungen werden sie aus finanziellen Gründen nicht anschaffen. Die Vorratsdatenspeicherung führt dadurch zu einer deutlichen Verschlechterung der telekommunikativen Infrastruktur, auch im internationalen Vergleich.

Die Verfassungsgerichte Österreichs und Frankreichs haben bereits entschieden, dass eine **entschädigungslose Inpflichtnahme der Wirtschaft zu Strafverfolgungszwecken verfassungswidrig** ist.[35] In der Tat sind Telekommunikationsunternehmen für den Missbrauch ihrer Dienste durch Straftäter nicht verantwortlich. Sie kontrollieren die Kommunikation ihrer Kunden nicht und dürfen dies wegen des Fernmeldegeheimnisses auch nicht. Die Telekommunikationsüberwachung erfolgt nicht zu ihren Gunsten, sondern ist eine öffentliche Angelegenheit, deren Lasten die Allgemeinheit der Steuerzahler zu tragen hat. In Deutschland ist deshalb aus Art. 12 und Art. 3 GG abzuleiten, dass der Staat Telekommunikationsunternehmen die Mehrkosten einer staatlich angeordneten Vorratsdatenspeicherung voll zu erstatten hat.[36] Eine Verfassungsbeschwerde gegen den Ausschluss der Kostenerstattung ist in Deutschland anhängig.[37] Das Verwaltungsgericht Berlin hält den Ausschluss für verfassungswidrig.[38]

Bislang ist in **Deutschland** eine (teilweise) Entschädigung für die Mitwirkung an der Telekommunikationsüberwachung nur für Mehrkosten infolge einzelner Überwachungsanordnungen vorgesehen (§ 23 Abs. 1 S. 1 Nr. 2 JVEG, § 20 G10). Diese

34 ISPA Austria, http://www.ispa.at/www/getFile.php?id=452.

35 Conseil constitutionnel, 2000-441 DC vom 28.12.2000, http://www.conseil-constitutionnel.fr/decision/2000/2000441/2000441dc.htm; Österr. Verfassungsgerichtshof, G 37/02-16 u.a. vom 27.02.2003, http://www.epic.org/privacy/intl/austrian_ct_dec_022703.html.

36 Näher Breyer, Vorratsspeicherung (2005), http://www.vorratsspeicherung.de.vu, 277 ff. und 357 ff.

37 Initiative Europäischer Netzbetreiber (IEN), Pressemitteilung vom 10.11.2006, http://www.ien-berlin.de/resources/061110-PM-AKUE.pdf.

38 Verwaltungsgericht Berlin, Beschluss v. 02.07.2008 - Az.: VG 27 A 3.07, http://www.webhosting-und-recht.de/urteile/Verwaltungsgericht-Berlin-20080702.html.

Entschädigung deckt nur 2% der Kosten ab, die Telekommunikationsunternehmen durch ihre gesetzlich angeordnete Mitwirkung an der Telekommunikationsüberwachung entstehen.[39] Insbesondere eine Entschädigung für gesetzlich vorgeschriebene Überwachungsvorrichtungen und für sonstige Vorhaltekosten (z.B. Personalkosten) ist gegenwärtig ausgeschlossen (§ 110 Abs. 1 und Abs. 9 S. 2 TKG). Viele Anbieter haben nicht einmal eine Überwachungsmaßnahme pro Jahr durchzuführen.

Müsste der Staat für die enormen Kosten der Vorratsdatenspeicherung aufkommen, so würde offenbar, dass der damit verbundene Aufwand zulasten tatsächlicher, gezielter Maßnahmen zur Gewährleistung der Sicherheit geht. Es würde sich schon aus **Haushaltssicht** die Frage stellen, ob die für die Vorratsdatenspeicherung aufgewandten Mittel nicht sinnvoller und effektiver eingesetzt werden könnten. Zum Schutz vor Netzkriminalität beispielsweise versprechen technische Schutzmaßnahmen und Aufklärungskampagnen einen weitaus größeren Erfolg als repressive Maßnahmen.[40]

e) Schutz von Datenpannen, Datendiebstahl und Datenmissbrauch verbessern

Folgende Maßnahmen erscheinen fünftens zur **besseren Sicherung von Telekommunikationsdaten** gegen Datenpannen, Datendiebstahl und Datenmissbrauch sinnvoll:

(1) Verschlüsselung der Vorratsdaten

Erstens sollten die Anbieter personenbezogene Telekommunikationsdaten mithilfe von asymmetrischen Schlüsseln der „Bedarfsträger“ **in Echtzeit verschlüsseln** und verschlüsselt in einer gesonderten Datenbank aufbewahren. Durch den Einsatz asymmetrischer Schlüssel ist gesichert, dass die Daten ausschließlich von den Bedarfsträgern unter Verwendung ihres geheimen Entschlüsselungs-Schlüssels (privater Schlüssel) wieder in Klartext verwandelt und genutzt werden können und nicht von dem Anbieter oder Dritten, wie es etwa bei der Deutschen Telekom AG systematisch geschehen ist. Auskunftsersuchen kann der Anbieter auch dann bedienen, wenn er die gespeicherten personenbezogenen Telekommunikationsdaten verschlüsselt hat. Er muss dazu nur die Suchkriterien aus dem Auskunftsersuchen mit den Schlüsseln der Bedarfsträger verschlüsseln und das Ergebnis mit seiner Datenbank abgleichen. Die ermittelten, verschlüsselten Daten übermittelt er an die Behörde. Die Behörde entschlüsselt die Daten sodann mit ihrem geheimen Schlüssel.

(2) Isolierung der Vorratsdatenspeicher

Damit Telekommunikationsdaten nicht versehentlich über das Internet veröffentlicht oder zugänglich gemacht werden, darf die Datenbank zweitens nicht an das Internet angebunden sein. Eine strenge **physikalische Trennung des Datenbankrechners vom Internet** ist dazu erforderlich.

(3) Sicherere Übermittlung von Vorratsdaten

39 Bitkom: Schriftliche Stellungnahme zur öffentlichen Anhörung am 09.02.2004 zum Entwurf eines Telekommunikationsgesetzes, in Ausschussdrucksache 15(9)961, http://www.bitkom.org/files/documents/StN_BITKOM_TKG_Wirtschaftsausschuss_03.02.04.pdf, 24.

40 Näher Breyer, Vorratsspeicherung (2005), http://www.vorratsspeicherung.de.vu, 338 ff.

Drittens ist gegenwärtig zu beklagen, dass die Anbieter **Auskunftsersuchen** verbreitet per E-Mail beantworten. Die angeforderten Telekommunikationsdaten werden entweder überhaupt nicht oder mit einem so schwachen Verfahren verschlüsselt (ZIP), dass sich der Schutz mit kostenloser Software aus dem Internet in Sekundenschnelle aufheben lässt. Da E-Mails über beliebige Rechner im In- und Ausland übertragen werden, bis sie zum Empfänger gelangen, liegt in dieser Verfahrensweise ein gravierendes Risiko für die Vertraulichkeit der übermittelten Telekommunikationsdaten. Zu fordern ist entweder eine wirksame Verschlüsselung oder die Nutzung eines anderen Übertragungsmediums (z.B. Post). Papier ist ohnehin besser vor unbefugter Weitergabe geschützt als elektronische Daten, die sich beliebig und spurenlos weiterstreuen lassen.

(4) Maßnahmen zur Gewährleistung der Datensicherheit müssen dem Stand der Technik entsprechen

In den letzten Monaten sind immer wieder **schwerwiegende Datenpannen mit Millionen von Betroffenen** bekannt geworden, die hätten vermieden werden können, wenn die Verarbeitungssysteme auf dem Stand der Technik gewesen wären (z.B. durch Anwendung von Updates).

Formulierungsvorschlag für Artikel 17 (1) RiL 95/46/EG – neu:

> „Die Mitgliedstaaten sehen vor, daß der für die Verarbeitung Verantwortliche die geeigneten technischen und organisatorischen Maßnahmen durchführen muß, die für den Schutz gegen die zufällige oder unrechtmässige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang – insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden – und gegen jede andere Form der unrechtmässigen Verarbeitung personenbezogener Daten erforderlich sind.Diese Maßnahmen müssen *dem Stand der Technik entsprechen und* ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.“

Rechtliche Anforderungen an die Datensicherheit werden allerdings verbreitet nicht beachtet, selbst wo sie bestehen. Dies zeigen die zahlreichen Datenmissbräuche, Datenpannen und sonstigen Datenskandale der vergangenen Monate. Um diesem **Durchsetzungsdefizit** besser zu begegnen, kommen etwa die folgenden Maßnahmen in Betracht:

(5) Einführung eines Verbandsklagerechts für Verbraucher- und Datenschutzverbände, damit sie gegen datenschutzwidrige Praktiken klagen können.

Begründung: Bei von Einzelnen angestrengten Prozessen wegen datenschutzwidriger Praktiken – etwa im Fall Voss ./. T-Online – gibt es immer wieder **Finanzierungsschwierigkeiten**; außerdem wird das Urteil von der Gegenseite oftmals nur für den jeweiligen Kläger umgesetzt und nicht für alle Kunden.

(6) Klarstellung, dass Datenschutzbestimmungen auch dem Schutz eines fairen Wettbewerbs dienen.

Begründung: Die Einhaltung des Datenschutzrechts ist **wettbewerbsrelevant**, weil sich hiergegen verstoßende Unternehmen im Wettbewerb mit datenschutzkonform arbeitenden Konkurrenten einen unlauteren Vorteil durch Rechtsbruch verschaffen. Bisher sind die Gerichte in Deutschland der Meinung, dass Datenschutzvor-

schriften nicht wettbewerbsschützend seien. Das Wettbewerbsrecht ist aber ein effizientes, unbürokratisches und erfolgreiches Instrument zur Rechtsdurchsetzung, das auf den Bereich des Datenschutzes erstreckt werden sollte.

(7) Einführung einer Herstellerhaftung für den Fall, dass unsichere Produkte zu Datenschutzverletzungen führen (Produkthaftung)

Begründung: Im Softwarebereich wäre es sinnvoll, die **Produkthaftung** von Herstellern informationstechnischer Produkte auf Vermögensschäden zu erstrecken, die dadurch entstehen, dass ein Produkt nicht wirksam (Stand der Technik) vor Computerattacken oder Datenverlust geschützt ist. Dann würden Softwarehersteller für die Folgen ihrer Sicherheitslücken („Bugs“) haften, die schon oft für Verluste persönlicher Daten und von Betriebsgeheimnissen gesorgt haben. Das Haftungsrecht ist ein sehr effizientes Rechtsdurchsetzungsinstrument, wie sich etwa im Bereich der Arbeitssicherheit gezeigt hat. Es sollte auch für den Datenschutz nutzbar gemacht werden.

(8) Verschuldensunabhängige Haftung für Datenschutzverletzungen mit pauschaler Entschädigungssumme

Die Datenverarbeiter sollten den Betroffenen auch fürimmaterielle Schäden haften (z.B. Sorge um einen möglichen Missbrauch ihrer Daten infolge einer Datenpanne), und zwar verschuldensunabhängig. Ein **Regelwert** für den immateriellen Schaden sollte festgelegt werden (z.B. 200 Euro pro Person). Entschädigungszahlungen wegen Datenpannen könnte der für die Verarbeitung Verantwortliche dann vom Hersteller ersetzt verlangen (siehe Punkt 3 oben), wenn ein unsicheres Produkt für den Schaden verantwortlich ist.

Begründung: Durch die Einführung einer Haftung für Datenpannen samt pauschaler Entschädigungssummen wären große Datenverarbeiter gezwungen, sich gegen Datenschutzverletzungen zu **versichern**. Durch die Versicherungsprämie hätten sie ein eigenes finanzielles Interesse daran, die Schadenswahrscheinlichkeit zu senken. Auf dem Gebiet der Unfallversicherung hat ein solches System bereits zu einem drastischen Rückgang der Zahl der Arbeitsunfälle geführt.

(9) Benachteiligungsverbot bei Gebrauchmachen von Datenschutzrechten

Begründung: In der Praxis werden unabdingbare Regelungen des Datenschutzrechts immer wieder dadurch umgangen, dass Unternehmen mit einer ordentlichen **Kündigung** reagieren, wenn Betroffene von ihren gesetzlich garantierten Rechten Gebrauch machen. Zu diesen unabdingbaren Betroffenenrechten zählt insbesondere das Recht, Auskunft über die zur eigenen Person gespeicherten Daten verlangen zu dürfen sowie die Rechte auf Berichtigung, Löschung und Sperrung personenbezogener Daten.

Formulierungsvorschlag Richtlinie 95/46/EG:

> *„Der für die Verarbeitung Verantwortliche darf den Betroffenen nicht benachteiligen, weil dieser in zulässiger Weise von Rechten aus dieser Richtlinie Gebrauch macht. Wenn im Streitfall der Betroffene Tatsachen glaubhaft macht, die eine Benachteiligung im Sinne des Satzes 1 vermuten lassen, trägt der Verantwortliche die Beweislast dafür, dass andere, sachliche Gründe die Behandlung des Betroffenen rechtfertigen.“*

(10) Einrichtung einer „Stiftung Datentest“

Eine Stiftung nach dem Vorbild der „Stiftung Warentest“ sollte geschaffen werden, um verschiedene Anbieter von Dienstleistungen einer Art **vergleichen** zu lassen im Hinblick auf die Menge der jeweils erhobenen personenbezogenen Daten, die Datenverwendung und -weitergabe (etwa ins Ausland, an Auskunfteien oder zu Werbezwecken) und die Datensicherheit.

Begründung: Verbraucher können heutzutage realistischerweise nicht **überblicken**, was einzelne Anbieter mit ihren Daten machen. Auf dem Gebiet der Qualitätssicherung hat sich in Deutschland das Modell der „Stiftung Warentest“ bewährt, die Produkte testet, vergleicht und benotet. Wenn es eine „Stiftung Datentest“ gäbe, könnten Verbraucher sich ausgehend von deren Urteil leicht für ein datenschutzfreundliches Produkt entscheiden. Hersteller würden schon präventiv für mehr Datenschutz sorgen, um eine Empfehlung zu erzielen und schlechte Bewertungen zu vermeiden.

Empfehlung: Die Europäische Kommission sollte erhöhte Anforderungen an die Sicherheit der angesammelten Informationen und vor allem Maßnahmen zur verbesserten Durchsetzung der Anforderungen vorschlagen.

3. Handlungsbedarf auf EU-Ebene

> *„2.A.3. Which ones of the measures mentioned under 2.A.2 should be addressed at the level of the European Union?“*

Alle der vorgeschlagenen Maßnahmen sollten auf europäischer Ebene angegangen werden.

4. Verschiebung der Balance von Ermittlungsinteressen und Freiheit

> *„2.A.4. Having regard to changes in technology and experience gathered with the operation of the Data Retention Directive, is the balance provided for by the Directive between enhancing security by means of retaining communication data and protecting civil liberties still appropriate. If a different balance is deemed to be appropriate, please provide details how to adjust the balance as well as the motivation underlying the assessment. [can entail Quantitative elements]“*

Vorab ist darauf hinzuweisen, dass sich die Fragestellung und der prospektive Teil der Evaluierung das **Hauptziel der Richtlinie zu verfehlen** scheint. Dieses liegt nicht in einer „Verbesserung der Sicherheit“, sondern in einer Harmonisierung nationaler Vorschriften zur Vorratsdatenspeicherung, um Wettbewerbsverzerrungen zu vermeiden.[41] Vor dem Hintergrund dieses Ziels ist die Frage, ob neuere Entwicklungen eine Ausweitung der Speicherpflichten im Sicherheitsinteresse gebieten, von vornherein unzulässig.

Stattdessen ist erstens zu fordern, den Katalog der zu speichernden Datentypen in Art. 5 der Richtlinie **abschließend** zu gestalten, falls die Richtlinie nicht insgesamt

41 EuGH, Urteil vom 10.02.2009 – Az. C-301/06, Abs. 60 ff.

aufgehoben wird. Eine Harmonisierung kann nicht erreicht werden, solange jeder Mitgliedsstaat eine eigene Vorratsdaten-Wunschliste aufstellt.

Zweitens ist vor dem Hintergrund der technischen Entwicklung zu fordern, zumindest **Standortdaten und Internetdienste aus dem Katalog der zu speichernden Datentypen zu streichen**, falls eine Aufhebung der Richtlinie nicht vorgeschlagen wird. Keinesfalls dürfen weitere Datentypen oder Dienste (z.B. mobile Breitbanddienste) aufgenommen werden.

Der Fragestellung der Kommission liegt die Vorstellung zugrunde, die **Balance zwischen den bürgerlichen Freiheiten und den Befugnissen** der Strafverfolgungsbehörden zu wahren. Dazu ist zunächst auszuführen, dass mündliche und schriftliche Kommunikation zwischen Menschen traditionell immer möglich gewesen ist, ohne dass jemand Kontakte und Aufenthaltsorte der gesamten Bevölkerung festgehalten hätte. Nur, wenn der Verdacht einer Straftat vorliegt, konnten die zuständigen Behörden versuchen, Kommunikation anhand von Zeugenaussagen und Spuren nachzuvollziehen. Diese Balance hat sich bewährt. Auch ohne Vorratsdatenspeicherung hat beispielsweise die Aufklärungsrate von Internetdelikten in Deutschland mit über 80%[42] die durchschnittliche Aufklärungsquote aller Delikte von 55%[43] bei weitem übertroffen. Weil diese Balance auch für mündliche und schriftliche Kommunikation, die technisch vermittelt wird, erhalten werden muss, ist die Richtlinie zur Vorratsdatenspeicherung insgesamt aufzuheben.

Was die Telefonie angeht, so ist die genannte Balance anfänglich gewahrt worden. Telefongespräche wurden analog vermittelt. **Informationen über die Gespräche wurden nicht festgehalten.** Nur wenn und wo es das nationale Recht ausnahmsweise vorsah, durften sich staatliche Stellen heimlich in die Kommunikation einschalten. Erst mit der Einführung digitaler Vermittlungsstellen bedrohte diese Balance. Die Telekommunikationsgesellschaften erfassten nun nicht mehr nur Abrechnungsdaten, sondern auch Verbindungsdaten. Die Richtlinie 2002/58/EG trug allerdings dafür Sorge, dass diese Daten mit Verbindungsende grundsätzlich zu löschen oder zu anonymisieren waren. Nach Maßgabe des nationalen Rechts erhielten die Strafverfolgungsbehörden Zugriff auf vorhandene Verkehrsdaten und die Befugnis, deren Erfassung im Einzelfall aufgrund eines begründeten Verdachts anzuordnen. Die Erfassung des Telekommunikationsverhaltens blieb weiterhin die Ausnahme, wenn man von freiwilligen Verbindungsnachweisen auf Kundenwunsch absieht. Unter diesem Regime blieben in Deutschland nur 4% aller Auskunftersuchen von Strafverfolgungsbehörden wegen gelöschter Daten unbeantwortet, während zu 96% die abgefragten Verkehrsdaten zur Verfügung standen.[44] Auch die Anschläge in Madrid konnten mit Hilfe betrieblich ohnehin gespeicherter Verkehrsdaten aufgeklärt werden.

Mit der Richtlinie 2006/24 kippte die Balance von Vertraulichkeit des Telekommunikationsverhaltens und staatlichem Informationsinteresse. Nun wird ohne Anlass und Verdacht das Kommunikations-, Bewegungs- und Internetzugangsverhalten jedes Bürgers festgehalten.

---

42 Bundeskriminalamt, Kriminalstatistik 2007, http://www.bka.de/pks/pks2007/download/pks-jb_2007_bka.pdf, 243.

43 Bundeskriminalamt, Kriminalstatistik 2007, http://www.bka.de/pks/pks2007/download/pks-jb_2007_bka.pdf, 65.

44 Gutachten des Max-Planck-Instituts zur „Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO“ (Februar 2008), 253.

Die Vorratsdatenspeicherung hat indes **weder zu einer Steigerung der Aufklärungsquote noch gar zu einer Senkung der Kriminalitätsrate** und damit Stärkung der Sicherheit der Bürger geführt. Weder bei Erlass der Richtlinie noch unter Berücksichtigung der späteren technologischen Entwicklung ist statistisch nachweisbar, dass die Aufklärungsquote im Bereich mittels Telekommunikation begangener Straftaten rückläufig wäre.

Sicherlich werden die Regierungen der Mitgliedsstaaten **eine Vielzahl von Fällen und Beispielen anführen**, in denen angeblich nicht genügend Informationen über das Kommunikationsverhalten der Bürger zur Verfügung gestanden hätten. Derartige Erfahrungsberichte und Einzelfälle begründen aus den folgenden Gründen aber kein Interesse an einer (gar erweiterten) Vorratsdatenspeicherung:

- Einzelfälle **ohne Angabe ihrer statistischen Relevanz** belegen nicht, dass die Vorratsdatenspeicherung die Aufklärungsrate irgend eines mittels Telekommunikation zu verwirklichenden Straftatbestandes oder einer einzigen Fallgruppe solcher Straftaten auch nur statistisch signifikant erhöht hätte oder erhöhen könnte.
- In vielen der von den Regierungen genannten Fälle handelt es sich **nicht um mittels Telekommunikation** begangene Straftaten. Im Bereich allgemeiner Kriminalität bilden Verkehrsdaten nur einen möglichen Ermittlungsansatz unter vielen und sind besonders häufig ersetzbar.
- In den meisten der von Regierungen genannten Fälle ist nicht dargetan, dass Vorratsdaten zur Identifizierung und Überführung des Täters **erforderlich** gewesen wären und nicht die Nutzung ohnehin gespeicherter Abrechnungsdaten, eine Fangschaltung oder eine Speicheranordnung im Einzelfall ausgereicht hätten.
- In den meisten der übrigen von den Regierungen genannten Fälle ist nicht dargetan, dass die gewünschten Vorratsdaten die Identifizierung und Überführung des Täters **ermöglichen** würden oder ermöglicht hätten. Die Regierungen lassen außer Acht, dass Verkehrsdaten in vielen Fällen nicht zur Identifizierung oder Überführung des Täters führen, etwa wegen der Vielzahl von Verschleierungs- und Anonymisierungsmöglichkeiten.
- Die Regierungen legen nicht offen, ob und in wie vielen der Fälle Vorratsdaten einen Einfluss auf den **Verfahrensausgang** gehabt hätten. Viele Strafverfahren werden auch bei vorhandenen Verkehrsdaten eingestellt, wie die Untersuchung des Max-Planck-Instituts zeigt.
- Die verbleibenden der von der Regierungen angeführten Beispielsfälle wären auch bei **Begehung der Straftat durch unmittelbare oder schriftliche Kommunikation** nicht nachvollziehbar gewesen. Eine Diskriminierung der modernen Kommunikationsformen allein wegen ihrer höheren Überwachungsanfälligkeit ist unzulässig.
- Das Aufklärungsinteresse, welches sich aus den angeführten Einzelfällen ergibt, besteht **unverhältnismäßig selten** gemessen an der Reichweite und Eingriffstiefe der flächendeckenden und anlasslosen Vorratsdatenspeicherung.

Wenn die technische Entwicklung eine Veränderung der Vorratsdatenspeicherung erforderlich macht, dann sind **Standortdaten und Internetdienste** aus dem Katalog der zu speichernden Datentypen zu streichen, falls eine Aufhebung der Richtlinie nicht vorgeschlagen wird. Zunächst ist daran zu erinnern, dass der Entwurf eines Berichts von Berichterstatter Alvaro keine Speicherung von Standortdaten und Internetdiensten vorgesehen hatte.[45]

Sodann ist darauf hinzuweisen, dass sich die **Menge der für staatliche Zwecke verfügbaren Verbindungsdaten** wegen der gesellschaftlichen und technischen Entwicklung von Jahr zu Jahr drastisch erhöht hat. Bis 1990 standen den Strafverfolgungsbehörden noch keinerlei Verkehrsdaten zur Verfügung, weil nach Takt abgerechnet wurde. Seit Einführung der digitalen Vermittlungsstellen Anfang der 90er Jahre hat die Verfügbarkeit von Verbindungsdaten beständig zugenommen. So fielen 1997 im Festnetz der Deutschen Telekom AG 54 Mrd. Verbindungsdatensätze an,[46] während dasselbe Unternehmen heute – trotz eingebrochenen Marktanteils – 120 Mrd. Verbindungsdatensätze pro Jahr verarbeitet.[47] Laut Statistischem Bundesamt hat sich auch das gesamte Gesprächsvolumen in Fest- und Mobilfunknetzen von 2000 bis 2006 von Jahr zu Jahr erhöht[48] und ist heute so hoch wie noch nie. Laut Eurostat ist dieser jährliche Anstieg schon seit Beginn der Statistik im Jahr 1997 zu verzeichnen.[49] Einem Gesprächsvolumen von 1997 185 Mrd. Gesprächsminuten standen 2005 348 Mrd. Gesprächsminuten gegenüber. Ebenso wächst die Zahl der Mobiltelefon- und Internetnutzer ebenso an wie das Maß an Nutzung dieser Medien. Damit steigt auch die Zahl an Informationen, die der Richtlinie zur Vorratsdatenspeicherung zufolge zu speichern nicht.

Die Richtlinie zur Vorratsdatenspeicherung wurde vom Europäischen Parlament im Jahr 2005 verabschiedet. Seither haben sich **mobile Endgeräte** etabliert und sind finanzierbar geworden, die periodisch Verbindungen zum Internet aufbauen, etwa um zu überprüfen, ob neue E-Mails eingegangen sind. Ähnlich verhält es sich, wenn man einen Dienst wie Twitter per SMS abonniert hat. Junge Leute stehen heutzutage ohnehin permanent per SMS miteinander in Verbindung. Die regelmäßige Herstellung mobiler Verbindungen führt nun aber dazu, dass im gesamten Tagesverlauf Standortkennungen und in der Summe ein sehr genaues Bewegungsprofil erstellt wird. Die technische Entwicklung führt außerdem dazu, dass die Funkzellen immer kleiner werden, mithin die Bewegungsdaten immer genauer werden. Die täglichen Bewegungen eines modernen Menschen lassen sich auf diese Weise auf 10-100m genau nachvollziehen.

Auch die **Technik zur Auswertung von Verkehrsdaten** hat sich weiter entwickelt. In einem Versuch des US-amerikanischen Forschungszentrums MIT wurden Telekommunikations-Verbindungsdaten und auf 10m genaue Standortdaten von 100 Versuchspersonen erhoben. Mithilfe dieser Daten gelang es mit einer 90%igen Genauigkeit, die Arbeitskollegen, Bekannten und Freunde einer jeden Person zu iden-

45 Alvaro, Entwurf eines Berichts des Ausschusses für bürgerliche Freiheiten (19.10.2005), http://www.europarl.europa.eu/meetdocs/2004_2009/documents/pr/583/583793/583793de.pdf .

46 Welp, TKÜV, 3 (9).

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

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

49 Indikatoren t501 - Inlandsgespräche und t504 - Anrufe aus dem Mobilfunknetz.

tifizieren.[50] Ferner waren umfangreiche Vorhersagen möglich. Anhand der Bewegungsdaten einer Person während eines Monats konnte mit einer 95%igen Genauigkeit vorhergesagt werden, wann sich die Person am Arbeitsplatz, zu Hause oder an einem anderen Ort aufhalten würde.[51] Weiter konnte mit einer 90%igen Genauigkeit vorhergesagt werden, ob sich zwei Personen innerhalb der nächsten Stunde begegnen würden.[52] Anhand der Aktivitäten einer Person während der ersten 12 Stunden eines Tages konnten die Aktivitäten während der verbleibenden 12 Stunden mit etwa 80% Genauigkeit vorhergesagt werden.[53] Auch die Zufriedenheit am Arbeitsplatz konnte anhand der Daten vorhergesagt werden.[54] Inzwischen kann aus Positionsdaten – auch ohne elektronische Verbindungen – mit 95%-iger Genauigkeit vorhergesagt werden, welche Personen miteinander persönlich befreundet sind.[55]

Das Leben des modernen Menschen verlagert sich immer weiter in den Bereich der Telekommunikationsnetze[56], wie bereits die Schlagworte Telearbeit, Telemedizin, Telebanking, Telelernen, Teleshopping und Telematik deutlich machen. Betroffen von diesem Trend ist nicht nur das öffentliche, sondern auch das Privatleben. Die Vorratsspeicherung von Telekommunikationsdaten erfasst vor diesem Hintergrund so große Teile des Privatlebens wie nie zuvor. Gleichzeitig ist es einem modernen Menschen so schwer wie nie zuvor, einer Erfassung seiner Kommunikationsbeziehungen, Bewegungen und seines Informationsverhaltens im Internet zu entgehen. Immer häufiger sind wir auf die Nutzung der elektronischen Kommunikationsmittel zwingend angewiesen.

Insbesondere die gewachsene Bedeutung von E-Mail und anderen Internetdiensten gegenüber 2005 ist nicht zu überschätzen. E-Mail ersetzt immer häufiger die Briefpost, selbst bei **vertraulicher Korrespondenz** wie mit oder zwischen Rechtsanwälten, Ärzten, Beratungsstellen und Regierungsbehörden. Es ist nicht gerechtfertigt, jeden E-Mail-Kontakt aufzuzeichnen, während dies bei Briefkontakten selbstverständlich nicht erfolgt. Das Internet bildet inzwischen die Grundlage des Informationsverhaltens der Bevölkerung. Es wird mehr genutzt als andere Massenmedien einschließlich des Fernsehens. Es ist nicht gerechtfertigt, jede Internetnutzung aufzuzeichnen, während dies bei der Nutzung anderer Medien (z.B. Zeitung, Fernsehen) undenkbar wäre.

Das von den Verkehrsdaten gezeichnete Bild unseres Verhaltens, in das der Staat Einblick nehmen kann, ist heute mithin so genau wie noch nie. Zugleich steigt die Zahl der staatlichen Auskunftersuchen, die sich diese Entwicklung zunutze machen, von Jahr zu Jahr rapide an.[57] Die Gewichte, die noch bei Beschluss der Richtlinie zur Vorratsdatenspeicherung bestanden haben, haben sich seither weiter zulasten der Privatsphäre und informationellen Selbstbestimmung der Betroffenen verschoben. Um wenigstens die bei Erlass der Richtlinie gegebene Verteilung der Gewichte zu wahren, müssten Positionsdaten und Internetdienste, die heute einen

50 MIT, Relationship Inference, http://reality.media.mit.edu/dyads.php.
51 MIT, User Behavior Modeling and Prediction, http://reality.media.mit.edu/user.php.
52 MIT, Relationship Inference, http://reality.media.mit.edu/dyads.php.
53 MIT, Eigenbehaviors, http://reality.media.mit.edu/eigenbehaviors.php.
54 Eagle/Pentland/Lazer, Inferring Social Network Structure using Mobile Phone Data, 2007, http://reality.media.mit.edu/pdfs/network_structure.pdf.
55 Eagle/Pentland/Lazer, Inferring Social Network Structure using Mobile Phone Data (2009), Proceedings of the National Academy of Sciences (PNAS), Vol. 106(36), 15274 ff.
56 DSB-Konferenz, Freie Telekommunikation (I).
57 Gutachten des Max-Planck-Instituts zur „Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO“ (Februar 2008), 73 ff.

ungleich größeren Einblick in unser Privatleben gewähren als damals, von der Vorratsdatenspeicherung ausgenommen werden.

Empfehlung: Die neueren technischen und gesellschaftlichen Entwicklungen sollten zum Anlass genommen werden, die Richtlinie zur Vorratsdatenspeicherung aufzuheben. Andernfalls sollten die darin genannten Daten- und Dienstetypen abschließend gestaltet werden. Informationen über den Standort mobiler Geräte sowie Informationen über Internetnutzer sollten nicht mehr gesammelt werden.

B. Identifizierungszwang

1. Identifizierbarkeit und Bürgerrechte

> *„2.B.1. What has been the effect, if any, on civil liberties of measures taken at national level to increase the traceability of users of communication devices? Please provide examples of these effects as well as indications of the size of their impact.“*

Seit 2004 dürfen **in Deutschland** Rufnummern für eingehende Verbindungen nur noch nach Erhebung von Name, Anschrift und Geburtsdatum vom Anschlussinhaber freigeschaltet werden. Dies ist insbesondere für vorausbezahlte und kostenfreie Dienste von Bedeutung, namentlich für Prepaid-Handykarten. Der Anbieter ist zu einer Überprüfung der Angaben nicht verpflichtet. Die Angaben werden zusammen mit der zugewiesenen Rufnummer über 1.000 öffentlichen Stellen[58] in einem Onlineverfahren zum unmittelbaren Abruf zur Verfügung gestellt einschließlich einer Jokersuche nach beliebigen Kriterien. 2008 wurden auch E-Mail-Anbieter und deren Kundenverzeichnisse in das Verfahren aufgenommen. Seither sind die Kundendaten von 120 Anbietern zugänglich.[59] Die Zahl der Zugriffe steigt von Jahr zu Jahr rasant an. Inzwischen wird jährlich über 4 Mio. mal auf die Kundendaten zugegriffen – ohne Eingriffsschwelle und richterliche Kontrolle.[60]

Dieser Identifizierungszwang führt bei dem Normalbürger dazu, dass ihm eine **anonyme Telekommunikation erschwert** oder unmöglich gemacht wird. Dies hat zum Teil gravierende Folgen, wie bereits oben zur Vorratsdatenspeicherung ausgeführt worden ist. Diese Ausführungen gelten hier entsprechend. Insbesondere ist darauf hinzuweisen, dass der einzige Umstand, der das Gewicht der Verkehrsdatenspeicherung mindert, die Möglichkeiten anonymer Kommunikation – etwa mithilfe vorausbezahlter Handykarten – sind. Diese ermöglichen es, trotz Verbindungsdatenspeicherung noch mehr oder weniger anonym zu kommunizieren. Würde auch diese von der Richtlinie voraus gesetzte Möglichkeit beseitigt, würde dies die Auswirkungen der Totalprotokollierung nochmals gravierend verschärfen.

Die fehlende Anonymität der Fernkommunikation wegen der Vorhaltung von Vertragsdaten bei einem Mittelsmann **beeinträchtigt die Bereitschaft zur vertraulichen Kommunikation** auf elektronischem Wege, weil man gegebenenfalls Nachteile infolge der eigenen Verbindungen, Aussagen, Bewegungen oder Interessen befürchten muss. Der Erläuternde Bericht zur Empfehlung des Europarats zum Datenschutz in der Telekommunikation[61] führt in Abs. 5 aus, dass die technische Entwicklung „nicht nur die Privatsphäre von Teilnehmern und Nutzern allgemein gefährden kann, sondern auch deren Kommunikationsfreiheit behindern kann, weil sie das Maß an Anonymität mindert, der sich Teilnehmer und Nutzer unter Umständen bei der Benutzung des Telefons bedienen wollen, indem sie gezwungen

58 Bundesnetzagentur, Jahresbericht 2008, http://www.bundesnetzagentur.de/media/archive/15901.pdf, 108.
59 Bundesnetzagentur, Jahresbericht 2008, http://www.bundesnetzagentur.de/media/archive/15901.pdf, 108.
60 Bundesnetzagentur, Jahresbericht 2008, http://www.bundesnetzagentur.de/media/archive/15901.pdf, 108.
61 Empfehlung R (95) 4 vom 07.02.1995.

werden, ihre Identitäten offenzulegen oder elektronische Spuren zu hinterlassen, die es ermöglichen, die Benutzung ihres Telefons zu überwachen."[62]

Dass das **Recht auf anonyme Meinungsäußerung** grundrechtlich geschützt ist, hat der US-amerikanische Oberste Gerichtshof (Supreme Court) schon früh anerkannt. Er hat in der Entscheidung Talley v. California[63] ausgesprochen, dass die „anonyme Meinungsäußerung" eine wertvolle Rolle für den „Fortschritt der Menschheit" gespielt habe. Verfolgte Gruppen seien im Lauf der Geschichte nur im Schutz der Anonymität in der Lage gewesen, Unterdrückungspraktiken und -gesetze zu kritisieren. Auch könne eine „Identifizierung und die Furcht vor Vergeltung von vollkommen friedlichen Diskussionen wichtiger öffentlicher Angelegenheiten abschrecken". Eine Pflicht zur Nennung der Verantwortlichen auf Flugzetteln hat der Gerichtshof daher als Verstoß gegen die Meinungsfreiheit verworfen. In einer späteren Entscheidung[64] 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.[65] Es müsse möglich bleiben, anonym Mitglied eines unbeliebten Vereins zu sein, um die Freiheit auch unpopulärer Meinungen zu gewährleisten. Zuletzt haben die US-amerikanischen Instanzgerichte das Recht auf Anonymität auch auf das Internet angewandt. Der Washington District Court entschied 2001,[66] das Recht auf anonyme Meinungsäußerung sei von grundlegender Bedeutung für die Verabschiedung der US-amerikanischen Verfassung selbst gewesen, weil sowohl Befürworter („Federalist Papers") wie auch Widersacher ohne Namensnennung über die Ratifizierung der Verfassung stritten. Das Gericht entschied wörtlich: „Das Internet begünstigt den reichhaltigen, vielfältigen und weitreichenden Austausch von Ideen. Die Möglichkeit, seine Meinung im Internet äußern zu können, ohne dass die andere Seite alle Tatsachen über die eigene Identität kennt, kann offene Kommunikation und robuste Debatte fördern."[67] Auch **in Deutschland** haben sich die politische Opposition und der Widerstand gegen die Obrigkeit immer wieder der Anonymität bedienen müssen. Berühmte Schriftsteller wie Erich Kästner oder Kurt Tucholsky schrieben nicht unter ihrem eigenen Namen. 1849 veröffentlichte der Rechtswissenschaftler Theodor Mommsen einen Kommentar über die in der neuen Verfassung von 1848 garantierten „Grundrechte des deutschen Volkes" – anonym. Im gleichen Jahr veröffentlichte Adolph Streckfuß sein Werk „Das freie Preußen. Geschichte des Berliner Freiheitskampfes vom 18. März 1848 und seine Folgen", ohne seinen Namen zu nennen.

Die Möglichkeit, sich anonym informieren und kommunizieren zu können, ist **für viele Menschen unverzichtbar**:

62 https://wcd.coe.int/ViewDoc.jsp?id=529277&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&-BackColorLogged=FFAC75.
63 362 U.S. 60 (1960).
64 McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995).
65 NAACP v. Alabama ex. rel. Patterson, 357 U.S. 449 (1958).
66 Doe v. 2TheMart.com, 140 F.Supp.2d 1088.
67 Doe v. 2TheMart.com, 140 F.Supp.2d 1088.

- Menschen in besonderen Situationen (z.B. **Notlagen**, Krankheiten) sind nur in vollständiger Anonymität bereit, Informationen und Hilfe zu suchen, sich untereinander auszutauschen und sich beraten zu lassen (z.B. Chatrooms für Opfer sexuellen Missbrauchs).
- **Unternehmen** kommunizieren anonym, um Wirtschaftsspionage im Zusammenhang mit Vertragsverhandlungen zu verhindern, aber auch um sich selbst bei Wettbewerbern zu informieren, ohne ihre Identität preisgeben zu müssen.
- **Regierungsbehörden** (z.B. Nachrichtendienste) kommunizieren anonym, um im Internet recherchieren zu können, ohne als Regierungsbehörde identifizierbar zu sein. Zugleich sind sie darauf angewiesen, dass Menschen Straftaten anonym anzeigen können, die andernfalls nicht gemeldet würden und unaufgeklärt blieben. Dies gilt für die anonyme Offenlegung verschiedenster Missstände wie Steuerhinterziehung oder Korruption (sogenanntes „Whistleblowing").
- Nur anonyme Telekommunikation erlaubt es der **Bevölkerung autoritärer Staaten**, sich über politische Nachrichten zu informieren, die in ihrem eigenen Land durch Zensurmaßnahmen gesperrt sind.
- Deutsche **Journalisten**, die in autoritären Staaten arbeiten, sind auf anonyme Fernkommunikation angewiesen, um Informationen sicher empfangen und nach Deutschland übermitteln zu können, ohne dass der Aufenthaltsstaat dies zum Anlass für Maßnahmen gegen sie nehmen kann. Auch im Inland sind Informanten zunehmend nur noch im Schutz der Anonymität bereit, Auskunft zu geben. Im Wege anonymer Kommunikation gelingt es dann nicht selten, gravierende Missstände an das Licht der Öffentlichkeit zu bringen.
- Deutsche **Menschenrechtsgruppen** brauchen anonyme Kommunikationstechnik für ihre Arbeit mit autoritären ausländischen Staaten, sei es, um von diesen Staaten aus unerkannt mit ihrem Heimatbüro zu kommunizieren, sei es, um unerkannt mit oppositionellen Gruppen in den entsprechenden Staaten in Verbindung zu treten. Eine offene Kommunikation ist hier regelmäßig mit einem nicht zu verantwortenden Sicherheitsrisiko für die Beteiligten verbunden.
- **Regierungskritiker**, Blogger, Journalisten und Oppositionelle in autoritären ausländischen Staaten (z.B. Iran, Burma, Tibet), die sich für demokratische Reformen in ihrem Land einsetzen, können nur mithilfe anonymer Netze untereinander kommunizieren und die Öffentlichkeit auf die Situation in ihrem Land aufmerksam machen. Ohne den Schutz der Anonymität sind sie Verhaftungen, Gefängnisstrafen und Folter ausgesetzt; anonyme Fernkommunikation schützt also Leben und Freiheit dieser Personen. Beispielsweise in Burma ist die demokratische Opposition auf die anonyme Kommunikation per Internet angewiesen.

Gary Marx nennt insgesamt 15 **Funktionen von Anonymität in unserer Gesellschaft**:[68]

1. Erleichterung des Informations- und Kommunikationsflusses über **öffentliche Angelegenheiten** durch Schutz des Informationsgebers (z.B. Hotlines zur anonymen Anzeige von Problemen oder Verstößen durch Whistle Blower, anonyme Informanten der Presse).

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

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

Ersetzt der Staat den **Grundsatz der Anonymität und Datensparsamkeit** durch einen Zwang zur Identifizierung und Datensammlung, hat dies dementsprechend gravierende Auswirkungen.

So verkaufte im Jahr 2006 ein Mitarbeiter des deutschen Mobilfunkunternehmens **T-Mobile** die Daten sämtlicher 17 Mio. Prepaid- und Postpaid-Kunden des Mobilfunkunternehmens. Die Daten umfassen den Namen, die Mobilfunknummer, die Anschrift, teils das Geburtsdatum und in einigen Fällen auch die E-Mail-Adresse. Die Daten werden in kriminellen Kreisen gehandelt. 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 musste nach dem Bekanntwerden eine Gefährdungsanalyse erstellen, um Betroffene schützen zu können.[69] Hätte T-Mobile nicht die Identität aller Kunden erhoben, wären weit weniger Personen gefährdet worden.

Der massiven Abschreckungswirkung sowie dem Risiko von Pannen und Missbrauch steht **kein nachweisbarer Nutzen** auf Seiten der staatlichen Ermittlungsbehörden gegenüber. Vielmehr berichten deren Vertreter, dass bei Ermittlungen im Bereich ernsthafter Kriminalität praktisch nie eine Handykarte auf den Nutzer registriert sei. Handykarten werden trotz Identifizierungspflicht mit Fantasiedaten angemeldet, von anderen Personen übernommen oder identifizierungsfrei außerhalb Deutschlands gekauft.

Eine Umfrage unter über 100.000 Internetnutzern im Jahr 2009[70] hat ergeben, dass jeder vierte Internet-Nutzer zum Schutz seiner Daten immer oder vorwiegend unter Fantasienamen im Netz unterwegs ist. Jeder fünfte Internetnutzer macht **Fantasieangaben** bei Online-Registrierungen. Fantasieangaben werden aus den folgenden Gründen gemacht:

- 66% wollen auf diese Weise die Zusendung **unerwünschter Werbung** verhindern.
- 62% wollen auf diese Weise einen **Verkauf ihrer Daten** verhindern.
- 58% wollen auf diese Weise ein Internetangebot **anonym nutzen**.
- 53% wollen sich dagegen wehren, dass **unangemessen viele Daten abgefragt** werden.
- 41% wollen im Internet **überall anonym** bleiben.

Wenngleich sich die Umfrage nicht auf **Telekommunikationsangebote** bezieht, ist zu vermuten, dass ebenso viele Menschen bei der Registrierung von Handy-SIM-Karten oder von E-Mail-Diensten Fantasieangaben machen wie bei der Registrierung von Internetdiensten.

Speziell zu Handy-SIM-Karten heißt es in einem Papier des **Bundeswirtschaftsministeriums** aus dem Jahr 2002:

---

69 Spiegel, Diebe klauten 17 Millionen T-Mobile-Kundendatensätze (04.10.2008), http://www.spiegel.de/wirtschaft/0,1518,581938,00.html.

70 http://www.w3b.org/nutzerverhalten/furcht-vor-datenmissbrauch-beeinflusst-nutzerverhalten.html.

> *„Derzeit werden Prepaid-Karten von Straftätern **häufig unter Angabe falscher bzw. fiktiver Personalien** oder unter dem Namen der Vertriebspartner (Händler) erworben und registriert, oder es werden nicht existente Anschriften angegeben. [...] Außerdem kommt es wegen der zum Teil falschen Angabe von Personalien unbeteiligter Dritter immer wieder zu [...] Ermittlungsmaßnahmen gegen Unschuldige. [...] Regelmäßig kommt es auch zu Schwierigkeiten bei der Telekommunikationsüberwachung (z.B. nach § 100a StPO), denn dort sind Anschlussinhaberfeststellungen von entscheidender Bedeutung. [...] Gegenwärtig sind lediglich in Frankreich die Anbieter von Prepaid-Karten verpflichtet, Kundendaten zu erheben. Es kommt vor, dass trotz Vorgaben von Regierungsseite völlig unzutreffende Angaben gemacht werden. In den anderen EU-Staaten, aus denen Informationen vorliegen, gibt es keine gesetzlichen Regelungen, die bei dem Verkauf von Prepaid-Karten zu beachten sind. [...] Etwa 50 % der Karten werde innerhalb eines Jahres verschenkt, größtenteils innerhalb der Familie."*[71]

Die in diesem Papier beschriebene Situation hat sich jedenfalls in den Kreisen, die für den Bereich ernsthafter Kriminalität von Interesse sind, durch die deutsche Identifizierungspflicht **nicht geändert**. Selbst die Bundesregierung schätzt, dass 10% der Bestandsdaten von Prepaidkunden gegenwärtig nicht korrekt sind.[72] Es ist nicht ersichtlich, dass die Identifizierungspflicht die Datenlage verbessert hätte. Erst recht nicht hat sie eine Erhöhung der Aufklärungsquote oder gar Senkung der Kriminalitätsrate bewirkt.

Ein Identifizierungszwang bewirkt im Ergebnis somit keine empirisch feststellbare, statistisch relevante Verbesserung der Strafverfolgung oder gar der Sicherheit. Berücksichtigt man demgegenüber die schweren Nachteile eines Identifizierungszwangs, so ergibt sich, **dass die Kommission keinesfalls die Einführung eines Identifizierungszwangs befürworten** oder gar vorschlagen darf. Dementsprechend sieht weder die Cybercrime-Konvention des Europarats noch die Richtlinie zur Vorratsdatenspeicherung einen Identifizierungszwang vor.

Abschließend ist darauf hinzuweisen, dass eine **Entscheidung des Bundesverfassungsgerichts** über die Vereinbarkeit eines allgemeinen Identifizierungszwangs von Telekommunikationsnutzern mit dem Verhältnismäßigkeitsgebot ansteht.[73] Bevor die Vereinbarkeit einer solchen Maßnahme mit den Grundrechten nicht geklärt ist, sollte die Europäische Kommission in keinem Fall einen entsprechenden Vorstoß befürworten, will sie nicht Gefahr laufen, dass das Bundesverfassungsgericht einen europäischen Identifizierungszwang für in Deutschland unanwendbar weil mit dem Grundgesetz unvereinbar erklärt.[74]

Empfehlung: Die Kommission darf keinesfalls die Einführung eines Identifizierungszwangs befürworten oder gar vorschlagen.

---

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

72 Bevollmächtigter der Bundesregierung, Schriftsatz vom 31.01.2007 an das Bundesverfassungsgericht, http://daten-speicherung.de/data/TKG-StN.pdf, 61.

73 Bundesverfassungsgericht, Erledigungskalender 2009, http://www.bundesverfassungsgericht.de/organisation/erledigungen_2009.html, Az. 1 BvR 1299/05.

74 Vgl. BVerfG, 2 BvE 2/08 vom 30.6.2009, http://www.bverfg.de/entscheidungen/es20090630_2bve000208.html.

2. Maßnahmen zur Begrenzung der nachteiligen Auswirkungen

> *„2.B.2. Which additional measures (administrative, technical, legal, or other) should be taken for the offset of negative impacts, if any?“*

Empfehlung: Die Europäische Kommission sollte den Mitgliedsstaaten im Bewusstsein ihrer Verantwortung vor den Bürgern und deren Grundrechten empfehlen, von einem unverhältnismäßigen allgemeinen Identifizierungszwang zugunsten gezielter Identifizierungsmaßnahmen im Verdachtsfall abzusehen. Diese Balance zwischen Bürgern und Staat, die im Bereich mündlicher und schriftlicher Kommunikation schon immer bestanden hat, muss auch im Zeitalter der Informationsgesellschaft bewahrt werden. Zugleich sollte die Europäische Union die grenzüberschreitende Erbringung anonymer Dienstleistungen erleichtern und fördern.

3. Handlungsbedarf auf EU-Ebene

> *„2.B.3. Which ones of these measures should be addressed at the level of the European Union?“*

Empfehlung: Die Europäische Union sollte von Vorschlägen zur Einführung eines Identifizierungszwangs absehen, weil ein Identifizierungszwang einen unverhältnismäßig geringen Nutzen bei unverhältnismäßig großen Nachteilen hätte. Stattdessen sollte die Europäische Union die grenzüberschreitende Erbringung anonymer Dienstleistungen erleichtern und fördern.

C. Weiteres

1. Vereinheitlichung des Datenformats

Wir erlauben uns abschließend **Bemerkungen** zu einzelnen Fragen, die leider nur an die Mitgliedsstaaten gerichtet wurden:

> *„1.A.1.f.2 Did your country standardise or seeking to standardise the format for the acquisition and disclosure of communications data between public authorities and communications service providers (for instance in service level agreements, or by making reference to relevant ETSI standards)? If so, please provide information about the standard (form or format) for requests, the message format, the technical modalities and/or interface.“*

Wir entnehmen dieser Frage, dass die Europäische Kommission erwägt, Anbietern künftig die **Speicherung und Übermittlung von Verkehrsdaten in einem einheitlichen Format** aufzuerlegen.

Diese Überlegung lehnen wir ab, weil die Standardisierung von Auskünften sogenanntes „**Data Mining**“ in weitem Umfang ermöglicht und erleichtert. In einigen Staaten stellen Behörden bereits heute Telekommunikations-Verkehrsdaten in große Datenbanken ein („Datawarehouse“), um sie automatisiert analysieren zu können. Kommerziell erhältliche Software etwa der Firma „Harlequin“ ermöglicht es, verfahrensübergreifend Kommunikationsdaten auf vermeintliche Verbindungen oder Auffälligkeiten zu analysieren sowie Kommunikationsnetzwerke grafisch offenzulegen. Diese Verfahren entfernen sich von dem rechtsstaatlichen Leitbild einer gezielten Ermittlung in konkreten Verfahren mit anschließender Löschung der nicht mehr benötigten Daten. Sie führen in Richtung der amerikanischen Praxis, gigantische Datenbanken mit personenbezogenen Daten über Jahrzehnte hinweg aufzubauen, um sie automatisiert durchsuchen und Verdachtsmomente schöpfen zu können. Gerade Telekommunikationsdaten betreffen überwiegend unverdächtige Personen, nämlich unbeteiligte Gesprächspartner.

In vielen Fällen wird das „Mining“ von Telekommunikationsdaten bisher dadurch ausgeschlossen, dass **Auskünfte meist in Papierform** und von Anbieter zu Anbieter in unterschiedlicher Aufbereitung erteilt werden. Dabei muss es bleiben, denn diese praktischen Sicherungen machen – effektiver als rechtliche Regelungen – eine breite Telekommunikationsdurchleuchtung von vornherein unmöglich. Eine internationale Verpflichtung zur Standardisierung von Auskünften besteht nicht und darf auch nicht begründet werden.

Empfehlung: Die Europäische Kommission sollte nicht vorschlagen, Anbietern künftig die Speicherung und Übermittlung von Verkehrsdaten in einem einheitlichen Format aufzuerlegen.

2. Wirksamkeit der Vorratsdatenspeicherung

„1.A.1.j Effectiveness - What is the success rate of the use of retained data"

Die unter diesem Punkt gestellten Fragen sollen dazu dienen, die **Effektivität der Vorratsdatenspeicherung** zu bewerten. Die Kommission läuft mit ihren Fragen Gefahr, subjektiv empfundene Nützlichkeit unzulässig mit objektiv nachweisbarer Wirksamkeit gleichzusetzen.

Effektiv kann die Vorratsdatenspeicherung nur genannt werden, wenn von unabhängiger Seite anhand aussagekräftiger, repräsentativer Daten nachgewiesen würde, dass sie die **Kriminalitätsrate** senkt oder wenigstens die Aufklärungsrate nicht nur vorübergehend erhöht. Entsprechende Untersuchungen fehlen und werden leider auch von der Kommission nicht angestrebt. Wenn die Richtlinie zur Vorratsdatenspeicherung nicht insgesamt aufgehoben wird, sind die Art. 10 und 14 dahin zu ändern, dass eine Untersuchung der genannten Fragen erfolgen kann und erfolgt.

Die **Abrufstatistiken** nach dem bisherigen Art. 10 lassen 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 die Erheblichkeit der Vorratsdaten für den Verfahrensausgang nicht erfasst wird. Aussagekräftig ist einzig die im Februar 2008 vorgelegte Untersuchung des unabhängigen Max-Planck-Instituts, der zufolge den Strafverfolgern nur in 0,01% aller Verfahren Verbindungsdaten fehlen.[75]

Der **Behauptung, ohne Vorratsdatenspeicherung sei die Aufklärung von Straftaten gefährdet**, ist entgegen zu halten:

- **Nützlichkeit ist nicht gleich Sicherheit.** Mehr Daten mögen in Einzelfällen nützlich sein. Im Ergebnis ist in Staaten mit Vorratsdatenspeicherung jedoch keine geringere Kriminalitätsrate zu verzeichnen als in Staaten ohne Vorratsdatenspeicherung. Insgesamt gesehen gibt es mit Vorratsdatenspeicherung nicht weniger Kindesmissbrauch, Vergewaltigungen, Körperverletzungen oder sonstige Straftaten als ohne Vorratsdatenspeicherung. Die Vorratsdatenspeicherung stärkt daher nicht unsere Sicherheit.
- **Aufklärung ist nicht gleich Schutz.** Es ist nicht nachweisbar, dass eine erleichterte Aufklärung von Straftaten irgend einen Einfluss auf die Kriminalitätsrate hat. Die Vorratsdatenspeicherung schützt uns daher nicht.
- **Arbeitserleichterung ist nicht gleich Erforderlichkeit.** Weltweit werden Straftaten auch ohne Vorratsdatenspeicherung erfolgreich aufgeklärt, gerade im Internet: Laut Bundeskriminalamt wurden 2007 ohne Vorratsdatenspeicherung 84,4% aller registrierten Internetdelikte einschließlich der Verbreitung von Kinderpornografie erfolgreich aufgeklärt – von den sonstigen Straftaten nur 55%.[76]
- **Einzelfallbetrachtung ist nicht gleich Verhältnismäßigkeit.** Aus einer Studie des Max-Planck-Instituts ergibt sich, dass die Vorratsdatenspeiche-

75 Näher der Schriftsatz der Beschwerdeführer an das Bundesverfassungsgericht vom 17.03.2008, http://www.vorratsdatenspeicherung.de/images/schriftsatz_2008-03-17.pdf, 1 ff.

76 Bundeskriminalamt, Kriminalstatistik 2007, http://www.bka.de/pks/pks2007/download/pks-jb_2007_bka.pdf, 65 und 243.

rung im besten Fall bei 0,01% aller Straftaten von Nutzen sein kann[77] – zu 99,99% wird sinnlos aufgezeichnet.

- **Massenverfolgung ist nicht gleich Effizienz.** Mithilfe von Telekommunikationsdaten werden hauptsächlich Betrügereien und Tauschbörsennutzer ermittelt.[78] Diese massenhafte Verfolgung von Kleinkriminalität kostet die Polizei Ressourcen, die bei der Ermittlung schwerer Straftäter und der Hintermänner fehlen. In den letzten Jahren sind bei der deutschen Polizei 17.000 Stellen gestrichen worden.[79]
- **Betriebsblindheit ist nicht gleich Klugheit.** In ihrer Jagd auf 0,01% der Straftäter verlieren die Befürworter der Vorratsdatenspeicherung aus den Augen, dass eine unprotokollierte Kommunikation Leben, Gesundheit und Freiheit von weit mehr Unschuldigen schützt, etwa wo Beratungsstellen gewalttätige Familienväter oder Pädophile überzeugen können, sich einer Therapie zu unterziehen. Im Jahr 2007 konnte beispielsweise ein bei der Telefonseelsorge tätiger Pfarrer einen Jugendlichen überzeugen, einen geplanten Amoklauf zu unterlassen. Wäre der Anruf rückverfolgbar gewesen, hätte der Jugendliche wohl nie über sein Vorhaben gesprochen. Einer Forsa-Umfrage vom Juni 2008 zufolge hält die Vorratsdatenspeicherung gegenwärtig jeden zweiten Deutschen davon ab, sich telefonisch beraten zu lassen.[80]
- **Telekommunikation ist nicht gleich Straftat.** Telefon, Handy und Internet werden zu 99,9% vollkommen legal eingesetzt. Gespräche müssen am Telefon ebenso wenig registriert werden wie sonstige Gespräche. Briefe müssen im Internet ebenso wenig registriert werden wie sonstige Briefe. Bewegungen müssen mit einem Handy ebenso wenig registriert werden wie sonstige Bewegungen.
- **Gefährdung ist nicht gleich Kriminalität.** Was Straftaten anbelangt, ist Europa eine der sichersten Regionen der Welt. Tod, Krankheit oder Behinderung beruhen bei uns nur zu 0,2% auf Gewalt und Straftaten.[81] Dagegen kosten Tabak, Alkohol, Cholesterin, Übergewicht, Fehlernäherung, Bewegungsmangel, Suizid, Stürze und der Straßenverkehr ein Vielfaches an Menschenleben – obwohl sie sehr viel leichter zu reduzieren wären.
- **Überwachung ist nicht gleich Sicherheit.** Umgekehrt ermöglichen Datenhalden erst Missbrauch wie bei der Deutschen Telekom AG und Betrug wie im Fall der Bankdaten. Nur nicht gespeicherte Daten sind sichere Daten. Die Vorratsdatenspeicherung stellt diese Erkenntnis auf den Kopf.
- **Freiheit ist nicht gleich Unsicherheit.** Es ist kein Zufall, dass Bürger in Staaten mit vergleichsweise wenig Überwachung und starkem Grundrechtsschutz sicherer leben als Kontrollstaaten wie Großbritannien oder die USA. Sicherheit braucht in erster Linie Vertrauen und Achtung vor dem Recht – auch vor den Grundrechten. Die verdachtslose Vorratsdatenspeicherung er-

77 Näher der Schriftsatz der Beschwerdeführer an das Bundesverfassungsgericht vom 17.03.2008, http://www.vorratsdatenspeicherung.de/images/schriftsatz_2008-03-17.pdf, 1 ff.
78 Näher die Beschwerdeschrift an das Bundesverfassungsgericht vom 31.12.2007, http://wiki.vorratsdatenspeicherung.de/images/Verfassungsbeschwerde_Vorratsdatenspeicherung.pdf, 36.
79 Gewerkschaft der Polizei, Skandalöser Stellenabbau bei der Polizei setzt Sicherheit Deutschlands aufs Spiel (29.06.2007), http://www.gdp.de/gdp/gdpcms.nsf/id/p70606?Open&ccm=500020000&L=DE&markedcolor=%23003399.
80 http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf.
81 http://www.daten-speicherung.de/?p=57.

klärt dagegen erstmals die gesamte deutsche Bevölkerung zu potenziellen Straftätern und bricht damit unsere im Grundgesetz verbürgten Rechte.

Empfehlung: Die Kommission sollte vorschlagen, die Art. 10, 14 der Richtlinie 2006/24 dahin zu ändern, dass eine aussagekräftige, unabhängige Untersuchung der Wirksamkeit der Vorratsdatenspeicherung gemessen an Aufklärung und Verhütung von Straftaten in Auftrag zu geben ist. Unabhängig davon sollte sie in eigener Initiative eine entsprechende Untersuchung in Auftrag geben. Bei der Auswertung der Antworten der Mitgliedsstaaten und dem Verfassen des Evaluierungsberichts sollte die Kommission angeben, dass eine echte Prüfung der Wirksamkeit aus den genannten Gründen bislang nicht erfolgt ist.

3. Grenzüberschreitender Zugriff auf Kommunikationsinformationen

„1.A.2 National and transnational requests and answers“

Obwohl diese Frage nur die innereuropäische Weitergabe von Verkehrsdaten betrifft, möchten wir die Kommission darauf aufmerksam machen, dass die sogenannte **Cybercrime-Konvention des Europarats** die Europäische Menschenrechtskonvention verletzt, weil sie für den weiteren Umgang mit den ausgelieferten Informationen im Ausland keinerlei angemessenes Schutzniveau vorsieht:

- Das **Verhältnismäßigkeitsgebot** ist verletzt:
    - Ein Ersuchen setzt nach dem Abkommen nur ein „strafrechtliches Verfahren“ voraus, ohne dass eine materielle Eingriffsschwelle besteht. Es wird **kein Anfangsverdacht** voraus gesetzt. Es ist auch nicht gewährleistet, dass das innerstaatliche Recht aller Vertragsparteien strafrechtliche Ermittlungsverfahren an den konkreten Verdacht einer bestimmten Straftat knüpft. Die Mitgliedsstaaten können ausländische Ersuchen, die zum Zweck von Initiativermittlungen ins Blaue hinein erfolgen, nicht ablehnen.
    - Es ist nicht festgelegt, dass nur Informationen über Personen angefordert und erhoben werden dürfen, die einer Straftat verdächtig sind. Es gibt auch keine besonderen Voraussetzungen einer Ermittlungsmaßnahme **gegen unverdächtige und unschuldige Dritte**.
    - Es ist nicht festgelegt, dass nur solche Informationen erhoben werden dürfen, die zur Aufklärung des Tatvorwurfs **geeignet** sind.
    - Es ist nicht festgelegt, dass zunächst **minder eingreifende Maßnahmen** auszuschöpfen sind.
    - Es ist nicht festgelegt, dass die Maßnahme nicht **außer Verhältnis** zu dem verfolgten Zweck stehen darf.
    - Es fehlen jegliche Vorkehrungen zum Schutz von Informationen, die den **Kernbereich privater Lebensgestaltung oder besondere Vertrauensverhältnisse** betreffen. Ersuchen auf Sicherung solcher Informationen können nach dem Übereinkommen nicht abgelehnt werden. Gleiches gilt für sonst besonders sensible (Computer-) Daten, aus de-

nen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben.

- Von den Computerdaten nimmt das Abkommen auch von staatlichen Stellen gespeicherte Daten nicht aus, die von **Amtsgeheimnissen besonders geschützt** sind (z.B. Sozialgeheimnis, Steuergeheimnis).
- Es **fehlt jegliche qualifizierte Eingriffsschwelle**, soweit Ersuchen Informationen über den grundrechtlich besonders geschützten Fernmeldeverkehr zum Gegenstand haben (Telekommunikationsverbindungen, Standortdaten, gespeicherte Telekommunikationsinhalte). Ein Zugriff auf solche Informationen ist nach dem Grundgesetz nur ausnahmsweise zur Verfolgung schwerer Straftaten verhältnismäßig. Das Abkommen erlaubt es aber nicht, Ersuchen zu verweigern, die wegen geringfügiger Straftaten oder eines bloß entfernten Verdachts oder einer fehlenden Nähebeziehung des Betroffenen oder einer geringen Beweiseignung auf vom Fernmeldegeheimnis geschützte Informationen zugreifen wollen. Das Abkommen zwingt insoweit nicht nur zur Sicherung von Verkehrsdaten, sondern nach Art. 30 CCC unter Umständen auch zu ihrer Herausgabe an ausländische Behörden, und zwar ohne Ablehnungsmöglichkeit und ohne Vorbehalt entgegen stehenden innerstaatlichen Rechts.
- Das Abkommen sieht nicht vor, dass die Entscheidung über die Erledigung eingehender Ersuchen den **Gerichten** obliegt. Die etwa nach deutschem Recht zuständigen Gerichte dürfen Ersuchen nach den Art. 29, 30 CCC daher nicht ablehnen.

- Das Abkommen beschränkt die **Verwendung übermittelter Daten** nicht auf das Verfahren, in welchem die Anfrage erfolgte. Es schreibt nicht vor, dass die Daten spätestens mit Abschluss des Verfahrens zu löschen sind.
- Das Abkommen sieht keinen **Auskunfts- und Berichtigungsanspruch** der Betroffenen vor.
- Das Abkommen sieht keine **unabhängige Aufsicht** über die Datenvereinbarung vor.
- Das Abkommen gewährleistet nicht den **Rechtsweg**, damit Betroffene ihre Rechte einklagen und gegen Rechtsverletzungen vorgehen können. Der fehlende Rechtsweg etwa in den USA stellt die Betroffenen rechtlos.

Vor dem Bundesverfassungsgericht ist gegenwärtig eine **Verfassungsbeschwerde** gegen das Abkommen anhängig.[82]

Empfehlungen: Die Europäische Kommission sollte ihre Möglichkeiten nutzen, um eine Nachbesserung der Cybercrime-Konvention in die Wege zu leiten. Außerdem muss sie die oben genannten Grundrechtsgarantien bei künftigen Abkommen zur Datenauslieferung an Drittstaaten (z.B. SWIFT-Abkommen, Fluggastdatenübermitt-

82 Az. 2 BvR 637/09. Beschwerdeschrift: http://www.daten-speicherung.de/data/Beschwerde_CCC_BVerfG_2009-03-17_anon.pdf.

lung, „High Level Contact Group on data protection and data sharing“) wahren, was bei den bisherigen Abkommen nicht der Fall ist.

4. Zentralisierung der Vorratsspeicher

„1.A.3.a.7 Centralised storage of data by Service providers“

Eine **zentrale Speicherung von Verkehrsdaten** führt auch innerhalb eines Unternehmens dazu, dass von Datenpannen und Missbrauch in Bezug auf einen Speicher mehr Personen betroffen sind als im Fall einer dezentralen Speicherung. In der IT-Sicherheit ist anerkannt, dass eine zentralisierte oder auch nur vernetzte Speicherung aus Sicherheitsgründen zu vermeiden ist. Eine zentrale Speicherung ist daher abzulehnen.

Empfehlung: Die Kommission sollte nicht vorschlagen, Anbieter zur Speicherung der Vorratsdaten in einer zentralen Datenbank zu verpflichten.

5. Kosten-Nutzen-Verhältnis der Vorratsdatenspeicherung

„1.B.1.c Efficiency“

Die unter diesem Punkt gestellten Fragen sollen dazu dienen, die **Effizienz der Vorratsdatenspeicherung** zu bewerten. Die gestellten Fragen scheinen aber nicht geeignet, dieses Ziel zu erreichen.

Ein effizientes Mittel der Strafverfolgung wäre die Vorratsdatenspeicherung nur, wenn die für sie aufgewandten Mittel nicht **an anderer Stelle mehr Sicherheit** bewirken würden. Dazu müssten für die Vorratsdatenspeicherung und für die vielfältigen Alternativen dazu[83] - insbesondere nachgewiesenermaßen wirksame Projekte zur gezielten Kriminalpräventionsarbeit – ermittelt werden, wie viele Straftaten pro Euro sie zu verhindern oder aufzuklären vermögen.

Von einer derartigen, **aussagekräftigen Kosten-Nutzen-Analyse** sind die Fragen der Kommission leider weit entfernt. Sie könnte auch nur wissenschaftlich durch repräsentative Untersuchungen vorgenommen werden.

Empfehlung: Die Kommission sollte vorschlagen, die Art. 10, 14 der Richtlinie 2006/24 dahin zu ändern, dass eine solche Untersuchung in Auftrag zu geben ist. Unabhängig davon sollte sie in eigener Initiative eine entsprechende Untersuchung in Auftrag geben. Bei der Auswertung der Antworten der Mitgliedsstaaten und dem Verfassen des Evaluierungsberichts sollte die Kommission angeben, dass eine echte Prüfung der Effizienz aus den genannten Gründen bislang nicht erfolgt ist.

83 Ausführlich Breyer, Vorratsspeicherung (2005), http://www.vorratsspeicherung.de.vu, 338 ff.

D. Zusammenfassung der Empfehlungen

1. **Die Kommission sollte vorschlagen, die Richtlinie 2006/24/EG zur Vorratsdatenspeicherung aufzuheben.**
2. Falls die Richtlinie 2006/24/EG zur Vorratsdatenspeicherung nicht aufgehoben werden soll, sollte sie so abgeändert werden, dass die Mitgliedsstaaten selbst entscheiden, ob sie Verkehrsdaten auf Vorrat speichern lassen oder nicht (**Opt-out-Recht**).
3. Falls die Richtlinie 2006/24/EG zur Vorratsdatenspeicherung nicht aufgehoben werden soll, sollte die Richtlinie 2002/21/EG in der deutschen Sprachfassung so abgeändert werden, dass **nicht-kommerzielle Anbieter** sicher von der Pflicht zur Vorratsdatenspeicherung ausgenommen sind.
4. Falls die Richtlinie 2006/24/EG zur Vorratsdatenspeicherung nicht aufgehoben werden soll, sollte sie so abgeändert werden, dass alle zur Speicherung verpflichteten Anbieter Anspruch auf **vollen Ersatz ihrer dadurch bedingten Investitions- und Vorhalteaufwendungen** haben.
5. Falls die Richtlinie 2006/24/EG zur Vorratsdatenspeicherung nicht aufgehoben werden soll, sollten diese Richtlinie sowie die Richtlinie 95/46/EG so abgeändert werden, dass höhere Anforderungen an die **Sicherheit der angesammelten Informationen** gestellt werden und die Umsetzung der Maßnahmen zur Datensicherheit verbessert wird. Konkret müssen Vorratsdaten für den Anbieter unlesbar verschlüsselt und auf separaten Systemen gespeichert werden. Sie dürfen nur in verschlüsselter Form übermittelt werden. Ein Verbandsklagerecht für Verbraucher- und Datenschutzverbände muss eingeführt werden. Unternehmen sollten Datenschutzverletzungen ihrer Wettbewerber abmahnen können. Die Hersteller sollten dafür haften, wenn unsichere Produkte zu Datenschutzverletzungen führen. Die datenverarbeitenden Unternehmen sollten verschuldensunabhängig für Datenschutzverletzungen haften, wobei eine pauschale Mindestentschädigungssumme vorgesehen werden sollte. Die Benachteiligung von Verbrauchern, die ihre Datenschutzrechte ausüben, muss untersagt werden. Eine „Stiftung Datentest“, die den Datenschutz bei verschiedenen Anbieter untersucht und bewertet, sollte gegründet werden.
6. Falls die Richtlinie 2006/24/EG zur Vorratsdatenspeicherung nicht aufgehoben werden soll, sollte sie so abgeändert werden, dass sie im Hinblick auf die zur Speicherung verpflichteten Anbieter und die zu speichernden Datentypen **abschließend** ist.
7. Falls die Richtlinie 2006/24/EG zur Vorratsdatenspeicherung nicht aufgehoben werden soll, sollte sie so abgeändert werden, dass der **Standort mobiler Geräte** (z.B. Handys) sowie Informationen über Internetnutzer nicht mehr aufgezeichnet werden.
8. Die Europäische Kommission sollte **keine Vorschläge zur leichteren Identifizierung** von Telekommunikationsnutzern unterbreiten. Die Europäische Kommission sollte stattdessen die grenzüberschreitende Erbringung anonymer Dienstleistungen erleichtern und fördern.

9. Die Europäische Kommission sollte nicht vorschlagen, die Art und Weise der Speicherung und Übermittlung von Verkehrsdaten zu **vereinheitlichen**.
10. Die Kommission sollte nicht vorschlagen, Anbieter zur Speicherung der Vorratsdaten in einer **zentralen Datenbank** zu verpflichten.
11. Falls die Richtlinie 2006/24/EG zur Vorratsdatenspeicherung nicht aufgehoben werden soll, sollten die Art. 10, 14 der Richtlinie dahin geändert werden, dass eine aussagekräftige, **unabhängige Untersuchung der Wirksamkeit und Effizienz** der Vorratsdatenspeicherung gemessen an Aufklärung und Verhütung von Straftaten sowie am Kosten-Nutzen-Verhältnis anderer Maßnahmen in Auftrag zu geben ist. Unabhängig davon sollte die Kommission in eigener Initiative eine entsprechende Untersuchung in Auftrag geben. Bei der Auswertung der Antworten der Mitgliedsstaaten und dem Verfassen des Evaluierungsberichts sollte die Kommission angeben, dass eine echte Prüfung der Wirksamkeit und Effizienz aus den genannten Gründen bislang nicht erfolgt ist.
12. Die Europäische Kommission sollte ihre Möglichkeiten nutzen, um eine Nachbesserung der Cybercrime-Konvention des Europarats in die Wege zu leiten. Außerdem muss sie Grundrechtsgarantien bei künftigen Abkommen zur **Datenauslieferung an Drittstaaten** (z.B. SWIFT-Abkommen, Fluggastdatenübermittlung, „High Level Contact Group on data protection and data sharing“) wahren.

13.11.2009

Arbeitskreis Vorratsdatenspeicherung

Der Arbeitskreis Vorratsdatenspeicherung (AK Vorrat) ist ein deutschlandweiter Zusammenschluss, der sich gegen die ausufernde Überwachung im Allgemeinen und gegen die Vollprotokollierung der Telekommunikation und anderer Verhaltensdaten im Besonderen einsetzt.

Homepage und Kontakt: http://www.vorratsdatenspeicherung.de