[...]

Antrag auf Zulassung als Streithelfer und Streithilfeschriftsatz

[...]

- Antragsteller -

Verfahrensbevollmächtigter: [...].

In den Vorabentscheidungsverfahren mit dem Aktenzeichen C-92/09 (Volker und Markus Schecke) und C-93/09 (Eifert) beantrage ich namens und in Vollmacht des Antragstellers,

den Antragsteller als Streithelfer zuzulassen.

Ich erkläre mich damit einverstanden, dass Zustellungen an mich per E-Mail an die Adresse [...] erfolgen.

Inhaltsverzeichnis

I. Zulässigkeit des Antrags

1. **Statthaftigkeit des Beitritts**

2. Ein Beitritt als Streithelfer ist in einem Vorabentscheidungsverfahren möglich. Nach Art. 40 der Satzung und Art. 93 der Verfahrensordnung des Gerichtshofes der Europäischen Gemeinschaften (EuGH) kann nach Veröffentlichung einer Verfahrensnachricht im Amtsblatt einen Antrag auf Zulassung als Streithelfer stellen, wer ein berechtigtes Interesse an dem Ausgang des Verfahrens glaubhaft machen kann.

3. Vorabentscheidungsverfahren sind von Art. 40 der Satzung nicht ausgenommen. Die Bestimmung nimmt nur „Rechtsstreitigkeiten zwischen Mitgliedstaaten, zwischen Gemeinschaftsorganen oder zwischen Mitgliedstaaten und Gemeinschaftsorganen“ aus, wie sie hier nicht vorliegen. In anderen Fällen muss im Umkehrschluss ein Beitritt zulässig sein.

4. Bei dem Gerichtshof ist auch ein „Rechtsstreit“ im Sinne von Art. 40 der Satzung „anhängig“, und zwar das Ausgangsverfahren zwischen den Klägern und dem Land Hessen.

5. Sähe man dies anders, wäre Art. 40 in Vorabentscheidungsverfahren jedenfalls analog anzuwenden. Nach Art. 103 § 1 VFO finden auf das Verfahren nach Art. 234 EG die Bestimmungen der Verfahrensordnung unter Berücksichtigung der Eigenart der Vorabentscheidungsvorlage entsprechende Anwendung. Zu den anzuwendenden Bestimmungen der Verfahrensordnung zählt auch Art. 93 VFO [Streithilfe].

6. In der Vergangenheit hat der Gerichtshof in Vorabentscheidungsersuchen vor allem als Streithelfer zugelassen, wer schon an dem Ausgangsverfahren beteiligt oder von dem vorlegenden Gericht als Streithelfer zugelassen worden war.[1] Ist danach anerkannt, dass in Verfahren nach Art. 234 EG Streithilfe grundsätzlich möglich ist, so spricht nichts gegen einen Beitritt erst vor dem EuGH. Insoweit ist auch zu beachten, dass der Antragsteller von den Ausgangsverfahren vor dem Verwaltungsgericht Wiesbaden erst durch die Veröffentlichung der Vorlagebeschlüsse dieses Gerichts erfahren hat und erfahren konnte. Ein Beitritt zu den Ausgangsverfahren ist dem Antragsteller wegen der Aussetzung der Verfahren nicht mehr möglich.

7. Die Zulassung des Antragstellers als Streithelfer der Kläger vor dem EuGH ist auch grundrechtlich geboten. Als allgemeiner Grundsatz des Gemeinschaftsrechts ist anerkannt, dass jeder Bürger Anspruch auf rechtliches Gehör hat, bevor über einen Eingriff in seine Grundrechte entschieden wird (vgl. Art. 6 (1) EMRK). Wie im Einzelnen noch auszuführen sein wird, greift die Richtlinie 2006/24/EG tief in die Grundrechte des Antragstellers auf Achtung seiner Privatsphäre und Meinungsfreiheit (vgl. Art. 8 und 10 EMRK) ein. Der EG-Vertrag sieht keinen direkten Rechtsweg zum

1 Siehe etwa die Rechtssache C-255/01.

EuGH gegen diesen Grundrechtseingriff vor, sondern erlaubt einzig die Anrufung der nationalen Gerichte, die sodann nach Art. 234 EG gegebenenfalls ein Vorabentscheidungsverfahren einzuleiten haben. Nach der Rechtsprechung des EuGH ist ein Vorabentscheidungsersuchen allerdings unzulässig, wenn der Gerichtshof die Vorlagefrage bereits geklärt hat. Mit Ausnahme des vorliegenden Beitritts hat der Antragsteller daher keine Möglichkeit, die Verletzung seiner Grundrechte durch die Richtlinie 2006/24/EG geltend zu machen, denn nach Entscheidung über die Vereinbarkeit der Richtlinie mit den Gemeinschaftsgrundrechten in den anhängigen Verfahren wird sich der EuGH nicht ein zweites Mal mit der Frage befassen. Würde der EuGH dem Antragsteller die Möglichkeit versagen, vor einer Entscheidung über die Vereinbarkeit der Richtlinie 2006/24/EG mit den Gemeinschaftsgrundrechten gehört zu werden, verletzte er den Anspruch des Antragstellers auf rechtliches Gehör.

8. Art. 13 EMRK gibt jedem Menschen, der in seinen Konventionsrechten verletzt worden ist, ein Recht auf wirksame Beschwerde hiergegen. Anders als mit dem vorliegenden Antrag auf Zulassung als Streithelfer kann der Antragsteller eine wirksame Beschwerde gegen die Richtlinie 2006/24/EG nicht erheben. Wie noch auszuführen sein wird, lehnt es das für den Antragsteller in Deutschland zuständige Bundesverfassungsgericht ab, über die Grundrechtskonformität zwingender europarechtlicher Vorgaben zu entscheiden oder die Frage ihrer Gültigkeit dem EuGH vorzulegen. Außerdem käme eine Vorlage in dem vom Antragsteller in Deutschland eingeleiteten Verfassungsbeschwerdeverfahren zu spät, um dem Antragsteller eine wirksame Beschwerde vor dem EuGH zu ermöglichen, weil der EuGH bereits in den vorliegenden Vorabentscheidungsverfahren über die Vereinbarkeit der Richtlinie 2006/24/EG mit den Grundrechten entscheiden wird.

9. Nach alledem kann der Antragstellers den vorbezeichneten Verfahren als Streithelfer beitreten.

10. **Berechtigtes Interesse des Antragstellers hinsichtlich der Gültigkeit der Richtlinie 2006/24/EG**

Der Antragsteller hat hinsichtlich zweier Vorlagefragen ein berechtigtes Interesse an dem Ausgang des Verfahrens:

11. Der Antragsteller ist erstens daran interessiert, dass der EuGH bei Beantwortung der Vorlagefragen zu 2 die Unvereinbarkeit der Richtlinie 2006/24/EG mit den Gemeinschaftsgrundrechten ausspricht.

12. Der Antragsteller ist [...]

13. Der Antragsteller sieht sich in seinen regierungskritischen Aktivitäten beeinträchtigt, weil nach der Richtlinie 2006/24/EG sein gesamtes Kommunikations-, Bewegungs- und Internetnutzungsverhalten über Monate hinweg für staatliche Stellen nachvollziehbar wird. In Anbetracht einer Reihe von Durchsuchungen und Festnahmen staatskritischer Personen in der Vergangenheit, deren Rechtswidrigkeit oder Unbe-

gründetheit später festgestellt wurde, will sich der Antragsteller nicht darauf verlassen, dass ihn die legale Ausübung seiner Grundrechte vor Nachteilen bewahrt.

14. Infolgedessen hat der Antragsteller vor dem Bundesverfassungsgericht Beschwerde gegen die Umsetzung der Richtlinie 2006/24/EG in Deutschland erhoben.[2] In einstweiligen Anordnungen hat das Bundesverfassungsgericht die Nutzung der anlasslos erfassten Kommunikations-, Bewegungs- und Internetnutzungsdaten beschränkt, dabei aber ausgeführt, dass es die Vereinbarkeit deutscher Gesetze, die der Umsetzung zwingenden Gemeinschaftsrechts dienten, mit den Grundrechten so lange nicht prüfen werde, wie der EuGH ein generell vergleichbares Niveau des Grundrechtsschutzes garantiere wie das Bundesverfassungsgericht.[3] Die Verletzung seiner Grundrechte durch die Vorratsspeicherung kann der Antragsteller mithin nur vor dem EuGH geltend machen.

15. Der EuGH hat in seiner Rechtsprechung bereits anerkannt, dass ein berechtigtes Interesse an dem Ausgang eines anhängigen Verfahrens hat, wer Partei in einem anderen Verfahren ist, dessen Ausgang von der Entscheidung des EuGH abhängt.[4] So liegt es hier im Hinblick auf die vom Antragsteller vor dem Bundesverfassungsgericht erhobene Verfassungsbeschwerde gegen die Vorratsspeicherung seiner Telekommunikationsdaten. Stellt der EuGH im vorliegenden Vorabentscheidungsverfahren die Ungültigkeit der Richtlinie 2006/24/EG fest, wird der Antragsteller auch in dem Verfassungsbeschwerdeverfahren vor dem Bundesverfassungsgericht obsiegen.

16. Aus den genannten Gründen ist offensichtlich, dass der Antragsteller ein rechtliches Interesse am Ausgang des vorliegenden Vorabentscheidungsverfahrens hat, in dem das vorlegende Gericht die vom Antragsteller geteilte Auffassung vertritt und zur Entscheidung des EuGH stellt, wonach die Richtlinie 2006/24/EG mit den Gemeinschaftsgrundrechten der Betroffenen – mithin auch des Antragstellers – unvereinbar sei. Neben dem in der eigenen Person begründeten Interesse des Antragstellers ergibt sich ein Interesse aus seiner Mitgliedschaft im Arbeitskreis Vorratsdatenspeicherung, dessen Ziel es ist, die in der Richtlinie 2006/24/EG angeordnete Vorratsdatenspeicherung zu stoppen und der zu diesem Zweck vielfältige Aktivitäten in Deutschland veranstaltet.

17. **Berechtigtes Interesse hinsichtlich der Aufzeichnung von IP-Adressen**

18. Der Antragsteller ist zweitens daran interessiert, dass der EuGH bei Beantwortung der Vorlagefragen zu 6 ausspricht, dass die Aufzeichnung von IP-Adressen durch den Betreiber eines Internetportals mit der Richtlinie 95/46/EG unvereinbar ist.

---

2 Az. 1 BvR 256/08.

3 BVerfG, Beschluss vom 11.3.2008, Az. 1 BvR 256/08, Abs. 134 ff.

4 EuGH, Beschluss vom 12.01.1993 in der Rechtssache T-29/92, Abs. 20.

19. Der Antragsteller ist [...]. Etliche der von ihm über das Internet genutzten Dienste der Informationsgesellschaft zeichnen auf, welche Internetseiten zu welchem Zeitpunkt unter Verwendung der Kennung (IP-Adresse) des Antragstellers abgerufen wurden, welche Suchwörter zu welchem Zeitpunkt unter Verwendung der IP-Adresse des Antragstellers eingegeben wurden und welche Beiträge zu welchem Zeitpunkt unter Verwendung der IP-Adresse des Antragstellers abgesandt wurden (z.B. Nachrichtenformulare, Blog-Kommentare).

20. Durch die Speicherung der IP-Adresse bei den Diensteanbietern kann nachvollzogen werden, welche Informationen der Antragsteller auf dem jeweiligen Internetportal betrachtet und wofür er sich interessiert. Aus den betrachteten Internetseiten können – je nach Inhalt – unter Umständen auch Rückschlüsse auf seine politische Meinung, Krankheiten, Religion, Gewerkschaftszugehörigkeit usw. abgeleitet werden. Eine Erfassung seines Internet-Nutzungsverhaltens ist nicht nur einer Filmaufzeichnung seines Zeitungslesens oder Fernsehens vergleichbar. Vielmehr können Internet-Nutzungsdaten – anders als Videoaufzeichnungen – maschinell zugeordnet und ausgewertet werden und weisen daher eine besonders „hohe Sensitivität“ auf. Was der Antragsteller im Internet liest, sucht und schreibt, spiegelt seine Persönlichkeit, seine Vorlieben und Schwächen in einmaliger Deutlichkeit wider.

21. In der letzten Zeit musste Deutschland zunehmend Fälle versehentlicher und absichtlicher Veröffentlichung und Zweckentfremdung von Informationen über die Nutzung von Diensten der Informationsgesellschaft erleben. Im Jahr 2008 wurden mehrere Fälle bekannt, in denen persönliche Daten von Internetnutzern offen gelegt und dem Risiko eines Missbrauchs ausgesetzt wurden. 18.000 Personen, die im Internet bei der Anzeigenblatt-Tochter WBV Wochenblatt des Axel Springer Verlages – zum Teil unter Chiffre – Anzeigen aufgegeben hatten, mussten ihre Privatanschrift, E-Mail-Adresse, Handynummer und Kontodaten im Internet wieder finden.[5] Das mit Diskretion werbende Erotikunternehmen Beate Uhse veröffentlichte die E-Mail-Adressen Tausender von Personen, die sich Sexfilme im Internet angesehen hatten.[6] In einem Forum des ZDF-Kinderkanals konnten sich beliebige Personen Klarnamen, Adresse, Telefonnummer und Geburtsdatum aller 1.000 registrierten Kinder verschaffen.[7]

    Diese Vorfälle haben in Erinnerung gerufen, dass nur nicht gespeicherte Daten sichere Daten sind. Auch aus diesem Datensicherheitsrisiko ergibt sich ein rechtliches Interesse des Antragstellers daran, dass sein Internet-Nutzungsverhalten nicht in personenbezogener Form aufgezeichnet wird.

22. Aus den genannten Gründen hat der Antragsteller im Jahr 2007 ein Urteil des Landgerichts Berlin erwirkt, mit dem die Bundesrepublik Deutschland verurteilt wurde,

5 Spiegel 43/2008 vom 20.10.2008, Seite 70.

6 Die Welt vom 04.09.2008: Beate Uhse verschlampt E-Mail-Adressen im Web.

7 Spiegel Online vom 16.10.2008: Kika stellt Daten von Kindern ungeschützt ins Web.

„es künftig zu unterlassen, die nachfolgend aufgelisteten personenbezogenen Daten des Klägers, die im Zusammenhang mit der Nutzung des Internetportals 'http://www.bmj.bund.de' übertragen wurden, über das Ende des jeweiligen Nutzungsvorgangs hinaus zu speichern: a) die Internetprotokolladresse (IP-Adresse) des zugreifenden Hostsystems; b) sofern auch die Internetprotokolladresse (IP-Adresse) des zugreifenden Hostsystems gespeichert wird, den Namen der abgerufenen Datei bzw. Seite, Datum und Uhrzeit des Abrufs, die übertragene Datenmenge sowie die Meldung, ob der Abruf erfolgreich war.“[8] Für den Fall einer Zuwiderhandlung gegen das Urteil hat das Amtsgericht Berlin-Mitte der Bundesrepublik Deutschland ein Ordnungsgeld von bis zu 250.000 Euro, ersatzweise eine bis zu sechsmonatige Inhaftierung von Bundesjustizministerin Brigitte Zypries angedroht.[9]

23. Einige andere Internetportale der Bundesrepublik protokollieren gleichwohl weiterhin die IP-Adressen aller Besucher. [...]

24. Aus alledem ergibt sich, dass der Antragsteller ein berechtigtes Interesse daran hat, dass der EuGH bei Beantwortung der Vorlagefragen zu 6 die Unvereinbarkeit einer Aufzeichnung von IP-Adressen mit der Richtlinie 95/46/EG ausspricht.

25. **Fristwahrung**

Nach Art. 40 der Satzung und Art. 93 der Verfahrensordnung des Gerichtshofes der Europäischen Gemeinschaften (EuGH) kann binnen sechs Wochen nach Veröffentlichung einer Verfahrensnachricht im Amtsblatt einen Antrag auf Zulassung als Streithelfer gestellt werden. Die Rechtssache C-92/09 ist am 06.06.2009 im Amtsblatt veröffentlicht worden,[10] so dass die Sechswochenfrist bis zum 18.07.2009 läuft und mit diesem Schriftsatz gewahrt ist. Die Rechtssache C-93/09 ist am 16.05.2009 im Amtsblatt veröffentlicht worden,[11] so dass die Sechswochenfrist bis zum 27.06.2009 läuft und mit diesem Schriftsatz gewahrt ist.

26. **Ordnungsgemäße Vertretung des Antragstellers**

Streithelfer müssen sich vor dem EuGH vertreten lassen, wobei die Vertretung durch einen Hochschullehrer möglich ist, wenn das nationale Recht dies zulässt (Art. 19 der Satzung). Die deutsche Verwaltungsgerichtsordnung, die auf das Ausgangsverfahren anzuwenden ist, lässt die Vertretung durch einen „*Rechtslehrer an einer deutschen Hochschule im Sinne des Hochschulrahmengesetzes mit Befähigung zum Richteramt*“ zu (§ 67 Abs. 1 S. 1 VwGO). Der Bevollmächtigte des Antragstellers im vorliegenden Verfahren ist Rechtslehrer an einer deutschen Hochschule – der Universität [...] – im Sinne des Hochschulrahmengesetzes mit Befähigung zum Richteramt. Er kann den Antragsteller somit im vorliegenden Verfahren vertreten.

8 Landgericht Berlin, Urteil vom 06.09.2007, Az. 23 S 3/07.

9 Amtsgericht Berlin-Mitte, Beschluss vom 10.01.2008, Az. 5 C 314/06.

10 ABl. C. 129 vom 06.06.2009, 4.

11 ABl. C. 113 vom 16.05.2009, 24.

II. Unvereinbarkeit der Richtlinie 2006/24/EG mit den Gemeinschaftsgrundrechten

1. Bei Beantwortung der Vorlagefragen zu 2 kann sich dem Gerichtshof die Frage stellen, ob die Richtlinie 2006/24/EG gültig ist. Diese Frage ist dahin zu beantworten, dass die Richtlinie 2006/24/EG ungültig ist, weil sie gegen mehrere Gemeinschaftsgrundrechte verstößt.[12]

2. Einen Teil des primären Gemeinschaftsrechts stellen die Gemeinschaftsgrundrechte dar, die der Europäische Gerichtshof als „allgemeine Grundsätze des Gemeinschaftsrechts“[13] aus den Rechtstraditionen der Mitgliedstaaten entwickelt hat. Der Europäische Gerichtshof wendet dabei in der Regel die EMRK in ihrer Auslegung durch den Europäischen Gerichtshof für Menschenrechte an.[14] Entsprechend Art. 8 EMRK hat der Europäische Gerichtshof beispielsweise den Schutz der Privatsphäre als Gemeinschaftsgrundrecht anerkannt.[15]

3. Im Jahr 2000 wurde die Charta der Grundrechte der Europäischen Union[16] beschlossen. Die Grundrechtscharta kann als Fest- und Fortschreibung der richterrechtlich entwickelten Gemeinschaftsgrundrechte angesehen werden. In Artikel 7 der Charta wird ein Recht der Bürger auf Achtung ihrer „Kommunikation“ garantiert. In Artikel 8 findet sich ein Grundrecht auf Schutz der eigenen personenbezogenen Daten, das auch die Aufsicht einer unabhängigen Stelle über jede Verarbeitung personenbezogener Daten vorsieht.

---

12 Ebenso: Deutscher Anwaltverein, Stellungnahme vom August 2007, http://www.anwaltverein.de/03/-05/2007/41-07.pdf, 35 f.; Art. 29-Gruppe der EU, Stellungnahme 5/2002, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp64_de.pdf und Stellungnahme 9/2004, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp99_de.pdf; Covington & Burling, Memorandum of laws concerning the legality of data retention with regard to the rights guaranteed by the European Convention on Human Rights vom 10.10.2003, http://www.statewatch.org/news/2003/oct/Data_Retention_Memo.pdf, 3; Empfehlung des Europäischen Parlaments zu der Strategie zur Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität (2001/2070(COS)) vom 06.09.2001, Dokument Nr. T5-0452/2001, Buchst. H; EDSB-Konferenz, Europäische Datenschutzbeauftragte: Statement at the International Conference in Cardiff (09.-11.09.2002) on mandatory systematic retention of telecommunication traffic data, BT-Drs. 15/888, 176.

13 Schwarze-Stumpf, Art. 6 EUV, Rn. 19.

14 EuGH, Urteil vom 20.05.2003, Az. C-465/00, EuGRZ 2003, 232 (238), Abs. 69 und 73 ff.

15 EuGH, Urteil vom 20.05.2003, Az. C-465/00, EuGRZ 2003, 232 (238), Abs. 68 ff.

16 ABl. EG Nr. C 364 vom 18.12.2000, www.europarl.eu.int/charter/pdf/text_de.pdf.

1. Verletzung des Rechts auf Achtung des Privatlebens und der Korrespondenz (Artikel 8 EMRK)

a) Eingriff durch die Richtlinie 2006/24/EG

4. Art. 8 EMRK garantiert unter anderem das Recht auf Achtung des Privatlebens und der Korrespondenz. Mit der Richtlinie 2006/24/EG greift der Richtliniengeber in Art. 8 EMRK ein, weil er Telekommunikationsunternehmen die Pflicht auferlegt, personenbezogene Kommunikationsdaten auf Vorrat zu erheben, zu speichern und für den Abruf durch staatliche Behörden verfügbar zu halten.

5. Der Europäische Gerichtshof für Menschenrechte (EGMR) hat wiederholt entschieden, dass auch Telefongespräche als „Korrespondenz" im Sinne des Art. 8 EMRK anzusehen sind.[17] Trotz des jedenfalls im Deutschen abweichenden Wortlauts ist diese Gleichstellung teleologisch geboten, weil sich der Bürger in beiden Fällen in einer vergleichbaren Gefährdungslage bezüglich seiner räumlich distanzierten Kommunikation befindet. Aus demselben Grund fasst der Gerichtshof auch die näheren Umstände der Telekommunikation unter den Begriff der „Korrespondenz".[18] Art. 8 EMRK schützt dabei sowohl geschäftliche als auch private Kommunikation.[19]

6. Die Subsumtion unter den Begriff des „Privatlebens" fällt leichter, weil der Gerichtshof unter Bezugnahme auf die Datenschutzkonvention allgemein anerkennt, dass die Sammlung und Speicherung personenbezogener Daten einen Eingriff in das Privatleben des Einzelnen darstellt,[20] ebenso wie die Verwendung solcher Daten und die Verweigerung ihrer Löschung.[21]

7. Der EGMR hat wiederholt entschieden, dass die Erhebung von Verbindungsdaten ohne Einwilligung des Betroffenen einen Eingriff in dessen Rechte auf Achtung der Korrespondenz und des Privatlebens darstellt,[22] weil Verbindungsdaten, „besonders die gewählten Nummern [...] integraler Bestandteil der Kommunikation" seien.[23] Dies gilt neben Telefonaten auch für die Erhebung näheren Umstände der E-Mail-Nutzung und der Internetnutzung.[24] Sowohl in der Erhebung wie auch in der Speicherung die-

17 Frowein/Peukert-Frowein, Art. 8, Rn. 34 m.w.N.

18 EGMR, Copland-UK (2007), MMR 2007, 431 (432), Abs. 41-44.

19 EGMR, Niemietz-D (1992), Publications A251-B, Abs. 29, 31 und 33; EGMR, Rotaru-ROM (2000), Decisions and Reports 2000-V, Abs. 43; EGMR, Amann-CH (2000), Decisions and Reports 2000-II, Abs. 65.

20 Frowein/Peukert-Frowein, Art. 8, Rn. 5 m.w.N.

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

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

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

24 EGMR, Copland-UK (2007), MMR 2007, 431 (432), Abs. 41.

ser Daten liegt ein Grundrechtseingriff, selbst wenn die Daten auf legalem Wege erlangt werden.[25] Zuletzt hat die Große Kammer des EGMR am 04.12.2008 bestätigt, dass schon die Speicherung von Daten über das Privatleben einer Person einen Eingriff in dessen Rechte aus Art. 8 EMRK darstellt.[26]

8. Würde die Aufzeichnung der Verkehrsdaten unmittelbar durch eine staatliche Stellen vorgenommen, bestünde danach kein Zweifel an dem Eingriff in die Rechte auf Achtung der Korrespondenz und des Privatlebens.

9. An der Eingriffsqualität der Vorratsdatenspeicherung ändert nichts, dass der Richtliniengeber die Speicherung anstelle einer staatlichen Behörde privaten Anbietern auferlegt.

10. Nach dem modernen Eingriffsbegriff schützen die Grundrechte auch vor mittelbaren Eingriffen durch staatliche Maßnahmen, welche die Beeinträchtigung eines grundrechtlich geschützten Verhaltens typischerweise und vorhersehbar zur Folge haben oder die eine besondere Beeinträchtigungsgefahr in sich bergen, die sich jederzeit verwirklichen kann.[27]

11. Dies ist bei der Vorratsspeicherung von Telekommunikationsdaten der Fall,[28] denn die Speicherung von Telekommunikationsdaten macht diese für eine spätere staatliche Kenntnisnahme verfügbar und birgt damit die latente Gefahr späterer, weiterer Eingriffe. Eine Verpflichtung zur Vorratsspeicherung von Verkehrsdaten über die Dauer des jeweiligen Kommunikationsvorgangs hinaus begründet die besondere Gefahr, dass der Staat die gespeicherten Daten in Anwendung staatlicher Zwangsmittel anfordert. Beeinträchtigungen der von Art. 8 EMRK gewährleisteten Vertraulichkeit der Telekommunikation vor dem Staat sind die typische und vorhersehbare Folge einer generellen Telekommunikationsdatenspeicherungspflicht. Damit stellt bereits die Anordnung einer generellen Vorratsspeicherung von Telekommunikationsdaten durch den Richtliniengeber einen staatlichen Eingriff in die Rechte aus Art. 8 EMRK dar.

12. Dass sich der Staat zur Speicherung privater Unternehmen bedient, kann keinen Unterschied machen, wenn er sich gleichzeitig den Zugriff auf die gespeicherten Daten eröffnet. Andernfalls könnte der Staat seine Grundrechtsbindung durch ein bloßes „Outsourcing“ umgehen. Die Inanspruchnahme Privater erhöht das Gewicht des Eingriffs sogar noch, weil sich der Kreis von – weitgehend ohne Schuld – beeinträchtigten Personen durch den zusätzlichen Eingriff in das Recht der Anbieter aus Art. 1 ZEMRK noch vergrößert. Zudem ist das Risiko, dass gespeicherte Daten missbraucht werden, bei einer Datenspeicherung durch eine Vielzahl von Privatunternehmen er-

25 EGMR, Copland-UK (2007), MMR 2007, 431 (432), Abs. 43 f.

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

27 Windthorst, § 8, Rn. 50 und 52 m.w.N.; Dreier, GG, Vorb., Rn. 82; Pieroth/Schlink, Rn. 240 ff.; Sachs, GG, Vor Art. 1, Rn. 83 ff.; Weber-Dürler, VVDStRL 57 (1998), 66 ff.

28 Ebenso für eine Pflicht zur generellen Speicherung von Telekommunikations-Bestandsdaten unter dem Aspekt des Grundrechts auf informationelle Selbstbestimmung BVerwGE 119, 123 (126).

heblich höher einzuschätzen als bei einer staatlichen Speicherung, so dass die Privilegierung einer privaten Vorratsspeicherung auch sachlich nicht gerechtfertigt wäre.

13. Bereits entschieden hat das Bundesverfassungsgericht, dass die Übermittlung von Telekommunikation an staatliche Stellen durch einen privaten Kommunikationsmittler, der die Telekommunikation auf staatliche Anordnung aufzeichnet und den staatlichen Stellen sodann verfügbar macht, einen Eingriff in das Fernmeldegeheimnis der an dem Kommunikationsvorgang Beteiligten darstellt.[29] Die Tatsache, dass sich der Staat dabei eines Privaten bediene, sei unerheblich, da der Eingriff hoheitlich angeordnet werde und dem Privaten kein Handlungsspielraum zur Verfügung stehe.[30] Ebenso verhält es sich bei der Pflicht zur Vorratsdatenspeicherung, welche die Richtlinie 2006/24/EG begründet.

14. In Erwägungsgrund 9 der Richtlinie 2006/24/EG hat der Richtliniengeber schließlich selbst anerkannt, dass er in Art. 8 EMRK eingreift.

b) Erfordernis einer gesetzlichen Grundlage

15. Eingriffe in Art. 8 EMRK bedürfen der Rechtfertigung. Gemäß Art. 8 Abs. 2 EGMR ist zunächst eine gesetzliche Grundlage für Eingriffe erforderlich. Eine solche Grundlage ist mit der Richtlinie 2006/24/EG geschaffen worden.

16. Aus dem Erfordernis einer gesetzlichen Grundlage in Verbindung mit dem in der Präambel der EMRK erwähnten Rechtsstaatsprinzip leitet der EGMR zudem ab, dass das eingreifende innerstaatliche Recht hinreichend bestimmt und für den Bürger zugänglich sein muss.[31] Dem Einzelnen müsse es möglich sein, sein Verhalten den Vorschriften entsprechend einzurichten, was ein – gemessen an der Schwere des Eingriffs[32] – hinreichendes Maß an Vorhersehbarkeit voraussetze.[33] Aus dem Rechtsstaatsprinzip leitet der EGMR auch inhaltliche Anforderungen an eingreifende Gesetze ab. So muss das nationale Recht einen hinreichenden und effektiven Schutz vor willkürlichen Eingriffen und vor Missbrauch der eingeräumten Befugnisse gewährleisten.[34]

    Ob die Richtlinie 2006/24/EG diesen Anforderungen genügt, kann offen bleiben, weil sie aus den nachfolgenden Gründen nicht in einer demokratischen Gesellschaft erforderlich ist.

---

29 BVerfGE 107, 299 (313 f.).

30 BVerfGE 107, 299 (313 f.).

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

32 EGMR, Kruslin-F (1990), Publications A176-A, Abs. 33.

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

34 EGMR, Malone-GB (1984), EuGRZ 1985, 17 (20 und 22), Abs. 67 und 81.

c) Fehlende Erforderlichkeit in einer demokratischen Gesellschaft

17. Nach Art. 8 Abs. 2 EMRK muss eine Beschränkung der Rechte aus Absatz 1 in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer erforderlich sein. Der Staat hat nach der Rechtsprechung des Gerichtshofs einen Beurteilungsspielraum bezüglich der Frage, ob eine Maßnahme zu einem der in Art. 8 Abs. 2 EMRK genannten Zwecke erforderlich ist.[35] Dabei behält sich der EGMR aber das Letztentscheidungsrecht vor, so dass er selbst vertretbare nationale Entscheidungen verwerfen kann.[36]

18. In einer demokratischen Gesellschaft erforderlich ist eine Maßnahme nur, wenn ein in Anbetracht des Stellenwerts des garantierten Freiheitsrechts hinreichend dringendes soziales Bedürfnis nach ihr besteht, sie einen legitimen Zweck verfolgt und ihre Belastungsintensität nicht außer Verhältnis zu dem Gewicht des Zwecks steht.[37] Der EGMR hat dazu eindeutig erklärt, dass das Interesse des Staates gegenüber den Interessen des Einzelnen an der Achtung seiner Privatsphäre abgewogen werden müsse.[38] Eingriffe sind zwar nicht auf das unerlässliche Maß beschränkt, aber ein bloßes Nützlich- oder Wünschenswertsein genügt nicht.[39]

aa) Übertragbarkeit des Urteils des EGMR in Sachen S. und Marper

19. Dass die Richtlinie 2006/24/EG das Grundrecht auf Achtung der Privatsphäre (Art. 8 EMRK) verletzt, ergibt sich aus dem Urteil der Großen Kammer des Europäischen Gerichtshofs für Menschenrechte vom 04.12.2008.[40] In diesem Urteil hat der Gerichtshof ausgeführt:[41]

„*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*

35 EGMR, Sunday Times-GB (1979), EuGRZ 1979, 386 (388 f.), Abs. 59; EGMR, Silver u.a.-GB (1983), EuGRZ 1984, 147 (152), Abs. 97; EGMR, Lambert-F (1998), Decisions and Reports 1998-V, Abs. 30; EGMR, Foxley-GB (2000), http://hudoc.echr.coe.int/Hudoc1doc2/HEJUD/200107/foxley%20-%2033274jv.chb3%2020062000e.doc, Abs. 43.

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

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

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

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

40 Az. 30562/04 und 30566/04.

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

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."

20. 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.

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

22. Erstens ist die Vorratsdatenspeicherung quantitativ weit eingriffsintensiver:

23. a) Während die englische Befugnis nur Personen betraf, die einer Straftat verdächtig waren, betrifft die Vorratsdatenspeicherung quasi jeden Menschen. In Großbritannien waren einige Millionen von Personen von einer Speicherung ihrer biometrischen Daten betroffen. Von der Richtlinie zur Vorratsdatenspeicherung sind demgegenüber praktisch alle 365 Mio. Europäer betroffen.

24. b) In der englischen Datensammlung waren von jedem Verdächtigen bis zu drei Angaben gespeichert: Fingerabdruck, Gewebeprobe und DNA-Profil. Aufgrund der Richtlinie 2006/24/EG wird demgegenüber unser gesamtes tägliches Telekommunikations-, Informations- und Bewegungsverhalten erfasst. Es handelt sich um eine weitaus größere Menge an Informationen.

25. Daneben ist die Vorratsdatenspeicherung auch qualitativ weit eingriffsintensiver:

26. a) Die in England gesammelten biometrischen Informationen konnten zur Identifizierung Verdächtiger verwendet werden; im Fall von Gewebeproben und DNA-Profilen auch zur Gewinnung von Informationen über Herkunft und Krankheiten.

    Die unter der Vorratsdatenspeicherung gesammelten Informationen betreffen zwar auch unsere Identität und erlauben die Identifizierung von Gesprächsteilnehmern (Art. 5 (1) a) und b) RiL 2006/24/EG). Sie betreffen vor allem aber unser alltägliches Kommunikations-, Informations- und Bewegungsverhalten (Art. 5 (1) c) bis f) RiL 2006/24/EG). 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

Telekommunikationsdaten 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.

27. b) Während in England nur Personen, die einer Straftat verdächtig waren, biometrische Merkmale abgenommen wurden, trifft die Vorratsdatenspeicherung sogar Menschen, die nie auch nur im Verdacht einer Straftat gestanden haben. Selbst der rechtstreueste Bürger kann die Erfassung seines Kommunikations- und Bewegungsverhaltens infolge der Vorratsdatenspeicherung nicht vermeiden.

28. 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 (auch unverdächtigen) Bevölkerung erst Recht.

29. Soweit der EGMR in einer Kammerentscheidung Finnland verurteilt hat, weil dessen Gesetze im Jahr 1999 die Aufklärung einer im Internet begangenen Straftat nicht zuließen,[42] steht dies der Unverhältnismäßigkeit der Vorratsdatenspeicherung nicht entgegen, weil diese Entscheidung eine andere Fallgestaltung betraf: In jenem Fall verfügte der finnische Internetanbieter über Daten, die eine Identifizierung des mutmaßlichen Täters ermöglicht hätten;[43] das finnische Recht erlaubte die Herausgabe dieser Daten aber nicht.[44] Der Gerichtshof hat mit seiner Entscheidung beanstandet, dass das finnische Recht einen Zugriff auf ohnehin vorhandene Daten selbst zur Aufklärung einer vom Gerichtshof als schwer angesehenen Straftat (sexuelle Verleumdung eines Kindes in der Öffentlichkeit, welche das Kind der Gefahr sexueller Übergriffe aussetzte) nicht zuließ. Dass der Staat zur Aufklärung schwerer Straftaten auf ohnehin zu betrieblichen Zwecken gespeicherte Daten zugreifen darf, steht hier nicht in Frage. Der Gerichtshof hat in der genannten Entscheidung demgegenüber nicht gefordert oder zugelassen, zur Aufklärung möglicher zukünftiger Straftaten rein vorsorglich das Kommunikations- und Bewegungsverhalten der gesamten Bevölkerung erfassen zu lassen. Gegen diese Annahme spricht auch die Anmerkung des Gerichtshofs, wonach Finnland das „Defizit“ in seinem Prozessrecht in einem späteren „Gesetz über die Ausübung der Meinungsfreiheit in Massenmedien“ angegangen sei.[45] Dieses Gesetz sah eine Befugnis zur Identifizierung von Kommunikationsteilnehmern auf richterliche Anordnung vor,[46] nicht jedoch eine anlasslose und flächendeckende Vorratsdatenspeicherung.

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

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

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

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

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

bb) Vorratsdatenspeicherung verzichtbar für die Strafverfolgung

30. In Sachen S. und Marper ist der EGMR zutreffend der Behauptung der britischen Regierung entgegen getreten, die damals angefochtene Vorratsspeicherung sei „unabdingbar" zur Verfolgung von Straftaten.[47] Dieser Behauptung hat der Gerichtshof erstens entgegen gehalten, dass England die Maßnahme selbst erst 2001 eingeführt habe.[48] Zweitens hat er darauf hingewiesen, dass die Strafverfolgungsbehörden anderer Staaten auch ohne eine solche Maßnahme auskommen.[49]

31. Nichts anderes gilt auch für die Vorratsspeicherung von Telekommunikationsdaten. Als die Richtlinie zur Vorratsdatenspeicherung beschlossen wurde, verfügte nur eine kleine Minderheit der Mitgliedsstaaten über Vorschriften zur verdachtslosen, flächendeckenden Vorratsspeicherung von Telekommunikationsdaten. Die große Mehrzahl der Mitgliedsstaaten kam ohne solche Vorschriften aus. Für andere westliche Staaten wie die USA, Kanada, Japan oder Norwegen und selbst EU-Staaten wie Österreich gilt dies bis heute.

32. **Minimale Relevanz für die Strafverfolgung**

33. Dass kein „hinreichend dringendes soziales Bedürfnis" nach einer permanenten, flächendeckenden Aufzeichnung des Telekommunikations- und Bewegungsverhaltens der gesamten Bevölkerung besteht, bestätigt eine ausführliche Untersuchung aus Deutschland. Das Bundesjustizministerium hat bei dem unabhängigen Max-Planck-Institut für ausländisches und internationales Strafrecht eine Untersuchung des Zugriffs auf Verkehrsdaten zum Zweck der Strafverfolgung in Auftrag gegeben.[50] Das Institut hat eine repräsentative Stichprobe von 467 strafrechtlichen Ermittlungsverfahren untersucht, in denen Telekommunikations-Verkehrsdaten erhoben worden waren.

34. Ausweislich der repräsentativen Aktenanalyse des Max-Planck-Instituts konnten auch ohne Vorratsdatenspeicherung nur bei 4% der Zielanschlüssen die von den Strafverfolgungsbehörden angeforderten Verkehrsdaten nicht mehr oder nicht vollständig erlangt werden.[51]

35. Die Zahl von 4% bezieht sich auf Strafverfahren, in denen Verkehrsdaten angefordert wurden. Das Gutachten schätzt, dass im Untersuchungsjahr 2005 insgesamt 40.000 Beschlüsse zur Herausgabe von Verkehrsdaten erlassen wurden.[52] Da in 467 der untersuchten Ermittlungsverfahren 1257 Beschlüsse erlassen wurden,[53] kann man von

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

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

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

50 Albrecht/Grafe/Kilchling, Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO (im Folgenden: MPI-Forschungsbericht), http://www.bmj.bund.de/files/-/3045/MPI-GA-2008-02-13%20Endfassung.pdf.

51 MPI-Forschungsbericht, 253.

52 MPI-Forschungsbericht, 76.

53 MPI-Forschungsbericht, 125.

2,7 Beschlüssen pro Verfahren ausgehen. Danach werden 2005 etwa 15.000 Ermittlungsverfahren bundesweit die Erhebung von Verkehrsdaten zum Gegenstand gehabt haben. Wenn in 4% dieser Verfahren Anfragen mangels gespeicherter Daten ergebnislos blieben, beträfe dies etwa 600 Verfahren bundesweit. Gemessen daran, dass in den Jahren 2003 und 2004 jeweils ca. 4,9 Mio. Ermittlungsverfahren bearbeitet wurden,[54] entspricht dies 0,01% aller Ermittlungsverfahren. Dies bestätigt, dass eine Vorratsdatenspeicherung nur in 0,01% aller strafrechtlichen Ermittlungsverfahren überhaupt einen Beitrag zur Strafverfolgung leisten kann.

36. Um den möglichen Nutzen der Richtlinie 2006/24/EG zu Strafverfolgungszwecken zu ermitteln, müssen indes von den Verfahren, in denen Abfragen wegen fehlender Verkehrsdaten ergebnislos blieben, noch diejenigen Verfahren in Abzug gebracht werden, die auf anderem Wege aufgeklärt werden konnten. Laut Studie blieb die Verkehrsdatenabfrage – trotz zu 96% vorhandener Daten – bei etwa 130 Beschuldigten erfolglos; dennoch wurde gegen etwa 45 von ihnen später Anklage erhoben.[55] Etwa ein Drittel der Verfahren mit erfolgloser Verkehrsdatenabfrage kann somit auf anderem Wege aufgeklärt werden.

37. Weiterhin müssen von den Verfahren, in denen Abfragen erfolglos blieben, noch diejenigen Verfahren in Abzug gebracht werden, die im Fall vorhandener Daten ebenfalls eingestellt worden wären. Auch in diesen Fällen leistet die Vorratsdatenspeicherung keinen Beitrag zur Verfolgung von Straftaten. Laut Studie wurden – trotz zu 96% vorhandener Daten – 60% der Verfahren eingestellt und in 23% der Verfahren Anklage erhoben.[56] Dies entspricht einer „Einstellungsquote“ von 72% der abgeschlossenen Verfahren; hinzu kommen noch die gerichtlichen Einstellungen und Freisprüche. In etwa drei Viertel der Verfahren würde eine Vorratsdatenspeicherung mithin schon deshalb keinen Beitrag zur Strafverfolgung leisten, weil die Verfahren selbst bei Vorliegen der angeforderten Verkehrsdaten eingestellt werden würden.

38. Unter Berücksichtigung all dieser Umstände ergibt sich, dass die Verfolgung von Straftaten zu gerade einmal 0,002% durch eine Vorratsspeicherung von Verkehrsdaten effektiviert werden kann.[57] Schon allein durch Zufälle und statistische Einflüsse schwankt die jährliche Zahl der aufgeklärten Straftaten um ein hundertfaches dieses Betrags. Nicht an dieser Stelle berücksichtigt werden soll der Umstand, dass die meisten der weit zurück reichenden Verkehrsdatenanforderungen auf eine bloß allgemeine Erforschung des Kommunikationsumfelds eines Tatverdächtigen und nicht auf eine gezielte Abfrage gerichtet sind.[58]

54 Statistisches Bundesamt, Staatsanwaltschaften - Fachserie 10 Reihe 2.6 - 2006, 13.

55 MPI-Forschungsbericht, 391.

56 MPI-Forschungsbericht, 390 f.

57 600 / 4.900.000 x 2/3 x (1-0,72) = 0,0023%.

58 MPI-Forschungsbericht, 115.

39. Auf der anderen Seite ist zu berücksichtigen, dass die Strafverfolgungsbehörden die Nichtspeicherung oder Löschung von Verkehrsdaten (vgl. Art. 6 (1) RiL 2002/58/EG) zum Teil antizipieren und daher bereits keine entsprechenden Anordnungen beantragen dürften. Die Strafverfolgungsorgane haben bislang keine belastbaren Zahlen darüber vorgelegt, in wie vielen Verfahren jährlich dies der Fall sei. Eine Untersuchung des Bundeskriminalamts dürfte Fälle, in denen eine Anforderung von Verkehrsdaten mangels Erfolgsaussicht unterblieb, einschließen und nennt dennoch über mehrere Jahre hinweg nur 381 Fälle fehlender Verkehrsdaten.[59] Einzig das Land Rheinland-Pfalz hat gegenüber dem Bundesverfassungsgericht eine Schätzung vorgetragen, der zufolge 700 erfolglosen Auskunftersuchen 1.050 Fälle gegenüber stünden, in denen von vornherein wegen mutmaßlich gelöschter Daten keine Auskunft angefordert worden sei.[60] Auf dieser Grundlage müsste die Zahl der erfolglosen Auskunftersuchen mit 2,5 multipliziert werden, um auf die Gesamtheit der Fälle fehlender Verkehrsdaten zu schließen.[61] Auf dieser Grundlage könnte eine Vorratsdatenspeicherung in 0,006%[62] der registrierten Straftaten von Nutzen sein, was an der offensichtlichen Unverhältnismäßigkeit der die gesamte Bevölkerung treffenden Maßnahme nichts ändern würde.

40. **Fehlende Relevanz für die Aufklärungsquote**

41. Dass eine pauschale und generelle Vorratsdatenspeicherung in einer demokratischen Gesellschaft nicht erforderlich ist, belegt zweitens die Aufklärungsquote im Bereich der Internetdelikte, die in Deutschland statistisch erfasst wird. Die Aufklärungsquote für Internetdelikte in Deutschland übertrifft die allgemeine Aufklärungsquote bei weitem und war in den letzten Jahren auch nicht rückläufig. Die durchschnittliche Aufklärungsquote von 55%[63] wurde im Bereich mittels Telekommunikation begangener Straftaten auch vor Umsetzung der Richtlinie 2006/24/EG weit übertroffen: Aufgeklärt wurden im Jahr 2007 86,3% der registrierten Straftaten im Bereich der Verbreitung pornographischer Schriften via Internet, 84% der Fälle von Internetbetrug und 94,8% der Straftaten gegen Urheberrechtsbestimmungen im Internet.[64] Es ist nicht ersichtlich, dass diese Aufklärungsquoten durch die Richtlinie 2006/24/EG überhaupt statistisch nachweisbar gesteigert werden könnten. Erst Recht kann von einem Leerlaufen einzelner Straftatbestände keine Rede sein.

42. Wie die Strafverfolgungsbehörden – ohne Vorratsdatenspeicherung – derart hohe Aufklärungsquoten erzielen können, bedarf hier keiner näheren Untersuchung. Es soll

---

59 Mahnken: Mindestspeicherungsfristen für Telekommunikationsverbindungsdaten - Rechtstatsachen zum Beleg der defizitären Rechtslage (2005), http://www.vorratsdatenspeicherung.de/images/bka_vorratsdatenspeicherung.pdf.

60 Stellungnahme des rheinland-pfälzischen Ministeriums der Justiz vom 19.02.2008, 2 f.

61 700 x 2,5 = 700 + 1.050.

62 0,0023% x 2,5 = 0,0058%.

63 Bundeskriminalamt, Polizeiliche Kriminalstatistik 2007, 65.

64 Bundeskriminalamt, Polizeiliche Kriminalstatistik 2007, 243.

nur ein weiteres Mal darauf hingewiesen werden, dass im Bereich der postalischen Kommunikation, der unmittelbaren Kommunikation und des Bewegungsverhaltens generell keine Aufzeichnungen über das Verhalten der gesamten Bevölkerung in der Vergangenheit zur Verfügung stehen und gleichwohl nicht die Rede davon sein kann, dass eine Aufklärung bestimmter Typen von Straftaten deswegen regelmäßig leer liefe. Die durchschnittliche Aufklärungsquote von 55% kann generell erzielt werden, ohne dass systematisch das Kommunikations-, Bewegungs- und Informationsverhalten der gesamten Bevölkerung aufgezeichnet wird. Im Telekommunikationsbereich besteht auch ohne die Richtlinie 2006/24/EG die bewährte Möglichkeit des Zugriffs auf Verkehrsdaten, die ohnehin zu Abrechnungszwecken gespeichert sind oder auf richterliche Anordnung im Einzelfall gespeichert werden (Art. 15 RiL 2002/58/EG). Diese Möglichkeiten haben in den letzten Jahren stets eine wirksame Strafrechtspflege auch im Bereich mittels Telekommunikation begangener Straftaten gesichert.

43. Im Übrigen ist für keinen der Mitgliedsstaaten nachgewiesen, dass eine Vorratsdatenspeicherung überhaupt zu einem statistisch signifikanten Anstieg der Aufklärungsquote – und sei es nur bei den mittels Telekommunikation begangenen Delikten – geführt habe. Vielmehr dürfte sich die Vorratsdatenspeicherung überhaupt nicht merklich auf Kriminalitätsrate oder Aufklärungsrate auswirken, auch nicht im Bereich mittels Telekommunikation begangener Straftaten.

44. **Unverhältnismäßigkeit**

45. In dem Urteil in Sachen S. und Marper hat der EGMR zutreffend die von der britischen Regierung vorgelegten Statistiken über die Zahl der erfolgreichen Abrufe aus der Datenbank hinterfragt. Er hat kritisiert, dass die Zahl der erfolgreichen Abrufe keinen Aufschluss darüber gebe, in wie viele Fällen ein erfolgreicher Abruf auch tatsächlich zur Verurteilung eines Straftäters geführt habe.[65] Auch sei nicht dargelegt, in wie vielen Fällen hierfür gerade die Vorratsspeicherung der Daten Nichtverurteilter erforderlich gewesen sei.[66] Die meisten der von der Regierung genannten erfolgreichen Abrufe wären auch ohne die beanstandete Vorratsspeicherung möglich gewesen.[67] Wenngleich der Gerichtshof im Ergebnis davon ausging, dass die Vorratsspeicherung biometrischer Daten einen gewissen Beitrag zur Strafverfolgung leistete,[68] verwarf er sie gleichwohl als unverhältnismäßig weitgehend.

46. Nichts anderes gilt auch für die Vorratsspeicherung von Telekommunikationsdaten. Aus den Statistiken der Mitgliedsstaaten (vgl. Art. 10 RiL 2006/24/EG) über die Zahl der Zugriffe auf Telekommunikationsdaten ergibt sich nicht, ob und in wie viele Fällen ein Abruf auch tatsächlich zur Verurteilung eines Straftäters geführt habe. Auch ergibt sich aus den Statistiken nicht, in wie vielen Fällen gerade eine anlasslose und flä-

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

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

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

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

chendeckende Vorratsdatenspeicherung erforderlich gewesen sei und Abrechnungsdaten (Art. 6 RiL 2002/58/EG) oder auf besondere Anordnung gespeicherte Daten oder andere Ermittlungsinstrumente nicht ausgereicht hätten. Wie oben dargelegt, kann eine Vorratsdatenspeicherung allenfalls in 0,01% aller Strafverfahren überhaupt von Bedeutung sein. Selbst wenn man dementsprechend davon ausgeht, dass die Richtlinie 2006/24/EG einen gewissen Beitrag zur Strafverfolgung leisten kann, greift eine flächendeckende und permanente Aufzeichnung des Kommunikations- und Bewegungsverhaltens doch unverhältnismäßig weit in das Grundrecht der Unionsbürger auf Wahrung ihrer Privatsphäre und der Vertraulichkeit ihrer Telekommunikation ein.

cc) Unzumutbar schwerer Grundrechtseingriff

47. Im Fall S. und Marper verwarf der Gerichtshof ferner die Argumentation der britischen Regierung, die bloße Aufbewahrung der Daten ohne ihre Nutzung könne sich auf die Betroffenen nicht nachteilig auswirken.[69] 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.[70]

48. Ebenso zieht die von der Richtlinie 2006/24/EG vorgeschriebene Vorratsdatenspeicherung bereits konkrete Nachteile für die betroffenen Bürger nach sich, und zwar in folgender Hinsicht:

49. **Staatliche Fehlurteile**

50. Die Richtlinie 2006/24/EG erhöht die allgemeine Gefahr, unschuldig einer Straftat verdächtigt zu werden:[71]

51. Erstens beziehen sich gesammelten Kommunikationsdaten stets nur auf den Inhaber eines Anschlusses. Wird der Anschluss von anderen Personen genutzt, dann kann der Inhaber leicht unschuldig in einen falschen Verdacht geraten.

52. Zweitens ermöglicht es der Zugriff auf Kommunikationsdaten den Behörden, nach dem Eliminierungsprinzip zu arbeiten. Dabei wird nicht, wie traditionell üblich, eine „heiße Spur“ verfolgt, sondern es werden – etwa mit Hilfe von Kommunikationsdaten – eine (oft große) Gruppe von Personen ermittelt, die aufgrund bestimmter Merkmale als Täter in Betracht kommen (beispielsweise alle Personen, die innerhalb eines bestimmten Zeitraums das Opfer einer Straftat angerufen haben). Es kommt dadurch quasi zu einer Inflation an Verdächtigungen, aus der sich die so Erfassten nur noch im Wege einer Art Beweislastumkehr befreien können.[72] Weil ein Kommunikationsdatensatz ein Indiz gegen den Angeklagten bilden kann, muss dieser unter Umständen

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

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

71 BVerfGE 107, 299 (321).

72 Hamm, TKÜV, 81 (86).

den Richter von seiner Unschuld überzeugen, um nicht zu Unrecht verurteilt zu werden.[73] Mangels eines Alibis wird Unschuldigen die Erschütterung der Indizienkette keineswegs immer gelingen. Aber auch, wenn sich die Unschuld einer Person noch vor ihrer Verurteilung herausstellt, kann ein falscher Verdacht ausreichen, um zu Hausdurchsuchungen, Untersuchungshaft, Bewegungseinschränkungen oder Aus- und Einreiseverboten zu führen, was mit schwerwiegenden Belastungen für die Betroffenen verbunden ist.

53. Folgende Fälle von Fehlurteilen aufgrund einer Analyse von Telekommunikationsdaten sind in Europa bereits bekannt geworden: In Österreich wurde ein Nigerianer mehrere Monate lang in Untersuchungshaft genommen, weil er wegen seiner zahlreichen Telefonkontakte als Anführer einer Rauschgiftbande in Verdacht geraten war.[74] Später stellte sich der Verdacht als unbegründet und der Nigerianer lediglich als gefragter Ratgeber in der schwarzen Gemeinschaft in Wien heraus.[75]

54. In Schweden gab es Fälle, in denen unschuldige Personen im Zusammenhang mit Ermittlungen wegen Netzkriminalität festgenommen wurden. Später stellte sich heraus, dass die wirklichen Straftäter den Internet-Zugangscode der festgenommenen Personen ohne deren Kenntnis missbraucht hatten.[76]

55. Zu Unrecht ins Visier der deutschen Kriminalpolizei ist ein 63-jähriger Mann aus Nürnberg geraten.[77] Er war angezeigt worden, da von seinem Internetanschluss aus kostenpflichtige Erotikseiten besucht wurden, ohne die angefallenen Kosten hierfür zu bezahlen. Das Fachdezernat der Kriminalpolizei konnte anhand der hinterlassenen „Internetspuren“ (IP-Adressen) den 63-Jährigen als verantwortlichen Anschlussinhaber ermitteln. Der überraschte Mann versicherte jedoch, derartige Seiten niemals besucht zu haben. Durch weitere Ermittlungen kam man schließlich dem eigentlichen Täter auf die Spur. Er hatte den Internetzugang des zu Unrecht Verdächtigen über Funknetz (WLAN) genutzt.

56. Aufgrund des begrenzten Aussagegehalts von Telekommunikationsdaten und der Tatsache, dass der Zugriff auf Kommunikationsdaten oft eine Vielzahl von Personen betrifft, birgt der Zugriff auf Kommunikationsdaten ein besonderes Risiko falscher Verdächtigungen. Weil die Richtlinie 2006/24/EG eine erheblich umfangreichere Spei-

---

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

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

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

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

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

cherung von Kommunikationsdaten als bisher zur Folge hat, ist davon auszugehen, dass auch die Anzahl der Zugriffe auf Kommunikationsdaten erheblich steigt. Damit erhöht sich auch das Risiko von Fehlentscheidungen in Ermittlungs- und Gerichtsverfahren.

57. **Risiko von Datenpannen und des Missbrauchs durch Private**

58. Die Aufzeichnung und Vorhaltung von Informationen über die Kommunikation, Bewegungen und Internetnutzung der gesamten Bevölkerung schafft zudem unvermeidbare Risiken eines gesetzwidrigen Missbrauchs dieser Informationen.

59. Sowohl in Griechenland wie auch in Italien sind in den letzten Jahren Fälle illegalen Abhörens durch kriminelle Netzwerke bekannt geworden.[78]

60. Im Jahr 2008 ist bekannt geworden, dass die Deutsche Telekom AG als größter Anbieter von Telekommunikationsdiensten in Deutschland in 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.[79] Ziel der Operation war die Auswertung der Festnetz- und Mobilfunk-Verbindungsdatensätze der wichtigsten über die Telekom berichtenden deutschen Journalisten und deren privater Kontaktpersonen.[80] Ausgewertet wurden nicht weniger als 250.000 Verbindungen.[81] Anhand von Handy-Standortdaten wurden selbst die Bewegungen der Betroffenen nachverfolgt, um mögliche Zusammentreffen zu ermitteln.[82] Bereits im Jahr 1997 hatte die Telekom Verbindungsdaten und Kommunikationsinhalte mutmaßlicher „Hacker“ ausgewertet. Später stellte sich heraus, dass der Verdächtigte ein legal tätiger Mitarbeiter des Tochterunternehmens T-Mobile war.[83]

61. Wenngleich diese missbräuchlichen Nutzungen gespeicherter Kommunikationsdaten vor Inkrafttreten der angefochtenen Regelungen 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.

---

78 Handelsblatt, Abhörskandal entsetzt die Griechen, 02.02.2006, http://www.handelsblatt.com/news/-Default.aspx?_p=200051&_t=ft&_b=1028595; Spiegel Online, Der ganz, ganz große Lauschangriff, 21.09.2006, http://www.spiegel.de/panorama/justiz/0,1518,438499,00.html.

79 Spiegel Online vom 24.05.2008, http://www.spiegel.de/wirtschaft/0,1518,555162,00.html.

80 a.a.O.

81 Spiegel Online vom 29.05.2008, http://www.spiegel.de/wirtschaft/0,1518,556398,00.html.

82 Handelsblatt vom 30.05.2008, http://www.handelsblatt.com/News/default.aspx?_p=201197&_t=ft&_b=1436894.

83 Spiegel Online vom 20.06.2008, http://www.spiegel.de/wirtschaft/0,1518,561076,00.html.

62. Einem heute stattfindenden Missbrauch von Kommunikationsdaten würden wegen der Richtlinie 2006/24/EG 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 Richtlinie 2006/24/EG entfallen. Inzwischen ist zusätzlich auch der gesamte E-Mail-Verkehr einer missbräuchlichen Auswertung ausgesetzt.

63. Das Risiko eines derartigen Missbrauchs ist mit der Richtlinie 2006/24/EG notwendig verbunden und lässt sich nicht ausschließen.[84] 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.[85] Dies zeigt, dass Sicherungsvorkehrungen auch in Zukunft weitere Fälle von Datenmissbrauch nicht werden verhindern können.

64. Einen wirksamen Schutz vor Missbrauch ermöglicht somit alleine die Unterbindung der Protokollierung des Verhaltens selbst entsprechend dem Gebot der Datensparsamkeit.[86] Nur nicht gespeicherte Daten sind sichere Daten.

65. Die von der Richtlinie beabsichtigte Datennutzung zu Strafverfolgungszwecken begründet nur einen kleinen Teil der insgesamt durch die Kommunikationsdatenerfassung drohenden Gefahren. Die Vorratsdatenspeicherung begründet das Risiko von

    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.

84 Gola/Klug/Reif, Datenschutz- und presserechtliche Bewertung der „Vorratsdatenspeicherung“ (2007), 38.

85 Bundesregierung, BT-Drs. 16/9894, 3.

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

66. **Abschreckungswirkung**

67. Da mit der zwingenden Aufzeichnung des elektronischen Kommunikations- und Bewegungsverhaltens notwendig das Risiko verbunden ist, dass dem Betroffenen aus dem Bekanntwerden seiner Kontakte und Aufenthaltsorte Nachteile entstehen können, entfaltet die Richtlinie 2006/24/EG eine Abschreckungswirkung. Die Vorratsdatenspeicherung in bestimmten Situationen davon ab, Telefon, Handy, E-Mail oder Internet zu nutzen. Dies hat teilweise schwere Nachteile für Einzelne und für unsere Gesellschaft insgesamt zur Folge.

68. Nach Umsetzung der Richtlinie 2006/24/EG berichteten viele Menschen dem Arbeitskreis Vorratsdatenspeicherung, dass sie seit Inkrafttreten der Vorratsdatenspeicherung weniger telefonieren, ihr Handy, E-Mail oder Internet seltener nutzen, oder dass sie in ihrem privaten Umfeld solche Einschränkungen erleben. Der Antragsteller etwa schaltet sein Mobiltelefon seit Inkrafttreten der Vorratsdatenspeicherung kaum noch ein, um eine Bewegungsdatenspeicherung zu verhindern. Damit ist er auf diesem Wege nicht mehr erreichbar, etwa für Pressekontakte. Amina R. aus Niedersachsen teilt mit, sie schränke sich stark in der E-Mail-Kommunikation mit ihrer Familie in Marokko ein, weil sie befürchtet, durch ihre Kontakte in diesen Staat verdächtig zu erscheinen. Anna T. (Name geändert) ist Opfer sexuellen Missbrauchs und tauschte sich früher in entsprechenden Foren und Chatrooms aus. Seit anhand ihrer IP-Adresse ihre Identität ermittelt werden kann, hat sie sich aus diesem Austausch zurückgezogen und somit keine Möglichkeit mehr, sich mit anderen anonymen Opfern auszutauschen.

69. Die Vorratsdatenspeicherung schreckt weiters Informanten davon ab, vertrauliche Informationen an die Presse weiterzugeben, weil ihr Kontakt und ihre Identität anhand der Telekommunikationsdaten nachvollzogen werden kann. Ohne solche Informationen kann die Presse öffentliche Missstände nicht aufdecken und ihrer Kontrollfunktion gegenüber dem Staat nicht mehr nachkommen. Die Rundfunkjournalistin Hilde W. aus Thüringen schrieb dem Arbeitskreis Vorratsdatenspeicherung, sie recherchiere die Unterbringung von Flüchtlingen und Asylbewerbern in Thüringen, habe aber seit Inkrafttreten der Vorratsdatenspeicherung Probleme, telefonisch oder per E-Mail Auskunft über sensible Daten wie illegale Flüchtlinge, Namen und Adressen zu erhalten. Der Journalist Gerrit W. aus Nordrhein-Westfalen befasst sich im Rahmen seiner Arbeit unter anderem mit Menschenrechtsverletzungen der EU-Agentur Frontex. Schon in den ersten Wochen nach Inkrafttreten der Vorratsdatenspeicherung lehnten zwei Kontaktpersonen den Informationsaustausch via E-Mail ab. Der freiberufliche Journalist Peter H. aus Hessen schreibt, seit Inkrafttreten der Vorratsdatenspeicherung sei die Kommunikation mit Informanten aus Firmen, Behörden, Parteien, Stadtverwaltungen und sonstigen Institutionen erschwert, teilweise auch unmöglich geworden.

70. Kommunikationsstörungen treten auch im Bereich der wirtschaftlichen und rechtlichen Beratung auf, wo oftmals schon der Kontakt zu einem – möglicherweise auf ein

bestimmtes Gebiet wie Steuerstrafrecht spezialisierten – Berater vertraulich bleiben muss. So hat der Steuerberater Matthias M. aus Baden-Württemberg hat bei einigen Mandanten festgestellt, dass sie den Weg der Kommunikation über das Telefon seit Inkrafttreten der Vorratsdatenspeicherung scheuen. Dies hält er für sehr bedenklich, weil in der Vergangenheit immer wieder der Fall eingetreten ist, dass Mandanten angefragt haben, ob diese oder jene steuerliche Gestaltung noch mit dem Steuerrecht konform ist. Solche Fälle konnte Herr M. häufig telefonisch mit einem kurzen Ja oder Nein beantworten und dem Mandant aufzeigen, dass es immer besser ist, auf dem ‚Pfad der Tugend' zu bleiben. Seine Befürchtung ist nun jedoch, dass es Mandanten zu kompliziert oder zeitaufwendig wird, derartige Dinge jedes Mal persönlich zu klären und somit auch schneller der Fall eintreten kann, dass sich die Mandanten mangels Beratung strafbar machen. Der Rechtsanwalt und Notar Dr. Engelbert S. aus Hessen hat wegen der Vorratsdatenspeicherung Mandanten ernsthaft davor gewarnt, durch Telefon, Fax oder E-Mail mit ihm Kontakt aufzunehmen oder Schriftstücke zu übermitteln. Dies habe zu einem Rückgang von Anfragen geführt, weil persönliche Besuche mit höherem Aufwand verbunden sind. Der Wirtschafts- und Finanzberater Jens-Oliver W. berichtet, seit Inkrafttreten der Vorratsdatenspeicherung sei mit einigen Mandanten eine telefonische Kommunikation nicht mehr möglich. Vermutlich werde er diese Mandanten nicht mehr betreuen können, da die Wege- und Zeitaufwandskosten in keinem Verhältnis mehr zum Verdienst stehen.

71. Im Bereich der Wirtschaft bringt die Vorratsdatenspeicherung ebenfalls schwere Probleme mit sich. Bei Vertragsverhandlungen und Geschäftsbeziehungen ist absolute Vertraulichkeit schon der Kommunikationsbeziehung oftmals essentiell. Unternehmen kommunizieren beispielsweise anonym, um Wirtschaftsspionage im Zusammenhang mit Vertragsverhandlungen zu verhindern, aber auch um sich selbst bei Wettbewerbern zu informieren, ohne ihre Identität preisgeben zu müssen. Erwin W. aus Bayern berichtet, Kunden oder Interessenten hätten technische Zeichnungen oder sicherheitsrelevante Beschreibungen, die für die Fertigung von Prototypen benötigt werden, früher per E-Mail oder Telefax übersandt. Seit Inkrafttreten der Vorratsdatenspeicherung werde dies zunehmend verweigert und müssten die Unterlagen persönlich bei den Geschäftspartnern in ganz Europa abgeholt werden. Dies sei oftmals nicht zu leisten. Das Unternehmen habe deswegen bereits einen Großkunden verloren, von dem 2-3 Arbeitsplätze abhingen. Der Betriebsrat Joachim B. aus Bayern berichtet, dass sich Mitarbeiter nicht mehr per E-Mail an ihn wenden, obwohl einige arbeitsrechtlich relevante Fälle möglichst unverzüglich geklärt werden müssten. Torsten T. aus Hessen ist Firmeninhaber und schaltet sein Mobiltelefon seit Inkrafttreten der Vorratsdatenspeicherung ab, weil er befürchtet, mit Straftaten in Verbindung gebracht zu werden, in deren Nähe er zufällig telefoniert hat. Die Deaktivierung des Mobiltelefons schade ihm jedoch wirtschaftlich.

72. Schließlich sind Menschen in besonderen Situationen (z.B. Notlagen, Krankheiten) zur Suche nach Informationen, zur Inanspruchnahme von Beratung und Hilfe sowie

zum Austausch untereinander (z.B. Chatrooms für Opfer sexuellen Missbrauchs) nur bereit, wenn dies anonym und nicht rückverfolgbar möglich ist. Oftmals lässt sich bereits aus dem Kontakt zu einer bestimmten Beratungsstelle oder zu einem bestimmten Arzt auf die zugrunde liegende Erkrankung, Abhängigkeit o.ä. schließen. Der Sozialpädagoge und Suchtberater Konstantin H. aus Schleswig-Holstein berichtet, in der niedrigschwelligen Arbeit mit Drogenabhängigen sei die Zahl der telefonischen Kontakte seit dem 1.1.2008 und der damit in Deutschland einsetzenden Vorratsdatenspeicherung „stark zurückgegangen". Die Abhängigen fürchteten eine Strafverfolgung. Durch die Personalstruktur in der Beratungsstelle – ein Berater müsse 200 Klienten betreuen – sei eine andere als telefonische Beratung oft nicht möglich; zudem bedürften die Klienten aufgrund von Begleiterkrankungen wie Hepatitis oftmals akuter medizinischer Behandlung. Der Rückgang der telefonischen Beratungsanfragen könne den Gesundheitszustand der Betroffenen sehr verschlechtern. Der Facharzt Achim R., der in einem Berliner Klinikum arbeitet, berichtet von mehreren Patienten, die nach Inkrafttreten der Vorratsdatenspeicherung von telefonischen Kontaktaufnahmen zwecks Beratung abgesehen hätten, wodurch medizinisch gefährliche Verzögerungen des Therapiebeginns entstanden seien. Beispielsweise habe sich die Behandlung einer Tumorerkrankung verzögert und sei der Tumor in der Zwischenzeit weiter gewachsen. Die Psychotherapeutin Cornelia P. aus Baden-Württemberg hat im Monat nach Inkrafttreten der Vorratsdatenspeicherung nahezu keine Anfragen per E-Mail oder Telefon nach Paartherapie, Eheberatung und Psychotherapie mehr erhalten.

73. Weitere Berichte über die Auswirkungen der Vorratsdatenspeicherung sind dem Bundesverfassungsgericht vorgelegt worden.[87]

74. Übrigens kommunizieren auch Regierungsbehörden (z.B. Nachrichtendienste) anonym, um im Internet recherchieren zu können, ohne als Regierungsbehörde identifizierbar zu sein. Zugleich sind Behörden 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").

75. **Meinungsumfragen belegen Abschreckungswirkung**

76. Um einen repräsentativen Überblick über die Auswirkungen der Vorratsdatenspeicherung zu gewinnen, ist eine repräsentative Umfrage des Meinungsforschungsinstituts Forsa unter 1.002 Bundesbürgern am 27./28. Mai 2008 durchgeführt worden.[88] Dem Umfrageergebnis zufolge würde die Mehrheit der Befragten wegen der Vorratsdatenspeicherung davon absehen, per Telefon, E-Mail oder Handy Kontakt zu einer Eheberatungsstelle, einem Psychotherapeuten oder einer Drogenberatungsstelle aufzu-

87 Schriftsatz vom 11.02.2009, http://www.vorratsdatenspeicherung.de/images/-schriftsatz_2008-02-11_anon.pdf.

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

nehmen, wenn sie deren Rat benötigten (517 der Befragten). Hochgerechnet entspricht dies über 43 Mio. Deutschen. Jede dreizehnte Person gab an, wegen der Verbindungsdatenspeicherung bereits mindestens einmal darauf verzichtet zu haben, Telefon, Handy oder E-Mail zu benutzen (79 der Befragten). Hochgerechnet entspricht dies 6,5 Mio. Deutschen. Jede sechzehnte Person 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).

77. Des weiteren hat der Deutsche Fachjournalistenverband eine Online-Befragung (Vollerhebung) freier Journalisten in Auftrag gegeben, die vom 8. bis 27. April 2008 durchgeführt wurde.[89] Es nahmen 1.630 freie Journalisten teil. Jeder vierzehnte Journalist erklärte, die Vorratsdatenspeicherung habe sich bereits negativ auf die Kommunikation mit seinen Informanten ausgewirkt. Jeder fünfte hält abschreckende Auswirkungen der Vorratsdatenspeicherung zumindest für möglich.[90]

78. Beide Umfragen weisen nach, dass bereits von der Vorratsdatenspeicherung und dem ihr inhärenten Risiko einer Offenlegung oder Auswertung der protokollierten Informationen schwere Nachteile für die Betroffenen ausgehen, unabhängig von der Frage, ob auf die Daten später tatsächlich zugegriffen wird oder nicht. Millionen von Menschen haben wegen der Vorratsdatenspeicherung in bestimmten Situationen bereits auf elektronische Kontaktaufnahmen verzichtet, weil sie etwaige Nachteile infolge der Protokollierung des Kontakts nicht verhindern können. Tausende von Journalisten und Berufsgeheimnisträgern werden in ihrer beruflichen Tätigkeit durch die globale Protokollierung sämtlicher elektronischer Kontakte gestört. Jede zweite Person würde im Fall der Hilfsbedürftigkeit keine telefonische Hilfe mehr in Anspruch nehmen. Es liegt auf der Hand, dass in vielen dieser Fälle auch eine persönliche Kontaktaufnahme zu einer Hilfseinrichtung unterbleiben wird und dass daraus – etwa in Fällen von Gewaltproblemen – Gesundheits- und Lebensgefahren für die Betroffenen und ihre Mitmenschen erwachsen können.

79. Im Fall S. und Marper argumentierte der EGMR, die Vorratsspeicherung biometrischer Daten sei im Fall besonderer Personengruppen besonders schädlich, nämlich im Fall von Minderjährigen.[91] Wie oben gezeigt, ist auch die Vorratsspeicherung von Kommunikationsdaten für die oben genannten Personengruppen besonders schädlich.

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

90 a.a.O., 22.

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

80. **Bedeutung von Anonymität für unsere Gesellschaft**

Gary Marx nennt insgesamt 15 Funktionen von Anonymität in unserer Gesellschaft,[92] welche eine Vorratsdatenspeicherung beeinträchtigt:

1. Erleichterung des Informations- und Kommunikationsflusses über öffentliche Angelegenheiten durch Schutz des Informationsgebers (z.B. Hotlines zur anonymen Anzeige von Problemen oder Verstößen durch Whistle Blower, anonyme Informanten der Presse).
2. Ermöglichung der wissenschaftlichen Erforschung von Sachverhalten, über die nur im Schutz der Anonymität Auskunft gegeben wird (z.B. Telefonstudien über Sexualverhalten, 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 eige-

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

nen 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, nicht rückverfolgbare und anonyme Briefe schreiben zu können).

In all diesen Situationen kann eine freie, unbefangene und im allem vertrauliche Kommunikation nur im Schutz fehlender Rückverfolgbarkeit erfolgen und verhindert die Richtlinie 2006/24/EG das Gebrauchmachen von grundrechtlich geschützten Freiheiten.

dd) Verletzung der Unschuldsvermutung

81. Im Fall S. und Marper leitete der EGMR aus dem Grundgedanken der Unschuldsvermutung ab, dass Nichtverurteilte einen Anspruch darauf hätten, nicht ebenso wie verurteilte Straftäter behandelt zu werden. In einer solchen Gleichbehandlung von Ungleichem liege eine Stigmatisierung der Betroffenen.[93]

    Dasselbe gilt für die Vorratsspeicherung von Telekommunikationsdaten. Nach der Richtlinie 2006/24/EG wird nicht nur das Kommunikationsverhalten Verdächtiger aufgezeichnet, sondern sogar das Kommunikationsverhalten gänzlich Unverdächtiger und Unbeteiligter. Rechtschaffene Bürger haben aber einen Anspruch darauf, nicht allesamt wie Verdächtige einer Straftat behandelt zu werden. Nur bei dem Verdacht einer Straftat darf der Staat die Aufzeichnung von Informationen über die Telekommunikation einer Person anordnen.

ee) Weitere Rechtsprechung

82. Im Jahr 2008 urteilte das deutsche Bundesverfassungsgericht, dass die automatisierte flächendeckende und anlasslose Erhebung der Kennzeichen von Kraftfahrzeugen selbst dann unverhältnismäßig ist, wenn die Daten nur mit Fahnungsausschreibungen abgeglichen und, wenn das Kennzeichen nicht zur Fahndung ausgeschrieben ist, ohne menschliche Kenntnisnahme sofort wieder gelöscht werden.[94]

83. Hiervon ausgehend ist offensichtlich, dass die von der Richtlinie 2006/24/EG angeordnete Vorratsdatenspeicherung als flächendeckende und anlasslose Maßnahme, deren Ergebnisse nicht sogleich wieder gelöscht werden und die gerade die Erstel-

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

94 BVerfG, Urteil vom 11.03.2008, Az. 1 BvR 2074/05 und 1 BvR 1254/07, http://www.bverfg.de/entscheidungen/rs20080311_1bvr207405.html.

lung von Kommunikations- und Bewegungsprofilen ermöglichen sollen, unverhältnismäßig ist. Zum Kfz-Kennzeichenabgleich hat das Bundesverfassungsgericht entschieden, dass eine anlasslose oder flächendeckende Speicherung des Bewegungsverhaltens verfassungswidrig ist. Eben dies ist aber Gegenstand der angefochtenen Regelungen, denen zufolge der Standort von Mobilfunknutzern zu Beginn jeder ein- oder ausgehenden Verbindung zu speichern ist. Im Vergleich zum Kraftfahrzeugverkehr ist unsere Fernkommunikation sogar noch weitaus sensibler und schutzbedürftiger, wie oben gezeigt worden ist. Das Kommunikationsverhalten einer Person und ihr soziales Netzwerk lässt noch größere Rückschlüsse auf ihre Persönlichkeit zu als ihre Bewegungen.

84. Im Jahr 2007 hat der EGMR ausdrücklich entschieden, dass die Sammlung der Verkehrsdaten von Arbeitnehmern des öffentlichen Dienstes nur „in bestimmten Situationen“ zulässig sein kann.[95]

ff) Drohender Dammbruch

85. Die Zulassung einer Vorratsdatenspeicherung durch den Gerichtshof wäre ein grundrechtlicher Dammbruch. Die globale Speicherung von Daten allein für eine mögliche künftige staatliche Verwendung würde allmählich alle Lebensbereiche erfassen, denn die vorsorgliche Protokollierung personenbezogener Daten ist für den Staat stets und in allen Bereichen nützlich.[96] Aus jedem personenbezogenen Datum können sich im Einzelfall einmal Schlüsse bezüglich einer begangenen oder geplanten schweren Straftat ergeben. Das Grundrecht auf informationelle Selbstbestimmung und das gesamte Datenschutzrecht beruhen indes auf dem Gedanken, dass nicht bereits die bloße Möglichkeit, dass ein Datum irgendwann in der Zukunft einmal gebraucht werden könnte, dessen Speicherung rechtfertigt, weil ansonsten sämtliche personenbezogene Daten unbegrenzt auf Vorrat gespeichert werden dürften. Dies aber wäre eine unverhältnismäßige und unangemessene Beeinträchtigung des Persönlichkeitsrechts der Betroffenen, denen aus der Aufbewahrung und späteren Verwendung personenbezogener Daten schwere Nachteile entstehen können.

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

87. Wenn eine flächendeckende Erfassung persönlicher Lebenssachverhalte ins Blaue hinein selbst bei der besonders sensiblen und geschützten Telekommunikation zuläs-

95 EGMR, Copland-UK (2007), MMR 2007, 431 (432), Abs. 48.

96 Klug/Reif, RDV 2008, 89 (93).

sig wäre, wäre sie auch überall sonst zulässig. Die Vorratsspeicherung von Flugreisen und Nahverkehrsfahrten, von Fahrzeugbewegungen auf Autobahnen, von Aufzeichnungen privater Überwachungskameras, von Einkäufen in Geschäften und Ausleihvorgängen in Büchereien sind allesamt Beispiele einer Vorratsspeicherung, die in einigen Staaten geplant oder bereits realisiert sind und in der EU auch schrittweise eingeführt würden. Es droht auch eine Totalerfassung von Schiffs- und Bahnreisen, des Brief- und Postverkehrs einschließlich der bestellten Zeitschriften und Zeitungen, der Stromnutzung und von Warenbestellungen. Dass diese Gefahr nicht imaginär ist, zeigen die unermesslichen „Data Warehouses" der USA, in denen schon heute über die gesamte Bevölkerung Telekommunikations-Verkehrsdaten,[97] Flugreisedaten,[98] Zahlungsverkehrsdaten[99] und Daten aus den verschiedensten privaten Datenbanken zusammen geführt werden.[100]

88. Wenn dem Staat die permanente Aufzeichnung des Verhaltens sämtlicher seiner Bürger ohne Anlass gestattet würde, würden schrittweise sämtliche Lebensbereiche in einer Weise registriert werden, wie es selbst unter früheren totalitären Regimes wie der DDR undenkbar war. Ein freiheitlicher Rechtsstaat, der das Verhalten eines jedes einzelnen seiner Bürger anlasslos erfassen lässt, hört auf, ein freiheitlicher Rechtsstaat zu sein und gibt seine eigenen Grundprinzipien auf. Diese Prinzipien sind nach dem Zusammenbruch des Dritten Reiches als unverbrüchliche Grundlage unserer Gesellschaft und des Weltfriedens in der Europäischen Menschenrechtskonvention festgeschrieben worden (vgl. Präambel), auf dass sie nie wieder aufgegeben werden mögen. Das Hohe Gericht ist aufgerufen, diesen grundlegenden Rechten im vorliegenden Verfahren zur Durchsetzung zu verhelfen und durch Aufhebung der Vorratsdatenspeicherung die Grundvoraussetzungen einer freien Kommunikation in unserer Gesellschaft wieder herzustellen.

gg) Ergebnis

89. Insgesamt ist festzuhalten, dass eine generelle, flächendeckende und permanente Aufzeichnung von Telekommunikationsdaten der gesamten Bevölkerung das Verhältnismäßigkeitsgebot verletzt.[101] Die Abwägung ergibt, dass eine Speicherung des

97 New York Times vom 24.12.2005, http://www.nytimes.com/2005/12/24/politics/24spy.html; USA Today vom 05.11.2006, http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

98 Wikipedia-Eintrag „Automated Targeting System", http://en.wikipedia.org/wiki/Automated_Targeting_System.

99 New York Times vom 23.06.2006, http://www.nytimes.com/2006/06/23/washington/23intel.html.

100 Electronic Privacy Information Center, http://epic.org/privacy/choicepoint/.

101 Bäumler/v. Mutius-Bäumler, Anonymität im Internet (2003), 8; Bizer, DuD 2007, 586 (588); Gitter/Schnabel, MMR 2007, 411 (414); Gola/Klug/Reif, NJW 2007, 2599 (2600 und 2602); dies., Datenschutz- und presserechtliche Bewertung der „Vorratsdatenspeicherung" (2007), 42; Klug/Reif, RDV 2008, 89 (93); Krader, DuD 2001, 344 (347); Kugelmann, DuD 2001, 215 (220); Puschke/Singelnstein, NJW 2008, 113 (118); Singelnstein, DANA 2008, 65 (66); Uhe/Herrmann, Überwachung im Internet, http://ig.cs.tu-berlin.de/oldstatic/da/2003-08/UheHerrmann-Diplomarbeit-082003.pdf, 164 m.w.N.; Ul-

Kommunikationsverhaltens der gesamten Bevölkerung grob unverhältnismäßig ist. Die staatlichen Behörden fragen nur einem geringen Teil der Ermittlungsverfahren (etwa 0,006%) die zusätzlich gespeicherten Telekommunikationsdaten jemals nach, während mehr als 99% der von der Maßnahme Betroffenen[102] vollkommen unschuldig, unverdächtig und ungefährlich sind. Eine generelle Vorratsspeicherung von Telekommunikationsdaten, wie sie die Richtlinie 2006/24/EG vorsieht, ist daher mit Art. 8 EMRK unvereinbar.[103]

2. Verletzung der Freiheit der Meinungsäußerung (Artikel 10 EMRK)

90. Art. 10 EMRK schützt unter anderem die ungehinderte Mitteilung und den freien Empfang von Tatsachen und Meinungen.[104] In technischer Hinsicht geschützt sind alle Kommunikationsformen,[105] also auch die Nutzung der Telekommunikationsnetze. Es kommt nicht darauf an, ob es sich um private oder um öffentliche, um individuelle oder um Massenkommunikation handelt.[106]

---

mer/Schrief, DuD 1994, 591 (596); Weßlau, ZStW 113 (2001), 681 (703); Westphal, EuR 2006, 706 (720 f.); Zöller, GA 2007, 393 (412 f.); Deutscher Anwaltverein, Stellungnahme vom August 2007, http://www.anwaltverein.de/03/05/2007/41-07.pdf, 39; Bundesrechtsanwaltskammer, Stellungnahme vom August 2007, http://brak.de/seiten/pdf/Stellungnahmen/2007/Stn31.pdf, 43; Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, DuD 2004, 603 (604 f.); Artikel-29-Gruppe der EU, Stellungnahme 5/2002, http://europa.eu.int/comm/internal_market/-privacy/docs/wpdocs/2002/wp64_de.pdf; Bundesbeauftragter für den Datenschutz, 19. Tätigkeitsbericht, BT-Drs. 15/888, 78; Bundesregierung in BT-Drs. 13/4438, 39; Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Entschließung vom 25./26.03.1999, http://www.datenschutz-berlin.de/doc/de/konf/57/telekomm.htm; Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Entschließung vom 24./25.10.2002, BT-Drs. 15/888, 199; Konferenz der Europäischen Datenschutzbeauftragten, Entschließung vom 09.-11.09.2002, BT-Drs. 15/888, 176; Konferenz der Europäischen Datenschutzbeauftragten, Entschließung vom 10.-11.05.2001), BT-Drs. 15/888, 178; Konferenz der Europäischen Datenschutzbeauftragten, Entschließung vom 06./07.04.2000, BT-Drs. 14/5555, 211.

102 Schaar, http://www.heise.de/ct/aktuell/meldung/62231.

103 Ebenso: Deutscher Anwaltverein, Stellungnahme vom August 2007, http://www.anwaltverein.de/03/-05/2007/41-07.pdf, 35 f.; Art. 29-Gruppe der EU, Stellungnahme 5/2002, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp64_de.pdf und Stellungnahme 9/2004, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp99_de.pdf; Covington & Burling, Memorandum of laws concerning the legality of data retention with regard to the rights guaranteed by the European Convention on Human Rights vom 10.10.2003, http://www.statewatch.org/news/2003/oct/Data_Retention_Memo.pdf, 3; Empfehlung des Europäischen Parlaments zu der Strategie zur Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität (2001/2070(COS)) vom 06.09.2001, Dokument Nr. T5-0452/2001, Buchst. H; EDSB-Konferenz, Europäische Datenschutzbeauftragte: Statement at the International Conference in Cardiff (09.-11.09.2002) on mandatory systematic retention of telecommunication traffic data, BT-Drs. 15/888, 176.

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

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

106 Vgl. Frowein/Peukert-Frowein, Art. 10, Rn. 15 ff.

91. Die vorbeugende, generelle Aufzeichnung der näheren Umstände der Telekommunikation greift in die Meinungsfreiheit der Betroffenen ein. Der Zweck des Art. 10 EMRK gebietet es, dem Staat auch eine mittelbare Behinderung der freien Kommunikation als Eingriff zuzurechnen, wenn die Maßnahme typischerweise und vorhersehbar den Austausch von Meinungen und Tatsachenbehauptungen beeinträchtigt. Wie schon zu Art. 8 EMRK gezeigt, ist dies bei einer generellen Vorratsspeicherung von Telekommunikations-Verkehrsdaten der Fall. Eine Behinderung der Kommunikation erfolgt durch den Abschreckungseffekt, der mit einer generellen Vorratsspeicherung von Verkehrsdaten verbunden ist. Die Richtlinie 2006/24/EG stellt damit einen Eingriff in Art. 10 EMRK dar.

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

93. Die Richtlinie 2006/24/EG bewirkt die Rückverfolgbarkeit jeder Meinungsäußerung und jeder Information über die Meinung anderer, die über Telekommunikationsnetze erfolgt. Dies hält Menschen, die das Risiko eines Bekanntwerdens ihres elektronischen Kommunikations- und Bewegungsverhaltens nicht eingehen wollen, von einem freien Meinungsaustausch ab. Das gilt besonders für politische und staatskritische Aktivitäten und für die vertrauliche Weitergabe von Informationen an die Presse.

94. Die Befürchtungen, der Staat werde Telekommunikationsdaten auch zur politischen Überwachung nutzen, sind nicht irreal, wie ein Bericht über die Möglichkeiten des Einsatzes von „Technologien zur politischen Kontrolle“, den das Europäische Parlament erstellen ließ, zeigt.[107] Der Bericht führt aus, dass ein Großteil moderner Überwachungstechnologie in Teilen der Welt eingesetzt wird, um die Aktivitäten von Dissidenten, Menschenrechtsaktivisten, Journalisten, Studentenführern, Minderheiten, Gewerkschaftsführern und politischen Gegenspielern zu überwachen.[108] Selbst der britische Geheimdienst GCHQ soll unschuldige Menschenrechtsorganisationen wie Amnesty International und Christian Aid überwachen.[109]

95. Im Jahr 2005 ist bereits bekannt geworden, dass der US-amerikanische Nachrichtendienst NSA seit dem 11.09.2001 in großem Umfang Telekommunikations- und Internetverbindungsdaten erhebt und analysiert.[110] Die gesammelten Daten werden nach

107 Omega Foundation, An Appraisal of the Technologies of Political Control (1998), http://cryptome.org/stoa-atpc-so.htm.

108 Omega Foundation, An Appraisal of the Technologies of Political Control (1998), http://cryptome.org/stoa-atpc-so.htm, Punkt 7.

109 Omega Foundation, An Appraisal of the Technologies of Political Control (1998), http://cryptome.org/stoa-atpc-so.htm.

110 Lichtblau/Risen: Spy Agency Mined Vast Data Trove, Officials Report, New York Times, 24.12.2005, http://nytimes.com/2005/12/24/politics/24spy.html?hp&ex=1135486800&en=7e76956223502390&-

Auffälligkeiten durchsucht (sog. „Musteranalyse“),[111] um daran weitere Maßnahmen gegen die ausgefilterten Personen anschließen zu können. Der ehemalige Manager eines Telekommunikationsunternehmens sagte der New York Times: „Wenn sie Inhalte bekommen können, ist das für sie auch nützlich, aber die wirkliche Gelegenheit stellen Transaktionsdaten und die Analyse von Verkehrsdaten dar. Immense Mengen an Verkehrsdaten [...] werden genutzt, um Kommunikationslinien zu identifizieren, die dann näher unter die Lupe genommen werden.“ Nach dem Ende der Amtszeit des US-Präsidenten George Bush hat der ehemalige Mitarbeiter der Nationalen Sicherheitsbehörde NSA Russell Tice enthüllt, dass die NSA auf diese Weise sämtliche in den USA anfallende Verkehrsdaten illegal auf Vorrat speichert und auswertet und es dabei insbesondere auf die Kommunikation und Bewegungen von Journalisten abgesehen hat.[112] Die Vorratsdatenspeicherung ermöglicht ähnlichen Missbrauch auch in Europa. Die Richtlinie 2006/24/EG begründet das Risiko, dass die gespeicherten Telekommunikationsdaten zu einer breit angelegten Überwachung grundrechtlich geschützten Verhaltens genutzt werden.

96. Gerade Verkehrsdaten erlauben es, soziale Netzwerke zu identifizieren, etwa die Mitglieder einer Organisation, einer Gruppe von Atomkraft- oder Globalisierungskritikern, eines Unternehmens.[113] Auch die Freunde und Unterstützer dieser Organisation können identifiziert werden, ebenso ihre Hierarchie, Anführer, Beziehungen zueinander, Treffpunkte, Entscheidungsfindungsprozesse.[114] Die Kontakte von Organisationen zueinander können aufgedeckt werden.[115] Schon die Verkehrsdaten weniger Angehöriger der Organisation erlauben die Aufdeckung und Beobachtung aller Beziehungen des Netzwerks.[116] Verkehrsdaten sind damit besonders geeignet zur politischen Kontrolle von Personen und Gruppierungen, die von ihrem Recht auf freie Meinungsfreiheit Gebrauch machen. Die Artikel-29-Datenschutzgruppe stellt fest: „Allein dadurch, dass es sie gibt, ermöglichen es Kommunikationsdaten, persönliches Verhalten in einem bisher ungekannten Maße zu überwachen und zu kontrollieren.“[117]

97. Telekommunikationsdaten werden in der Praxis der Ermittlungsbehörden in Datenbanken wie „rsCase“ eingestellt. Aufgrund der großen Datenmengen kann bei Aus-

ei=5094&partner=homepage.

111 Bush, zit. bei Pricacy International, US Government accused of communications data retention and data mining, 12.05.2006, http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-537226.

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

113 Danezis, Traffic Data Retention, http://www.worldcivilsociety.org/onlinenews/docs/18.09_danezis_george_wcsf-position.pdf, 3 f.

114 Danezis, Traffic Data Retention, http://www.worldcivilsociety.org/onlinenews/docs/18.09_danezis_george_wcsf-position.pdf, 3 f.

115 Danezis, Traffic Data Retention, http://www.worldcivilsociety.org/onlinenews/docs/18.09_danezis_george_wcsf-position.pdf, 3 f.

116 Danezis, The Economics of Mass Surveillance, http://weis2006.econinfosec.org/docs/36.pdf, 13.

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

wertung der Daten zwangsläufig nur nach dem Muster der Rasterfahndung vorgegangen werden, indem nach bestimmten, auffälligen Merkmalen gesucht wird („Data Mining", „Verdachtssuche"). Gerade diese Vorgehensweise fügt der freien Kommunikation in unserer Gesellschaft großen Schaden zu. Jeder, dessen Kommunikationsverhalten von dem des europäischen Durchschnittsbürgers abweicht, hat dann nämlich zu befürchten, allein wegen dieses abweichenden Verhaltens von den Behörden unter die Lupe genommen zu werden und weiteren Ermittlungen, die zwangsläufig das Risiko von Vor- und Fehlurteilen mit sich bringen, ausgesetzt zu werden.

98. Der US-amerikanische Oberste Gerichtshof (Supreme Court) hat bereits in der frühen Entscheidung Talley v. California[118] ausgesprochen, dass die „anonyme Meinungsäußerung" eine wertvolle Rolle für den „Fortschritt der Menschheit" gespielt habe. Anonymität sei mitunter für überaus wertvolle Zwecke genutzt worden. Verfolgte Gruppen seien im Lauf der Geschichte nur im Schutz der Anonymität in der Lage gewesen, Unterdrückungspraktiken und –gesetze zu kritisieren. Auch könne eine „Identifizierung und die Furcht vor Vergeltung von vollkommen friedlichen Diskussionen wichtiger öffentlicher Angelegenheiten abschrecken". Eine Pflicht zur Nennung der Verantwortlichen auf Flugzetteln hat er daher als Verstoß gegen die Meinungsfreiheit verworfen.

99. In einer späteren Entscheidung[119] 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".

100. Der Oberste Gerichtshof hat auch anerkannt, dass Vereine die Liste ihrer Mitglieder nicht offen legen müssen.[120] Es müsse möglich bleiben, anonym Mitglied eines unbeliebten Vereins zu sein, um die Freiheit auch unpopulärer Meinungen zu gewährleisten.

101. Diese Erwägungen zum Recht auf anonymen Meinungsaustausch lassen sich auf das Recht zum spurenlosen Meinungsaustausch übertragen. Die vermeintliche Anonymität der elektronischen Kommunikation ist wertlos, wenn sie mithilfe von Telekommunikationsdaten jederzeit aufgehoben werden kann. Es ist den Bürgern auch nicht zumutbar, nur noch anonyme Telekommunikationsdienste zu nutzen, zumal solche teuer, in vielen Situationen unpraktikabel und in einigen Mitgliedsstaaten sogar verboten sind (z.B. in Deutschland). In einer demokratischen Gesellschaft muss es -

118 362 U.S. 60 (1960).

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

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

z.B. durch Buchen einer „Flatrate“ - möglich sein, über den eigenen Telefonanschluss anonyme Informationen an die Presse weiter zu geben oder eine Demonstration zu koordinieren, ohne dass jeder Kontakt protokolliert und nachvollziehbar gemacht wird.

102. In einer ausführlichen Untersuchung gelangt Catherine Crump ausgehend von der genannten Rechtsprechung des Obersten Gerichtshofs zu dem Ergebnis, dass eine Vorratsdatenspeicherung das Recht auf freie Meinungsäußerung verletzt.[121] Eine Vorratsdatenspeicherung eliminiere die anonyme Äußerung von Meinungen im Internet, weil durch sie jede Meinungsäußerung über Telekommunikationsnetze rückverfolgbar werde. Außerdem werde die anonyme Bildung von Vereinigungen über Telekommunikationsnetze unmöglich, weil sich Mitgliedschaften in einer Internet-Vereinigung – etwa derjenigen des Antragstellers – mithilfe von Telekommunikationsdaten aufdecken ließen.

103. Dass der Oberste Gerichtshof die Aufklärung von Straftaten zur Rechtfertigung einer flächendeckenden Vorratsdatenspeicherung nicht würde genügen lassen, begründet die Autorin mit den folgenden Ausführungen des Gerichtshofs in einem Urteil aus dem Jahr 2002: „Das Argument geht im Kern dahin, dass geschützte Meinungsäußerungen verboten werden dürften, um ungeschützte Meinungsäußerungen verhindern zu können. Diese Analyse stellt die Meinungsfreiheit auf den Kopf. Der Staat darf rechtmäßige Meinungsäußerungen nicht unterdrücken, um unrechtmäßige Meinungsäußerungen zu verhindern. [...] Die Verfassung gebietet das Gegenteil.“[122] Schon in einer früheren Entscheidung hatte der Gerichtshof ausgeführt, „in unserer Gesellschaft hat der Wert freier Meinungsäußerung ein höheres Gewicht als die Gefahren ihres Missbrauchs“.[123]

104. Die Autorin sieht in einer Vorratsdatenspeicherung eine Verletzung dieser Grundsätze, weil eine Vorratsdatenspeicherung zur Aufklärung unrechtmäßiger Handlungen unterschiedslos auch rechtmäßige Meinungsäußerungen erfasst und rückverfolgbar macht. Die Autorin gelangt zu dem folgenden Ergebnis: „Untersucht man eine Vorratsspeicherungspflicht im Lichte der vom Gerichtshof anerkannten Bedeutung anonymer Meinungsäußerung, so gibt es überzeugende Gründe dafür, sie wegen ihrer Auswirkungen auf anonyme Meinungsäußerungen als verfassungswidrig anzusehen.“[124]

105. Wie zu Art. 8 EMRK gezeigt worden ist, steht der schwerwiegenden Beeinträchtigung der Meinungsfreiheit durch die Vorratsdatenspeicherung keine nennenswerte Erleichterung der Strafverfolgung gegenüber. Damit stellt die Richtlinie 2006/24/EG einen unverhältnismäßigen und unzumutbar tiefen Eingriff auch in die Rechte aus Art. 10 EMRK dar.

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

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

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

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

106. Die Richtlinie 2006/24/EG ist daher mit Art. 10 EMRK unvereinbar und ungültig.

III. Unvereinbarkeit der Vorratsspeicherung von IP-Adressen mit der Richtlinie 95/46/EG

107. Unter Ziff. 6 fragt das vorlegende Gericht, ob Art. 7 - und hier insbesondere Buchstabe e - der Richtlinie 95/46/EG dahin auszulegen ist, dass er einer Praxis, die IP-Adressen der Benutzer einer Homepage ohne deren ausdrücklicher Einwilligung zu speichern, entgegensteht. Diese Frage ist zu bejahen.

1. Anwendbarkeit der Richtlinie 95/46/EG

108. Nach Art. 7 RiL 95/46/EG dürfen personenbezogene Daten nur unter bestimmten Voraussetzungen verarbeitet werden. Wenn der Betreiber eines Internetportals die IP-Adressen der Nutzer des Portals speichert, verarbeitet er personenbezogene Daten.

109. Nach Art. 2 RiL 95/46/EG sind „personenbezogene Daten“ alle Informationen über eine bestimmte oder bestimmbare natürliche Person. Nach Art. 2 RiL 95/46/EG wird eine Person als bestimmbar angesehen, wenn sie direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennummer. Nach Erwägungsgrund 26 der Richtlinie sollten bei der Entscheidung, ob eine Person bestimmbar ist, alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen.

110. Eine Liste der IP-Adressen der Besucher eines Internetportals enthält die Information, wer auf ein bestimmtes Internetportal zugegriffen und darauf bestimmte Informationen gelesen oder geschrieben hat.

111. Ausgehend von der IP-Adresse eines Internetnutzers ist regelmäßig die – zumeist natürliche – Person bestimmbar, auf deren Namen der genutzte Internetanschluss registriert ist. Nach der Richtlinie 2006/24/EG oder 2002/58/EG speichern die Anbieter von Internetzugängen, wem eine statische Internetkennung (IP-Adresse) zur Nutzung zugewiesen ist oder welchem Kunden zu welchem Zeitraum eine Internetkennung zur vorübergehenden Nutzung überlassen war (dynamische IP-Adresse). Da Betreiber von Internetportalen, die eine Zugriffsprotokollierung vornehmen, gewöhnlich neben der IP-Adresse der Nutzer auch den genauen Zeitpunkt des Zugriffs protokollieren, lässt sich durch Zusammenführung eines solchen Protokolls („access log“) mit den Aufzeichnungen des Internet-Zugangsanbieters des Nutzers die Person des Anschlussinhabers ermitteln. Welcher Internet-Zugangsanbieter genutzt wurde, kann jedermann ausgehend von der IP-Adresse des Nutzers über öffentliche Register im Internet feststellen.

112. Inhaber einer statischen IP-Adresse können über diese Register von jedermann unmittelbar identifiziert werden. Eine statische IP-Adresse ist daher personenbezogen.

113. Nutzer einer dynamischen IP-Adresse können jedenfalls von staatlichen Behörden identifiziert werden, welche Internet-Zugangsanbieter zur Herausgabe der erforderlichen Protokolle zwingen können (vgl. Art. 15 RiL 2002/58/EG sowie RiL 2006/24/EG). Zu einer solchen Zusammenführung kann es auch kommen, indem der Internet-Zugangsanbieter oder aber der Internetportal-Betreiber freiwillig die entsprechenden Daten an die jeweils andere Stelle übermitteln. Nach Art. 2 RiL 95/46/EG ist der Inhaber des genutzten Internetanschlusses bestimmbar, weil er zumindest indirekt identifiziert werden kann, insbesondere durch Zuordnung zu der IP-Kennummer. Nach Erwägungsgrund 26 der Richtlinie müssen bei der Entscheidung, ob der Anschlussinhaber bestimmbar ist, auch die Mittel berücksichtigt werden, die von einer staatlichen Behörde eingesetzt werden können, um die Person des Anschlussinhabers zu bestimmen. Auch eine dynamische IP-Adresse ist daher personenbezogen. Sie erlaubt die Bestimmung der Person des Inhabers des genutzten Internetanschlusses. Oftmals wird der Anschlussinhaber seinen Anschluss selbst genutzt haben.

114. Die Anwendbarkeit der Richtlinie 95/46/EG setzt danach nicht voraus, dass der Betreiber des Internetportals selbst und mit eigenen Mitteln den Inhaber des genutzten Internetanschlusses identifizieren kann. In diesem Punkt sind sich Datenschutzbehörden und Gerichte praktisch einig. Dies entspricht der Position der Artikel 29-Datenschutzgruppe der EU[125] und auch der Gerichte, die sich bislang mit der Frage befasst haben: das vorlegende Gericht,[126] das Amtsgericht Berlin,[127] das schweizerische Bundesverwaltungsgericht[128] und das schwedische Oberste Verwaltungsgericht[129]. Die Richtlinie 95/46/EG soll auch davor schützen, dass eine Identifizierung des Betroffenen erst durch die Zusammenführung mit weiteren Daten erfolgt, wie sie etwa im Fall von IP-Adressen bei dem Internet-Zugangsanbieter vorhanden sind.

115. Falsch wäre die Auffassung, eine Bestimmbarkeit des Betroffenen liege nur vor, wenn der Betroffene vom dem für die Verarbeitung Verantwortlichen mit legalen Mitteln identifiziert werden könne. Die Richtlinie 95/46/EG soll gerade vor dem Missbrauch von Daten schützen, wie er in der Praxis leider tagtäglich vorkommt. Man braucht nur die Tätigkeitsberichte der Datenschutzbeauftragten zu lesen, um festzustellen, dass

125 Stellungnahme vom 21.11.2000, WP37, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37de.pdf, 17; Stellungnahme 2/2002 vom 30.05.2002, WP58, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp58_de.pdf, 3; Stellungnahme 4/2007 vom 20.06.2007, WP136, http://ec.europa.eu/justice_home/fsj/privacy/docs/-wpdocs/2007/wp136_de.pdf, 19.

126 Abs. 36 der Gründe des Vorlagebeschlusses.

127 Urteil vom 27.03.2007, Az. 5 C 314/06, http://www.daten-speicherung.de/?p=197#ag.

128 Urteil vom 27.05.2009, Az. A-3144/2008, http://relevancy.bger.ch/pdf/azabvger/2009/-a_03144_2008_2009_05_27_t.pdf.

129 Regeringsrätten, 3978-07 vom 16.07.2009; Kammarrätt i Stockholm, 285-07 vom 08.06.2007, http://arkiv.idg.se/it24/SthlmRRejpt_3978_07.pdf.

Staat und Wirtschaft immer wieder unter Verstoß gegen Datenschutzrecht Daten übermitteln. Der Einzelne wäre schutzlos gestellt, würde man eine unbeschränkte Speicherung seiner Daten mit dem Argument zulassen, seine Person könne von der momentan speichernden Stelle mit legalen Mitteln nicht bestimmt werden. Diese Auffassung würde ein Eldorado für Kreditauskunfteien, Detekteien, Werbeunternehmen usw. eröffnen. Diese könnten dann nämlich unbegrenzt sensible Daten über jegliche Personen ansammeln und weitergeben, solange sie nicht den Namen der Betroffenen, sondern nur deren Personalausweisnummer, Kundennummer, Kontonummer o.ä. speicherten. Sie könnten sich dann darauf berufen, dass sie selbst die Betroffenen mit legalen Mitteln nicht bestimmen könnten. Dies wäre mit dem Grundrecht auf Datenschutz offensichtlich unvereinbar. Bei der Auslegung des Begriffs der Bestimmbarkeit darf das Risiko einer unbefugten Bestimmung des Betroffenen nicht unbeachtet bleiben. Das Datenschutzrecht und die dort vorgesehenen Löschungspflichten dienen gerade dazu, dieses Missbrauchsrisiko von vornherein auszuschließen.

116. Konsequenz der Verneinung des Personenbezugs von Internet-Nutzungsprotokollen wäre, dass unser Internet-Nutzungsverhalten inhaltlich und zeitlich unbegrenzt protokolliert werden dürfte. Die Schutzvorschriften der RiL 95/46/EG würden insoweit vollkommen bedeutungslos. Schon die Befürchtung eines Missbrauchs dieser Datenhalden würde die Informations- und Meinungsfreiheit im Internet unangemessen beeinträchtigen. Im Volkszählungsurteil hat das Bundesverfassungsgericht zutreffend ausgeführt: „*Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.*“[130] Auch im Internet wäre eine unbefangene Ausübung der Informations- und Meinungsäußerungsfreiheit unmöglich, wenn jeder Klick und jede Eingabe personenbeziehbar registriert werden dürfte.

117. Zwar kann es im Einzelfall einmal unmöglich sein, eine IP-Adresse einer natürlichen Person zuzuordnen, so dass die Richtlinie 95/46/EG auf dieses Datum nicht anwendbar ist. Der Betreiber eines Internet-Portals kann aber nicht erkennen, welche der IP-Adressen seiner Nutzer sich einer natürlichen Person zuordnen lassen und welche nicht. Um die Einhaltung der Richtlinie 95/46/EG zu gewährleisten, muss er folglich alle potenziell personenbezogenen IP-Adressen im Einklang mit der Richtlinie verarbeiten.[131]

130 BVerfGE 1, 43.

131 Artikel 29-Gruppe, Stellungnahme 4/2007 vom 20.06.2007, WP136, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_de.pdf, 19 f.

2. Verstoß gegen Art. 7 RiL 95/46/EG

118. Die Aufzeichnung der IP-Adressen der Benutzer einer Homepage ohne deren ausdrückliche Einwilligung verstößt gegen Art. 7 RiL 95/46/EG, weil keine der Voraussetzungen des Art. 7 erfüllt ist. Ein besonders schwerwiegender Verstoß liegt vor, wenn die Protokollierung ohne konkreten Anlass, permanent, ungezielt und flächendeckend für alle Nutzer erfolgt (Totalprotokollierung).

a) Art. 7 a-e) RiL 95/46/EG nicht einschlägig

119. Vereinbar mit Art. 7 RiL 95/46/EG ist die Verarbeitung der IP-Adresse eines Nutzers nur bis zum Abschluss der Übermittlung der Daten, die der Nutzer angefordert hat (vgl. Art. 6 (1) RiL 2002/58/EG). Zur Bereitstellung eines Internetportals ist es technisch erforderlich, dass der Betreiber die von einem Nutzer angeforderten Informationen an dessen IP-Adresse adressiert. Deswegen rechtfertigt es das berechtigte Interesse des Betreibers, die IP-Adresse eines Nutzers bis zum Abschluss des Versands der Daten, die der Nutzer angefordert hat, zu verarbeiten (Art. 7 (f) RiL 95/46/EG).

120. Art. 7 a) RiL 95/46/EG rechtfertigt eine darüber hinaus gehende Speicherung der IP-Adresse nur, wenn der Betroffene in eine solche Speicherung eingewilligt hat. Das setzt voraus, dass er von der beabsichtigten Speicherung Kenntnis hat und seine Zustimmung erklärt hat. Zu den Voraussetzungen einer wirksamen Einwilligung bestimmt Erwägungsgrund 17: „Die Einwilligung kann in jeder geeigneten Weise gegeben werden, wodurch der Wunsch des Nutzers in einer spezifischen Angabe zum Ausdruck kommt, die sachkundig und in freier Entscheidung erfolgt; hierzu zählt auch das Markieren eines Feldes auf einer Internet-Website."

121. Mit der bloßen Benutzung eines Internetportals erklärt sich ein Nutzer nicht damit einverstanden, dass der Anbieter seine IP-Adresse protokolliert und über die Dauer des Nutzungsvorgangs hinaus aufbewahrt. Die Benutzer eines Internetportals stellt keine „spezifische Angabe" im Sinne des 17. Erwägungsgrundes dar. Die meisten Nutzer haben von einer solchen Protokollierungspraxis schon keine Kenntnis. Auch im Kenntnisfall kann in der bloßen Hinnahme einer solchen Praxis keine Einwilligung gesehen werden. Das Internet ist heutzutage ein unverzichtbares Medium der Information und Kommunikation. Viele Personen sind beruflich, privat oder sonst zwingend auf die Nutzung des Internet angewiesen. Um das Internet nutzen zu können, ist es technisch notwendig, dass die IP-Adresse des Nutzers an den Betreiber des Zielservers übertragen wird. Deshalb kann in der Nutzung des Internet, welche die Übermittlung der eigenen IP-Adresse zwingend voraussetzt, keine „ohne Zwang" erklärte Einwilligung in die Speicherung der Adresse über die Dauer des Übertragungsvorgangs hinaus gesehen werden. Allenfalls bei anmeldepflichtigen Diensten ist es denkbar, dass der Anbieter die Einwilligung der Nutzer in eine Vorratsspeicherung seiner IP-Adresse einholen kann. Die Nutzung des Internetportals www.agrar-fischerei-zahlungen.de

setzt aber keine Anmeldung voraus, und die Nutzer werden auch sonst nicht um ihre Einwilligung gebeten.

122. Eine Protokollierung der IP-Adressen von Internetnutzern rechtfertigt auch Art. 7 b) RiL 95/46/EG nicht. Zwischen dem Nutzer eines Internetportals wie www.agrar-fischerei-zahlungen.de und dem Betreiber besteht weder ein Vertrag, noch wird ein Vertrag angebahnt. Es verhält sich nicht anders als mit dem Leser eines Buches, der ebenfalls keinen Vertrag mit dem Verlag schließt.

123. Bei der Inanspruchnahme entgeltlicher Internetdienste besteht zwar ein Vertragsverhältnis. Eine Protokollierung der IP-Adresse ist aber auch in diesem Fall nicht zur Gebührenabrechnung erforderlich (vgl. Art. 6 (2) RiL 2002/58/EG). Denn die Gebührenabrechnung entgeltlicher Internetdienste erfolgt anhand eines Benutzernamens, eines Passwortes und einer Sitzungskennung. Da die IP-Adresse eines Internetnutzers typischerweise von Sitzung zu Sitzung wechselt (dynamische IP-Adresse), ist sie zur Abrechnung ungeeignet.

124. Eine Protokollierung der IP-Adressen von Internetnutzern rechtfertigt auch Art. 7 c) RiL 95/46/EG nicht. Es gibt keine rechtliche Verpflichtung zu einer Protokollierung von IP-Adressen. Für kommerzielle Anbieter gibt es zwar Pflichten zur Rechnungslegung. Diese Vorschriften fordern aber nur die Aufbewahrung von Rechnungen und Geschäftsbriefen. Informationen über die Nutzung eines Internetportals müssen danach nicht aufgezeichnet werden.

125. Die Protokollierung von IP-Adressen ist nicht erforderlich für die Wahrung lebenswichtiger Interessen des Internetnutzers (Art. 7 d) RiL 95/46/EG).

126. Die Protokollierung von IP-Adressen ist nicht erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und dem für die Verarbeitung Verantwortlichen übertragen wurde (Art. 7 e) RiL 95/46/EG). Das Land Hessen bietet das Internetportal www.agrar-fischerei-zahlungen.de in Erfüllung seiner europarechtlichen Veröffentlichungspflichten an. Zur Wahrnehmung dieser Aufgabe ist es nicht erforderlich, die IP-Adressen der Besucher aufzuzeichnen und aufzubewahren. Dies ergibt sich schon aus der eigenen Information des Betreibers, wonach nur „die anonymisierte IP-Adresse des Anwenders, Datum und Uhrzeit sowie die besuchte Internetseite gespeichert“ werden soll.[132] Eine Aufzeichnung der vollständigen IP-Adresse ist folglich nach der eigenen Aussage des Betreibers nicht erforderlich.

b) Kein berechtigtes Interesse des Anbieters

127. Die Protokollierung von IP-Adressen ist nicht zur Wahrnehmung eines berechtigten Interesses des Betreibers des Internetportals erforderlich (Art. 7 f) RiL 95/46/EG). Zur Rechtfertigung kommen insbesondere die folgenden Zwecke nicht in Betracht:

132 Hinweise zum Datenschutz, http://agrar-fischerei-zahlungen.de/impressum.html.

128. **Statistik, Verbesserung des Angebots, personalisierte Angebote**

129. Zur statistischen Auswertung und Verbesserung eines Internetportals ist die Protokollierung personenbezogener Daten nicht erforderlich. Es genügt, anonyme Nutzungsprotokolle aufzuzeichnen. Mithilfe einer Sitzungsnummer („session ID“, Cookie) kann das Nutzungsverhalten einer Person anonym aufgezeichnet und ausgewertet werden.

130. Was das Angebot personalisierter Dienste oder Werbung angeht, kann der Nutzer um Einwilligung in die Verarbeitung der dazu erforderlichen Daten gebeten werden. Es besteht kein berechtigtes Interesse des Anbieters daran, allen Nutzern gegen ihren Willen und ohne ihre Einwilligung personalisierte Dienste aufzudrängen.

131. **Erkennung und Abwehr von Angriffen und Störungen**

132. Dass die Protokollierung von IP-Adressen nicht erforderlich ist, um Angriffe auf die Verfügbarkeit, Vertraulichkeit und Integrität des Webservers oder technische Störungen abzuwehren, ergibt sich schon daraus, dass eine Vielzahl von Internetangeboten ohne Protokollierung von IP-Adressen bereit gestellt wird – ohne dass darunter ihre Verfügbarkeit, Vertraulichkeit oder Integrität leiden würde. In Deutschland werden dementsprechend beispielsweise die Internetportale des Bundesjustizministeriums (www.bmj.bund.de), des Bundesdatenschutzbeauftragten (www.bfdi.bund.de), des Bundesrechnungshofes (www.bundesrechnungshof.de), des Bundesbildungsministeriums (www.bmbf.de), des Bundesverwaltungsgerichts (www.bundesverwaltungsgericht.de) und des Bundeskriminalamts (www.bundeskriminalamt.de) ohne Protokollierung der IP-Adressen der Nutzer bereit gestellt. Gleiches behauptet der aktuelle Datenschutzhinweis des Portals www.agrar-fischerei-zahlungen.de. Es ist nicht empirisch nachweisbar, dass die Protokollierung von IP-Adressen die Verfügbarkeit, Vertraulichkeit oder Integrität eines Servers erhöhen würde.

133. Angesichts dieses faktischen Belegs der fehlenden Erforderlichkeit wird an dieser Stelle darauf verzichtet, technisch im Einzelnen darzulegen, weshalb die Protokollierung von IP-Adressen über die Dauer des Nutzungsvorgangs hinaus nicht erforderlich ist, um IT-Angriffe und Störungen abzuwehren. Es sei lediglich gesagt, dass zur Abwehr von Angriffen und zur Behebung von Störungen Technologien (z.B. „Firewalls“) und Methoden zur Verfügung stehen, die eine Protokollierung der IP-Adressen der Internetnutzer über die Dauer des Übertragungsvorgangs hinaus nicht erfordern. DoS-Angriffe, unbefugte Manipulationen, Viren oder andere Infiltrierungen können nicht verhindert werden, indem man Daten sammelt. Vielmehr muss die vom Anbieter genutzte Hardware und Software so eingerichtet werden, dass sie solchen Angriffen stand hält. Sicherheitsmechanismen wie Firewalls und Software-Aktualisierungen funktionieren ohne personenbezogene Protokolle. Die Verarbeitung von IP-Adressen ist schon deswegen nicht zur Abwehr von Angriffen geeignet, weil Angreifer heutzutage eine Vielzahl wechselnder IP-Adressen („Botnetze“) und gefälschte IP-Adressen

(„IP-Spoofing“) nutzen, so dass Maßnahmen unter Anknüpfung an eine IP-Adresse zwecklos sind.

134. **Verhinderung von Klickbetrug**

135. Einige Anbieter von Werbung im Internet wollen mit der Protokollierung von IP-Adressen verhindern, dass Personen ungewöhnlich häufig auf Werbebanner klicken, um davon finanziell zu profitieren oder anderen zu schaden. Ein Vorgehen gegen Klickbetrug erfordert von vornherein allenfalls die Protokollierung der Klicks auf Werbebanner und nicht die Protokollierung des gesamten Nutzungsverhaltens auf einem Internetportal, wie es hier in Rede steht. Auch die personenbezogene Protokollierung der Klicks auf Werbebanner rechtfertigt die Protokollierung von IP-Adressen jedoch nicht, weil mildere Mittel zur Verhinderung betrügerischer Verhaltensweisen zur Verfügung stehen, etwa die Beschränkung der gezahlten Vergütung auf eine „normale“ Anzahl von Klicks pro Stunde. In Zeiten von Botnetzen ist die Anknüpfung an eine IP-Adresse ohnehin nicht mehr wirksam, um Klickbetrug zu verhinden.

136. Für das Portal www.agrar-fischerei-zahlungen.de sind diese Fragen von vornherein ohne Bedeutung, weil es sich um ein nicht-kommerzielles Angebot handelt und keine Werbebanner eingeblendet werden.

137. **Verfolgung von Angreifern**

138. Internet-Nutzungsprotokolle können im Einzelfall zur Verfolgung eines Angreifers genutzt werden, etwa zum Zweck der Strafverfolgung. Die Identifizierung von Angreifern ist allerdings in der Praxis weitgehend unmöglich. Angreifer verstecken sich verbreitet hinter fremden IP-Adressen (z.B. Anonymisierungsdienste, Proxies) oder fälschen IP-Adressen („IP spoofing“). Genutzte IP-Adressen sind meist auf obskure Personen oder Firmen in China oder im sonstigen Ausland registriert.

139. Zudem haben die Betreiber von Internet-Portalen kein berechtigtes Interesse an einer Verfolgung von Angreifern, weil die Strafverfolgung eine öffentliche Aufgabe ist. Welche Ermittlungsmaßnahmen und Datenspeicherungen zur Aufklärung des Verdachts einer Straftat rechtmäßig und verhältnismäßig sind, entscheiden öffentliche Justizbehörden und unabhängige Gerichte. Ohne richterliche Anordnung kann es einem Diensteanbieter nicht gestattet sein, auf eigene Faust rein vorsorgliche Überwachungsmaßnahmen durchzuführen. Auf die staatliche Strafverfolgung von Angreifern findet die Richtlinie 95/46/EG keine Anwendung (Art. 3 (2) RiL 95/46/EG).

c) Überwiegendes Interesse an einem Ausschluss der Vorratsspeicherung

140. Will man im Einzelfall entgegen der obigen Ausführungen ein berechtigtes Interesse eines Internetportal-Betreibers an der Protokollierung von IP-Adressen seiner Nutzer anerkennen, überwiegen jedenfalls das Interesse sowie die Grundrechte und Grundfreiheiten der betroffenen Nutzer. Internetnutzer haben einen Anspruch darauf, das

Internet ebenso protokollierungsfrei nutzen zu können, wie sie Bücher und Zeitschriften lesen oder fernsehen können.

141. Wenn wir Zeitungen, Magazine oder Bücher lesen, wenn wir im Radio Musik hören oder fernsehen, brauchen wir nicht zu befürchten, dass uns jemand über die Schulter schauen oder mitschreiben könnte. Lesen wir hingegen Zeitungen, Magazine oder Bücher im Internet, hören wir dort Musik oder betrachten wir Videos im Internet, muss der Anbieter für die Dauer der Übertragung aus technischen Gründen unsere Internet-Adresse kennen. Anhand dieser Adresse oder anderer Nutzerkennungen kann jede unserer Eingaben und jeder unserer Mausklicks beim Lesen, Schreiben und Diskutieren im Internet erfasst, aufgezeichnet, ausgewertet, weiter gemeldet und offen gelegt werden.

142. Informationen über die Internetnutzung einer Person sind hochsensibel. Im Internet betätigt und informiert man sich politisch, praktiziert seine Religion oder wird gewerkschaftlich tätig. Man diskutiert und informiert sich über seine Krankheiten, über sexuelle Fragen und über Probleme und Notlagen (z.B. verfolgte Personen, bei Eheproblemen, Missbrauchsopfer). Die Aufzeichnung von IP-Adressen ermöglicht tiefgreifende Rückschlüsse auf das Privatleben, die Persönlichkeit, die Einstellungen, die Interessen und die Schwächen der Betroffenen.

143. Eine Erfassung unseres Internet-Nutzungsverhaltens ist nicht nur einer Filmaufzeichnung unseres Zeitungslesens oder Fernsehens vergleichbar. Vielmehr können Internet-Nutzungsdaten – anders als Videoaufzeichnungen – maschinell zugeordnet und ausgewertet werden und weisen daher eine besonders hohe Sensitivität auf. Was wir im Internet lesen, suchen und schreiben, spiegelt unsere Persönlichkeit, unsere Vorlieben und Schwächen in einmaliger Deutlichkeit wider. Unsere Mediennutzung bedarf daher in besonderem Maße des Schutzes vor Erfassung.

144. Im wirklichen Leben ist eine derart lückenlose Aufzeichnung des Lese-, Such- und Schreibverhaltens der Bevölkerung, wie sie das Internet ermöglicht, unmöglich. Beim Abholen eines Formulars einer Behörde, beim Betreten eines Buchladens oder beim Betrachten eines Schaufensters bleibt man anonym. Es gibt keinen Grund, warum dies bei vergleichbaren Handlungen im Internet anders sein sollte. Niemand muss in einer öffentlichen Bibliothek registrieren lassen, welche Seite er in welchem Buch aufschlägt. Eine vergleichbar umfassende Kontrolle entsprechender Online-Aktivitäten (Nutzung des World Wide Web) ist ebenso wenig hinnehmbar.[133] Welche Seiten der Nutzer auf einem Internetportal betrachtet, geht den Betreiber ebensowenig an wie ein Nachrichtenmagazin wissen muss, welche Artikel einen Leser interessieren. Dass in Telekommunikationsnetzen Angriffe auf Computersysteme vorkommen, stellt keine Besonderheit dar. Auch auf der Straße oder in Wohnungen geschehen Straftaten,

133 Datenschutzbeauftragte des Bundes und der Länder: Entschließung zur systematischen verdachtslosen Datenspeicherung in der Telekommunikation und im Internet der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./25.10.2002, BT-Drs. 15/888, 199.

ohne dass dies eine Totalaufzeichnung des Verhaltens unzähliger Personen legitimieren würde.

145. Die Veröffentlichung der Sucheingaben von 600.000 Menschen durch das Internetunternehmen AOL im Jahr 2006 hat die Dringlichkeit eines verbesserten Datenschutzes im Internet erstmals in das öffentliche Bewusstsein gerückt. Den 20 Mio. Datensätzen ließen sich Namen, finanzielle Informationen, Krankheiten, Informationen über das Sexualleben, teilweise sogar ganze Lebensschicksale entnehmen.[134] Ein Missbrauch solcher Informationen durch Kriminelle liegt nahe (z.B. für Einbrüche, Erpressung, Identitätsdiebstahl, Kontakte Pädophiler zu Minderjährigen, Stalking). 57% der Internetnutzer sind „sehr besorgt" darüber, dass viele Internetunternehmen ihr Nutzerverhalten in personenbeziehbarer Form protokollieren.[135]

146. In der letzten Zeit mussten wir immer häufiger Fälle versehentlicher und absichtlicher Veröffentlichung und Zweckentfremdung von Informationen über unsere Internetnutzung erleben. Im Jahr 2008 wurden mehrere Fälle bekannt, in denen persönliche Daten von Internetnutzern offen gelegt und dem Risiko eines Missbrauchs ausgesetzt wurden. 18.000 Personen, die im Internet bei der Anzeigenblatt-Tochter WBV Wochenblatt des Axel Springer Verlages – zum Teil unter Chiffre – Anzeigen aufgegeben hatten, mussten ihre Privatanschrift, E-Mail-Adresse, Handynummer und Kontodaten im Internet wieder finden.[136] Das mit Diskretion werbende Erotikunternehmen Beate Uhse veröffentlichte die E-Mail-Adressen Tausender von Personen, die sich Sexfilme im Internet angesehen hatten.[137] In einem Forum des ZDF-Kinderkanals konnten sich beliebige Personen Klarnamen, Adresse, Telefonnummer und Geburtsdatum aller 1.000 registrierten Kinder verschaffen.[138]

147. Diese Vorfälle haben uns in Erinnerung gerufen, dass nur nicht gespeicherte Daten sichere Daten sind. Sie haben bestätigt, dass der europäische Ansatz eines Verbots der Aufzeichnung von Nutzungsdaten richtig ist. Die Beschränkung der Aufzeichnung von Nutzungsdaten minimiert den Schaden aus Datenlecks und gewährleistet unsere Sicherheit vor einer missbräuchlichen Aufdeckung und Auswertung unserer Internetnutzung.

148. Die Wertungen, die der – grundrechtswidrigen – Richtlinie 2006/24/EG zugrunde gelegen haben, lassen sich auf die Internetnutzung schon deshalb nicht übertragen, weil IP-Adressen und andere Internet-Nutzungsdaten nicht nur über die näheren Umstände von Individualkommunikation, sondern über den Inhalt der abgerufenen und eingegebenen Informationen (z.B. Internetseiten, Suchwörter) Aufschluss geben und damit weit reichende Rückschlüsse auf die Persönlichkeit des Nutzers zulassen, wie

134 Breyer, http://www.daten-speicherung.de/index.php/aol-skandal-erfordert-aenderungen-am-telemediengesetz-entwurf/.

135 Icomp, Consumer Understanding, http://snipurl.com/7sfrm.

136 Spiegel 43/2008 vom 20.10.2008, Seite 70.

137 Die Welt vom 04.09.2008: Beate Uhse verschlampt E-Mail-Adressen im Web.

138 Spiegel Online vom 16.10.2008: Kika stellt Daten von Kindern ungeschützt ins Web.

sie bei sonstigen Medien undenkbar wären. Die von dem Betreiber eines Internetportals gespeicherte IP-Adresse gibt Aufschluss über den Inhalt der Kommunikation. Sie erlaubt den Rückschluss, dass sich der Internetnutzer für die Informationen des jeweiligen Internetportals interessiert hat. Meist werden auch die Adressen (URLs) der abgerufenen Seiten protokolliert, so dass sich ein noch genaueres Personenprofil erstellen lässt. Dementsprechend nimmt Art. 5 (2) RiL 2006/24/EG Daten, die Aufschluss über den Inhalt einer Kommunikation geben, ausdrücklich von der Vorratsdatenspeicherung aus.

149. Es lässt sich zwar nie ganz ausschließen, dass eine IP-Adresse im Rahmen der Aufklärung eines Computerangriffs irgendwann einmal die Rolle eines Beweismittels spielen könnte. Dasselbe gilt aber für alle anderen Nutzungsdaten einschließlich der abgerufenen und eingegebenen Inhalte und im Übrigen auch für jegliches sonstige personenbezogene Datum über einen Nutzer. Aus jedem auf seine Person bezogenen Datum können sich im Einzelfall einmal Schlüsse bezüglich eines Angriffs auf Computersysteme ergeben. Das gesamte Datenschutzrecht beruht indes auf dem Gedanken, dass nicht bereits die bloße Möglichkeit, dass ein Datum irgendwann in der Zukunft einmal gebraucht werden könnte, dessen Speicherung rechtfertigt, weil ansonsten sämtliche personenbezogenen Daten zeitlich unbegrenzt auf Vorrat gespeichert werden dürften. Dies aber wäre eine unverhältnismäßige und unangemessene Beeinträchtigung des Persönlichkeitsrechts des Betroffenen, dem aus der Aufzeichnung seiner sensiblen Internetnutzung schwere Nachteile entstehen können.

150. Wegen der bloßen entfernten Möglichkeit einer Nützlichkeit der streitgegenständlichen Daten ist deren Aufbewahrung nicht verhältnismäßig. Nur zu einem verschwindend geringen Teil (vermutlich nicht einmal ein Datensatz von 1.000.000) kann die Speicherung von Nutzungdaten überhaupt zur Aufklärung von „Angriffen auf die Internetinfrastruktur“ der Betreiber von Internetportalen nützlich sein. Selbst wenn der Betreiber ohne protokollierte IP-Adressen in ein oder zwei Fällen pro Jahr nicht in der Lage sein sollte, einen Angreifer zu identifizieren, dann ist ihm das zumutbar, weil er technische Abhilfemaßnahmen zur Beendigung des Angriffs treffen kann, die eine Identifizierung des Angreifers nicht erfordern.

151. Das Interesse des Betreibers an einer straf- oder zivilrechtlichen Verfolgung einzelner Angriffe muss daher hinter das Recht auf informationelle Selbstbestimmung der unzähligen rechtmäßig handelnden Nutzer zurücktreten.

152. Dass das Verbot der Protokollierung von IP-Adressen den Betreibern zumutbar ist, ergibt sich im Übrigen aus der deutschen Rechtslage, die genau dies seit Jahren vorsieht. Nach § 15 (1) des deutschen Telemediengesetzes dürfen IP-Adressen und andere Nutzungsdaten nur verarbeitet werden, „soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen“. Nach § 13 (4) des deutschen Telemediengesetzes müssen „die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Be-

endigung gelöscht“ werden. Diese seit Jahren bestehende Rechtslage hat sich bewährt und die Internetnutzer in unzähligen Fällen zuverlässig vor Datenpannen, Überwachung und Missbrauch geschützt. Der Deutsche Bundestag strich zuletzt am 18.06.2009 einen massiver Kritik ausgesetzten Änderungsvorschlag der Bundesregierung, der Anbietern von Internetportalen eine Protokollierung des Internet-Nutzungsverhaltens „zum Erkennen, Eingrenzen oder Beseitigen von Störungen seiner für Zwecke seines Dienstes genutzten technischen Einrichtungen“ gestatten sollte.[139]

153. Nach der Rechtsprechung des Bundesverfassungsgerichts darf eine automatisierte Datenerfassung „nicht anlasslos erfolgen oder flächendeckend durchgeführt werden“.[140] Im Rahmen der „technischen Möglichkeit und Praktikabilität“ hat eine „sofortige Datenlöschung“ zu erfolgen.[141] Gleiches ergibt sich aus dem Urteil des EGMR zur Vorratsspeicherung biometrischer Daten und aus den obigen Ausführungen zur Vorratsspeicherung von Telekommunikationsdaten. Ebenso wie die Vorratsspeicherung von Telekommunikationsdaten die Art. 8 und 10 EMRK verletzt, ist dies erst Recht im Fall der Vorratsspeicherung von Internet-Nutzungsdaten der Fall.

154. Jede Ermächtigung zur personenbezogenen Erfassung von Nutzungsdaten würde die Gefahr begründen, dass hochsensible Informationen über unsere Internetnutzung versehentlich abhanden kommen, veröffentlicht werden oder absichtlich zweckentfremdet werden. Da die Vorratsspeicherung von IP-Adressen und anderer Nutzungsdaten eine potenziell unbegrenzte Menge äußerst sensibler Daten über unsere Internetnutzung Offenlegungs- und Missbrauchsrisiken aussetzen würde, muss sie für rechtswidrig erklärt werden. Das Verbot der Vorratsdatenspeicherung, welches Art. 6 RiL 2002/58/EG für TK-Anbieter bereits kodifiziert hatte, stellt erwiesenermaßen die beste Garantie für unsere Sicherheit in der Informationsgesellschaft dar.

3. Ergebnis

155. Die Vorlagefrage zu 6 sollte somit wie folgt beantwortet werden: „Art. 7 der Richtlinie 95/46/EG ist dahin auszulegen, dass er einer Praxis, die IP-Adressen der Benutzer einer Homepage ohne deren ausdrücklicher Einwilligung zu speichern, entgegensteht.“

[...]

---

139 Regierungsentwurf eines „Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes“ vom 14.01.2009 (BT-Drs. 16/11967), geändert durch Beschluss des Bundestages vom 18.06.2009 (BT-Drs. 16/13259).

140 BVerfG, MMR 2008, 308, 308; BVerfG, NVwZ 2007, 688, 691.

141 BVerfG, Beschluss vom 27.10.2006, Az. 1 BvR 1811/99.