An das
Bundespräsidialamt
11010 Berlin

4. Dezember 2007

Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG

Sehr geehrter Herr Bundespräsident,

zurzeit liegt Ihnen das am 9. November 2007 vom Bundestag beschlossene Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG zur Prüfung und gegebenenfalls Unterzeichnung vor.

In der Vergangenheit haben Sie gezeigt, dass Sie – gerade in Zeiten einer großen Koalition – Ihren verfassungsrechtlichen Prüfauftrag ernst nehmen und offensichtlich verfassungswidrige Gesetze nicht unterzeichnen. Dementsprechend appellieren wir an Sie, das oben genannte Gesetz nicht zu unterzeichnen, weil die darin vorgesehene Vorratsdatenspeicherung offensichtlich verfassungswidrig ist.

I. Inhalt und Auswirkungen

Das Gesetz zur Neuregelung der Telekommunikationsüberwachung sieht vor, Telekommunikationsunternehmen ab 2008 zu verpflichten, Daten über die Kommunikation ihrer Kunden auf Vorrat zu speichern (§§ 113a, 113b TKG-E). Zur verbesserten Strafverfolgung soll nachvollziehbar werden, wer mit wem in den letzten sechs Monaten per Telefon, Handy oder E-Mail in Verbindung gestanden hat. Bei Handy-Telefonaten und SMS würde auch der jeweilige Standort des Benutzers festgehalten. Zudem soll die Internetnutzung nachvollziehbar werden.

Darin läge eine weitreichende Registrierung des Verhaltens der Menschen in Deutschland. Ohne jeden Verdacht einer Straftat würden sensible Informationen über die sozialen Beziehungen (einschließlich Geschäftsbeziehungen), die Bewegungen und die individuelle Lebenssituation (z.B. Kontakte mit Ärzten, Rechtsanwälten, Psychologen, Beratungsstellen) von über 80 Millionen Bundesbürgerinnen und Bundesbürgern gesammelt. Damit höhlt eine Vorratsdatenspeicherung Anwalts-, Arzt-, Seelsorge-, Beratungs- und andere Berufsgeheimnisse aus und begünstigt Wirtschaftsspionage. Sie untergräbt den Schutz journalistischer Quellen und beschädigt damit die Pressefreiheit im Kern. Überdies steht zu erwarten, dass die enormen Kosten einer Vorratsdatenspeicherung Telekommunikationsunternehmen und Verbraucher belasten, indem sie Preiserhöhungen sowie die Einstellung von Angeboten nach sich ziehen.

Derzeit dürfen Telekommunikationsanbieter nur die zur Abrechnung erforderlichen Verbindungsdaten speichern. Dazu gehören Handy-Standorte, Internetkennungen und Email-Verbindungsdaten nicht. Auch Daten über eingehende Verbindungen – etwa aus dem Ausland – dürfen bisher nicht gespeichert werden, weswegen die Suche nach den Gesprächspartnern einer Person („Zielwahlsu-

che“) etwa bei der Deutschen Telekom gegenwärtig nur für die letzten drei Tage möglich ist.[1] Der Kunde kann verlangen, dass Abrechnungsdaten mit Rechnungsversand gelöscht werden.[2] Durch die Benutzung von Pauschaltarifen kann eine Speicherung zudem bisher gänzlich vermieden werden, was etwa für Journalisten und Beratungsstellen wichtig sein kann. All diese Mechanismen zum Schutz sensibler Kontakte und Aktivitäten würde eine Vorratsdatenspeicherung beseitigen.

Bei Inkrafttreten des Gesetzes droht Journalisten der Verlust von Informanten und damit von Informationen, mit deren Hilfe Missstände in Staat und Gesellschaft aufgedeckt werden können. Der Journalist Detlef Drewes hat nach Inkrafttreten der Vorratsdatenspeicherung in Belgien erlebt, dass Informanten den Kontakt mit ihm abbrachen.[3] Ferner droht die Vorratsdatenspeicherung von der Inanspruchnahme telefonischer Beratungsangebote (z.B. Telefonseelsorge, Eheberatung, Suchtberatung, AIDS-Beratung) abzuschrecken. Wenn Menschen, die ohnehin in einer Notlage sind, aus Furcht vor dem Bekanntwerden ihrer Situation keine Hilfe suchen, kann dies schwerste Folgen haben, bis hin zu Suiziden. Den Strafverfolgungsbehörden drohen wichtige Informationen über Straftaten zu entgehen, weil Voraussetzung einer Übermittlung solcher Insider-Informationen oft die absolute Anonymität des Informants ist. Auch andere Aufsichtsbehörden und Stellen würden Informationen von Whistleblowern einbüßen, wenn jedes Telefonat, Telefax und jede E-Mail monatelang nachvollzogen werden kann. Es droht eine Beeinträchtigung der Arbeit regierungs- und staatskritischer Personen und Gruppierungen (z.B. Globalisierungsgegner), wenn sie Ermittlungen aufgrund ihrer elektronischen Kontakte befürchten müssen. Dies kann etwa die Vorbereitung von Demonstrationen beeinträchtigen, die ein wichtiges Mittel zur Mitwirkung an der politischen Willensbildung sind. Ferner droht eine schwere Beeinträchtigung der Internetnutzung, wenn man Nachteile durch den Aufruf „potenziell verdächtiger“ Seiten oder die Verwendung „potenziell verdächtiger“ Suchwörter befürchten muss. Schon heute ermittelt das Bundeskriminalamt gegen Personen, die „auffällig oft“ auf Internetseiten über die „militante gruppe“ zugreifen,[4] obwohl dies aus vielerlei Gründen, etwa journalistischer Art, legitim sein kann. Dieses Jahr ist eine – ergebnislose – Wohnungsdurchsuchung bei Globalisierungskritikern damit begründet worden, der Betroffene habe eine „umfassende Internetrecherche“ zu einer Firma vorgenommen, die später Ziel eines Brandanschlags wurde.[5] Gegenwärtig ist das Internet-Nutzungsverhalten nur wenige Tage lang nachvollziehbar, weil Internet-Zugangsanbieter die Zuordnung von IP-Adressen nicht speichern dürfen.[6] Bei Inkrafttreten des Gesetzes könnten die in Internet-Nutzungsprotokollen („Logfiles“) enthaltenen IP-Adressen über § 113 TKG ohne richterliche Anordnung sechs Monate lang der Person des Anschlussinhabers zugeordnet werden. Insgesamt droht bei Inkrafttreten des Gesetzes, dass sensible Kontakte und Kommunikationen entweder erschwert werden oder insgesamt enden. Damit wird die freie Kommunikation in Deutschland gravierend beeinträchtigt, was unserer freiheitlichen Gesellschaft insgesamt erheblichen Schaden zufügt.

47 Verbände und Organisationen aus allen Bereichen der Gesellschaft haben sich in einer gemeinsamen Erklärung gegen die Vorratsdatenspeicherung ausgesprochen,[7] darunter Bürgerrechts-, Da-

---

1 Dr. Bernd Köbele, Deutsche Telekom: Wirtschaftsunternehmen – verlängerter Arm der Sicherheitsbehörden? https://www.datenschutzzentrum.de/sommerakademie/2007/video/sak2007-vortrag-schrief-koebele.htm

2 Vgl. BVerfG, 1 BvR 1811/99 vom 27.10.2006, http://www.bverfg.de/entscheidungen/rk20061027_1bvr181199.html für Prepaid-Mobiltelefonkarten.

3 Märkische Allgemeine vom 11.10.2007, http://www.maerkischeallgemeine.de/cms/beitrag/11038603/492531/.

4 Bundesregierung, BT-Drs. 16/6938.

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

6 § 96 TKG, vgl. LG Darmstadt, Urteil vom 07.12.2005, Az. 25 S 118/2005, http://www.law.olnhausen.com/olg/lgda-verbindungsdaten.html.

7 http://erklaerung.vorratsdatenspeicherung.de.

tenschutz- und Menschenrechtsverbände, Journalistenorganisationen und Medienverbände, Internetwirtschaft und Telefonseelsorge, Anwalts- und Juristenverbände und die Verbraucherzentrale. Auf mehreren Demonstrationen haben tausende von Menschen gegen eine Vorratsspeicherung ihres Telekommunikationsverhaltens protestiert, etwa 15.000 Menschen am 22. September in Berlin.[8] Eine fünfstellige Zahl von Menschen hat bereits einen Rechtsanwalt bevollmächtigt, Verfassungsbeschwerde gegen das Gesetz zu erheben, falls es in Kraft treten sollte.[9]

II. Offensichtliche Unvereinbarkeit mit den Grundrechten

Der Einführung von Speicherungspflichten für Verkehrsdaten in Deutschland stehen die Grundrechte der betroffenen Bürger und die dazu ergangene verfassungsgerichtliche Rechtsprechung entgegen.

Dies gilt zum einen für das vom Bundesverfassungsgericht ausgesprochene „außerhalb statistischer Zwecke bestehende strikte Verbot der Sammlung personenbezogener Daten auf Vorrat".[10] Entgegen der Ansicht der Verfasser des Regierungsentwurfs[11] (S. 66) gilt dieses Verbot nicht nur für eine Vorratsdatenspeicherung „zu unbestimmten oder noch nicht bestimmbaren Zwecken". Diese Einschränkung hat das Bundesverfassungsgericht in seinem Rasterfahndungsbeschluss aufgegeben und nicht mehr genannt.[12] Stattdessen hat das Gericht präzisiert, dass eine Vorratsdatenspeicherung nur zu statistischen Zwecken zulässig ist.

Unabhängig davon sieht der Regierungsentwurf durchaus eine Datensammlung „zu unbestimmten oder noch nicht bestimmbaren Zwecken" im Sinne der Rechtsprechung des Bundesverfassungsgerichts vor. Eine allgemeine Aufgabenbeschreibung wie die des § 113b TKG-E („zur Verfolgung von Straftaten", „zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit", „zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes") stellt keine hinreichende Zweckbestimmung in diesem Sinne dar.[13] Dies ergibt sich schon daraus, dass das Bundesverfassungsgericht die Datenspeicherung zu statistischen Zwecken gesondert zulässt, also auch die Zweckbestimmung „zu statistischen Zwecken" nicht hinreichend präzise wäre. Würde man schon eine allgemeine Aufgabenbeschreibung zur Rechtfertigung einer Sammlung personenbezogener Daten auf Vorrat genügen lassen, so wäre das vom Bundesverfassungsgericht ausgesprochene Verbot gegenstandslos. Eine allgemeine Beschreibung der denkbaren Verwendungszwecke ist stets möglich. So kann die Rechtsprechung des Bundesverfassungsgerichts nicht gemeint sein.

---

8 http://www.vorratsdatenspeicherung.de/content/view/13/37/.

9 http://verfassungsbeschwerde.vorratsdatenspeicherung.de

10 BVerfG, 1 BvR 518/02 vom 04.04.2006, NJW 2006, 1939 (1943), Abs. 105.

11 BT-Drs. 16/5846.

12 Die frühere Rechtsprechung wird nur unter „vergleiche" zitiert: „*Dadurch entsteht ein Risiko, dass das außerhalb statistischer Zwecke bestehende strikte Verbot der Sammlung personenbezogener Daten auf Vorrat (vgl. BVerfGE 65, 1 <47>) umgangen wird.*"

13 Ebenso Deutscher Anwaltverein, Stellungnahme vom August 2007, http://www.anwaltverein.de/03/-05/2007/41-07.pdf, 39.

In der Entscheidung des Bundesverfassungsgerichts vom 04.04.2006 heißt es weiter:

> „*Selbst bei höchstem Gewicht der drohenden Rechtsgutbeeinträchtigung kann auf das Erfordernis einer hinreichenden Wahrscheinlichkeit nicht verzichtet werden.*“[14] „*Der Grundsatz der Verhältnismäßigkeit führt dazu, dass der Gesetzgeber intensive Grundrechtseingriffe erst von bestimmten Verdachts- oder Gefahrenstufen an vorsehen darf [...] Verzichtet der Gesetzgeber auf begrenzende Anforderungen an die Wahrscheinlichkeit des Gefahreneintritts sowie an die Nähe der Betroffenen zur abzuwehrenden Bedrohung und sieht er gleichwohl eine Befugnis zu Eingriffen von erheblichem Gewicht vor, genügt dies dem Verfassungsrecht nicht.*“[15]

Eine Vorratsdatenspeicherung verzichtet auf jeden Verdachtsgrad und auf jede Nähe der Betroffenen zu den aufzuklärenden Straftaten, stellt gleichzeitig aber einen schwerwiegenden Grundrechtseingriff dar, weil sensible Daten über das Kommunikationsverhalten der gesamten Bevölkerung gesammelt werden. Dies ist mit dem Verfassungsrecht offensichtlich unvereinbar.

Mit keinem Wort würdigt die Begründung des Regierungsentwurfs ferner das Urteil des Bundesverfassungsgerichts vom 12.03.2003, in dem es wörtlich heißt:

> „*Insofern genügt es verfassungsrechtlichen Anforderungen nicht, dass die Erfassung der Verbindungsdaten allgemein der Strafverfolgung dient. Vorausgesetzt sind vielmehr eine Straftat von erheblicher Bedeutung, ein konkreter Tatverdacht und eine hinreichend sichere Tatsachenbasis*“.[16]

Mit diesen Vorgaben steht die beabsichtigte Vorratsdatenspeicherung im evidenten Widerspruch. Insbesondere kann die Maßnahme nicht damit gerechtfertigt werden, dass die Datenspeicherung bei privaten Unternehmen erfolgen soll und nicht bei staatlichen Stellen. Nicht erst die Kenntnisnahme und Verwertung von Kommunikationsdaten ist ein Grundrechtseingriff, sondern schon die Aufzeichnung der Daten.[17] Mit § 113a TKG-E ordnet der Staat die Aufzeichnung und Speicherung von Daten an, auf die er sich gleichzeitig Zugriffsrechte einräumt (vgl. nur § 100g StPO). Dieses bloße „Outsourcing“ der Datenvorhaltung an Private ist für die verfassungsrechtliche Beurteilung unerheblich. Entscheidend ist, dass die staatliche Speicherpflicht die spätere Kenntnisnahme der Daten durch staatliche Stellen ermöglicht.[18] Dementsprechend stellt das Bundesverfassungsgericht allgemein auf die „Erfassung“ von Verbindungsdaten ab, wenn es ausführt: „*Insofern genügt es verfassungsrechtlichen Anforderungen nicht, dass die **Erfassung** der Verbindungsdaten allgemein der Strafverfolgung dient.*“[19]

Mit § 113a TKG-E ordnet der Staat eine Erfassung und Vorhaltung von Verbindungsdaten an, die nur allgemein der Strafverfolgung dienen soll (§ 113b Abs. 1 TKG-E), aber keinen konkreten Tatverdacht und keinerlei Anhaltspunkte einer Straftat voraussetzt. Dies genügt den verfassungsrechtlichen Anforderungen offensichtlich nicht.

Vor dem Hintergrund der klaren verfassungsgerichtlichen Rechtsprechung war es ein vorsätzlicher Verfassungsbruch, eine Vorratsspeicherung von Telekommunikations-Verkehrsdaten gleichwohl zu beschließen.

III. Keine Bindung durch Europarecht

Die Grundrechtsverletzung ist nicht durch die EG-Richtlinie 2006/24/EG zur Vorratsdatenspeicherung vorgegeben.

---

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

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

16 BVerfG, 1 BvR 330/96 vom 12.03.2003, NJW 2003, 1787 (1791), Abs. 75.

17 BVerfGE 100, 313 (366), Abs. 185.

18 BVerfGE 107, 299 (314).

19 BVerfG, 1 BvR 330/96 vom 12.03.2003, NJW 2003, 1787 (1791), Abs. 75.

1. Überschießende und richtlinienwidrige Umsetzung in Deutschland

Eine Umsetzungspflicht besteht jedenfalls insoweit nicht als das beschlossene Gesetz weit über die in der Richtlinie vorgesehenen Regelungen hinaus geht, teilweise sogar unter Verstoß gegen die Richtlinie selbst:

a) Richtlinienwidrige Verwendung von Verbindungsdaten

In Deutschland sollen Zugriffe auf vorratsgespeicherte Verbindungsdaten bei jedem Verdacht einer „erheblichen" oder einer „mittels Telekommunikation begangenen" Straftat zulässig sein (§ 100g StPO-E), außerdem „zur Abwehr von erheblichen Gefahren" und zur Sammlung von Erkenntnissen durch die Nachrichtendienste (§ 113b TKG-E). Die EU-Richtlinie sieht eine Datenspeicherung nur „zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten" vor (Art. 1 RiL 2006/24/EG). Diese enge Zweckbestimmung ist auch für die Verwendung der gespeicherten Daten verbindlich und darf von den Mitgliedsstaaten nicht überschritten werden.[20]

b) Überschießendes Verbot von Anonymisierungsdiensten

§ 113a Abs. 6 TKG-E soll Internet-Anonymisierungsdienste zur Vorratsdatenspeicherung verpflichten, was sie praktisch wirkungslos machen würde und die weitgehende Einstellung solcher Dienste in Deutschland zur Folge hätte. Die EU-Richtlinie gilt für Anonymisierungsdienste nicht.

c) Überschießende Identifizierungspflicht

Nach § 111 TKG-E erhält eine Telefonnummer oder sonstige Anschlusskennung nur, wer seinen Namen, seine Anschrift und sein Geburtsdatum angibt (Identifizierungszwang). Diese Daten sind für eine Vielzahl staatlicher Behörden abrufbar (§§ 112, 113 TKG). Selbst Anbieter vorausbezahlter und kostenloser Dienste (z.B. Prepaid-Handykarten) müssen diese Daten erheben. Die EU-Richtlinie sieht keine Identifizierungs- bzw. Datenerhebungspflicht vor. Sie schreibt lediglich vor, dass Daten zur Identifizierung von Kommunikationsteilnehmern, die ohnehin im Zuge der Bereitstellung von Telekommunikationsdiensten anfallen, auf Vorrat zu speichern sind.

d) Richtlinienwidrige Verwendung von Bestandsdaten

Die §§ 112, 113 TKG eröffnen allen Behörden Zugriff auf die Identität von Telefon-, Handy-, E-Mail- und Internetnutzern (Name, Anschrift, Geburtsdatum), die irgend ein Interesse daran haben können (z.B. Polizei, Staatsanwaltschaft, Geheimdienste, Zoll, Behörden zur Bekämpfung von Schwarzarbeit). Schon die Verfolgung von Ordnungswidrigkeiten (z.B. Falschparken) soll Zugriffe im automatisierten Abrufverfahren des § 112 TKG rechtfertigen. Die EU-Richtlinie sieht eine Datenspeicherung dagegen nur „zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten" vor (Art. 1 RiL 2006/24/EG). Dies gilt ausdrücklich auch für Bestandsdaten.

e) Überschießende Speicherdauer von Bestandsdaten

Nach den §§ 95, 111 TKG sind die Daten über die Identität von Telefon-, Handy-, E-Mail- und Internetnutzern (Name, Anschrift, Geburtsdatum) nach Vertragsende bis zu zwei Jahre lang auf Vorrat zu speichern. Die EU-Richtlinie fordert dagegen nur eine sechsmonatige Speicherung.

f) Überschießender Umfang der Speicherung von E-Mail-Verbindungsdaten

In Deutschland soll bei jedem Versenden und Abrufen von E-Mail die Kennung (IP-Adresse) des Nutzers gespeichert werden, bei jedem Empfangen von E-Mail die Kennung des Absenders (§ 113a Abs. 3 TKG-E). In der EU-Richtlinie ist davon keine Rede.

g) Fehlende Entschädigung

---

20 Generalanwältin am EuGH, Schlussanträge vom 18. Juli 2007 in der Rechtssache C-275/06, Rn. 124: „Wenn man der Richtlinie 2006/24 überhaupt etwas für den vorliegenden Fall entnehmen kann, so ist dies die Wertentscheidung des Gemeinschaftsgesetzgebers, dass bislang nur schwere Kriminalität eine gemeinschaftsweite Vorratsspeicherung von Verkehrsdaten **und ihre Verwendung** erfordert"; ebenso Gitter/Schnabel, MMR 2007, 411 (415).

Nach dem Regierungsentwurf sollen Anbieter von Telefon-, Handy-, E-Mail- und Internetdiensten keine Entschädigung für die Vorratsspeicherung und die dafür anfallenden Kosten erhalten. Die Kosten müssen deswegen im Wege von Preiserhöhungen auf die Nutzer umgelegt werden. Bisher kostenlosen Diensten droht die Einstellung. Die EU-Richtlinie steht einer Entschädigung demgegenüber nicht entgegen.

h) Verfrühte Umsetzung

In Deutschland sollen die Speicherpflichten für E-Mail- und Internetzugangsanbieter bereits ab dem 1. Januar 2009 gelten. Die EU-Richtlinie fordert eine Speicherung dagegen erst ab dem 15. März 2009.

2. Keine Umsetzungspflicht Deutschlands

Deutschland ist zur Umsetzung der Richtlinie 2006/24/EG ohnehin nicht verpflichtet.

Der Regierungsentwurf vertritt unter Hinweis auf Art. 242 EG die Auffassung (S. 61), bis zur Entscheidung des Europäischen Gerichtshofs über Irlands Nichtigkeitsklage[21] bleibe die Umsetzungspflicht Deutschlands bestehen. Tatsächlich ist Art. 242 EG lediglich zu entnehmen, dass eine Nichtigkeitsklage die Pflicht zur Umsetzung einer wirksamen Richtlinie unberührt lässt. Demgegenüber sagt Art. 242 EG nichts darüber aus, ob der angegriffene Rechtsakt überhaupt Rechtswirkungen entfaltet.

Nach der Rechtsprechung des Europäischen Gerichtshofs spricht für die Rechtsakte der Gemeinschaftsorgane zwar eine Vermutung der Rechtmäßigkeit.[22] Diese Vermutung gilt dem Gerichtshof zufolge aber nicht für Rechtsakte, die mit einem Fehler behaftet sind, dessen Schwere so offensichtlich ist, dass er von der Gemeinschaftsrechtsordnung nicht geduldet werden kann.[23] In einem solchen Fall ist der Rechtsakt von vornherein „inexistent“ und erzeugt keine Befolgungs- oder Umsetzungspflicht.

Die Richtlinie 2006/24/EG erfüllt diese Voraussetzungen und löst daher keine Umsetzungspflicht aus:

a) Formelle Rechtswidrigkeit

Die Richtlinie ist in formeller Hinsicht rechtswidrig, weil die Europäische Gemeinschaft über keine Kompetenz zum Erlass der in der Richtlinie enthaltenen Regelungen verfügte.[24]

Kommission, Europaparlament und Rat stützten die Richtlinie 2006/24/EG auf Art. 95 EG als Rechtsgrundlage. Sie begründen dies mit Rechtsgutachten, die im Auftrag der Kommission[25] und des Rates[26] erstellt wurden. Diesen Gutachten zufolge sei die Speicherung von Kommunikationsdaten in der Richtlinie 2002/58/EG bereits umfassend gemeinschaftsrechtlich geregelt. Die Einführung von Mindestspeicherfristen für solche Daten falle deswegen als Annex ebenfalls in die Kompetenz der Europäischen Gemeinschaft nach Art. 95 EG. Außerdem beeinträchtigten unterschiedliche nationale Vorschriften zur Vorratsdatenspeicherung den Binnenmarkt.

Einige Mitgliedsstaaten wie Irland und die Slowakei sowie der Deutsche Bundestag vertreten demgegenüber die Auffassung, dass die dritte Säule der EU die richtige Rechtsgrundlage gewesen wä-

---

21 Az. C-301/06

22 EuGHE 1979, 623; EuGH, C-475/01 vom 05.10.2004, Abs.-Nr. 18.

23 EuGHE 1988, 3611; EuGHE I 1992, 5437; EuGH, C-475/01 vom 05.10.2004, Abs.-Nr. 19; st. Rspr.

24 Ebenso: Simitis, NJW 2006, 2011 (2013); Westphal, EuZW 2006, 555 (557); Gitter/Schnabel, MMR 2007, 411 (413); Deutscher Anwaltverein, Stellungnahme vom August 2007, http://www.anwaltverein.de/03/05/2007/41-07.pdf, 35 f.

25 Juristische Analyse vom 22.03.2005, SEC(2005)420, http://www.statewatch.org/news/2005/apr/Commission-legal-opinion-data-retention.pdf.

26 Rechtsgutachten des Juristischen Dienstes des Rates vom 05.04.2005, http://www.statewatch.org/news/2005/apr/Council-legal-opinion-data-retention.pdf.

re, weil Ziel der Datenspeicherung die Erleichterung der Strafverfolgung ist.[27] Im Juli 2006 reichte Irland beim Europäischen Gerichtshof eine Nichtigkeitsklage gegen die Richtlinie zur Vorratsdatenspeicherung ein (Az. C-301/06). Stützen kann es sich dabei auf die zwischenzeitlich ergangene Entscheidung des Europäischen Gerichtshofs zur Fluggastdatenübermittlung in die USA.[28] Auch in jenem Fall hatte die Kommission die Datenübermittlung auf der Grundlage der Binnenmarktkompetenz (Art. 95 EG) autorisiert. Sie argumentierte, Fluggastdaten würden von den Fluggesellschaften zur Erbringung einer Dienstleistung erhoben und fielen deshalb in den Anwendungsbereich des Gemeinschaftsrechts. Zum Funktionieren des Binnenmarkts sei eine harmonisierte Regelung der Fluggastdatenübermittlung erforderlich, weil international agierende Unternehmen ansonsten in jedem Mitgliedsstaat unterschiedlichen Regelungen nachkommen müssten.

Der Europäische Gerichtshof verwarf diese Argumentation und erklärte die Rechtsakte mangels Kompetenz der Europäischen Gemeinschaft für nichtig. Die Binnenmarktkompetenz des Art. 95 EG sei nicht einschlägig. Die Fluggastdatenübermittlung sei

> *„eine Datenverarbeitung, die nicht für die Erbringung einer Dienstleistung erforderlich ist, sondern zum Schutz der öffentlichen Sicherheit und zu Strafverfolgungszwecken als erforderlich angesehen wird."*[29]

Auch die Vorratsspeicherung von Telekommunikationsdaten ist nicht für die Erbringung einer Dienstleistung der Telekommunikationsunternehmen erforderlich, sondern wird lediglich zu Strafverfolgungszwecken als erforderlich angesehen (vgl. Art. 1 RiL 2006/24/EG). Damit kommt Art. 95 EG als Rechtsgrundlage auch für die Vorratsdatenspeicherung nicht in Frage, so dass die Richtlinie zur Vorratsdatenspeicherung mangels Rechtsgrundlage rechtswidrig ist.[30] Ausgehend von der eindeutigen Rechtsprechung des Europäischen Gerichtshofs kann hieran kein Zweifel bestehen.

Der Generalanwalt beim Europäischen Gerichtshof hatte bereits in seinen Schlussanträgen zur Fluggastdatenübermittlung die fehlende Kompetenz der Europäischen Gemeinschaft abstrahiert auf alle Fälle, in denen „eine juristische Person zu einer solchen Datenverarbeitung und zur Übermittlung dieser Daten verpflichtet" wird.[31] Er hat sogar ausdrücklich auf die Vorratsdatenspeicherung Bezug genommen.[32] Dies verdeutlicht, dass die Entscheidung des Europäischen Gerichtshofs direkt auf die Richtlinie zur Vorratsdatenspeicherung übertragbar ist und es auch dieser Richtlinie an einer Rechtsgrundlage mangelt.

b) Materielle Rechtswidrigkeit

Die Richtlinie 2006/24/EG ist auch materiell rechtswidrig, weil sie gegen mehrere Gemeinschaftsgrundrechte verstößt.[33]

---

27 So auch der Deutsche Bundestag, BT-Drs. 16/545, 3: „Dass sich die nun geplante Maßnahme auf Artikel 95 EGV, d. h. auf die 'Erste Säule' stützt, begegnet Bedenken, weil Artikel 95 EGV an sich der Sicherstellung des Funktionierens des Binnenmarktes dient, während die Richtlinie primär Strafverfolgungsinteressen verfolgt."

28 EuGH, Urteil vom 30.05.2006, Az. C-317/04 und C-318/04, NJW 2006, 2029.

29 EuGH, Urteil vom 30.05.2006, Az. C-317/04 und C-318/04, NJW 2006, 2029, Abs. 57.

30 Ebenso: Simitis, NJW 2006, 2011 (2013); Westphal, EuZW 2006, 555 (557); Gitter/Schnabel, MMR 2007, 411 (413); Deutscher Anwaltverein, Stellungnahme vom August 2007, http://www.anwaltverein.de/03/05/2007/41-07.pdf, 35 f.

31 Abs-Nr. 160 der Schlussanträge vom 22.11.2005.

32 Abs-Nr. 160 der Schlussanträge vom 22.11.2005.

33 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,

Einen Teil des primären Gemeinschaftsrechts stellen die Gemeinschaftsgrundrechte dar, die der Europäische Gerichtshof als „allgemeine Grundsätze des Gemeinschaftsrechts“[34] aus den Rechtstraditionen der Mitgliedstaaten entwickelt hat. Der Europäische Gerichtshof wendet dabei in der Regel die Europäische Menschenrechtskonvention (EMRK) in ihrer Auslegung durch den Europäischen Gerichtshof für Menschenrechte an.[35] Entsprechend Art. 8 EMRK hat der Europäische Gerichtshof beispielsweise den Schutz der Privatsphäre als Gemeinschaftsgrundrecht anerkannt.[36]

Die Richtlinie 2006/24/EG verstößt gegen das Recht auf Achtung des Privatlebens und der Korrespondenz (Artikel 8 EMRK) sowie gegen die Freiheit der Meinungsäußerung (Artikel 10 EMRK). Diese Rechte dürfen nach der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte nur eingeschränkt werden, wenn die Belastungsintensität nicht außer Verhältnis zu dem Gewicht des Zwecks steht.[37] Das Interesse des Staates muss gegenüber den Interessen des Einzelnen an der Achtung seiner Privatsphäre abgewogen werden.[38] Eingriffe sind zwar nicht auf das unerlässliche Maß beschränkt, aber ein bloßes Nützlich- oder Wünschenswertsein genügt nicht.[39]

Die Abwägung ergibt, dass eine Speicherung des Kommunikationsverhaltens der gesamten Bevölkerung grob unverhältnismäßig ist.[40] Die staatlichen Behörden würden nur einen kleinen Bruchteil (etwa 0,0004%[41]) der anfallenden Kommunikationsdaten jemals nachfragen, während mehr als 99% der Betroffenen[42] vollkommen unschuldig, unverdächtig und ungefährlich sind.

c) Schwere und Offensichtlichkeit der Fehler

Die beschriebenen Rechtsverletzungen stellen besonders schwere Fehler dar.

Wenn die Europäische Gemeinschaft einen Rechtsakt auf einem Gebiet erlässt, für das sie überhaupt nicht zuständig ist, wenn sie also außerhalb ihrer begrenzten Einzelermächtigungen handelt, so liegt ein besonders schwerer Verstoß gegen die Gründungsverträge als Grundlage der Europäischen Gemeinschaft vor. Zumal durch den Beschluss der Richtlinie das im Rahmen der Dritten Säule geltende Einstimmigkeitsprinzip umgangen wurde.

Wenn ein Rechtsakt der Europäischen Gemeinschaft mehrere Gemeinschaftsgrundrechte verletzt, weil er grob unverhältnismäßig ist, so liegt ebenfalls ein besonders schwerer Verstoß gegen primäres Gemeinschaftsrecht vor. Die Vorratsdatenspeicherung verkehrt das Regelungssystem der Grundrechte in ihr Gegenteil. Den Grundrechten zufolge ist das geschützte Verhalten grundsätzlich frei, und Einschränkungen sind nur dann und nur insoweit zulässig, wie dies tatsächlich erforder-

---

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.

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

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

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

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 Vgl. Belege in Fußnote 33 oben.

41 Uhe/Herrmann, Überwachung im Internet, http://ig.cs.tu-berlin.de/oldstatic/da/2003-08/UheHerrmann-Diplomarbeit-082003.pdf, 161.

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

lich ist. Die Vorratsdatenspeicherung demgegenüber erklärt den Eingriff unabhängig von seiner Erforderlichkeit zum Normalfall und stellt so die Grundrechtsordnung auf den Kopf.

Die Verstöße sind auch offensichtlich.

Dass der Richtlinie 2006/24/EG eine Rechtsgrundlage fehlt und die EG außerhalb ihrer Kompetenz gehandelt hat, ergibt sich ohne Weiteres aus dem Urteil des Europäischen Gerichtshofs zur Fluggastdatenübermittlung in die USA.[43] Die dortigen Erwägungen sind wörtlich auf die Vorratsdatenspeicherung übertragbar. Die fehlende Rechtsgrundlage steht der Richtlinie 2006/24/EG „auf die Stirn geschrieben".

Auch der Verstoß gegen die Gemeinschaftsgrundrechte liegt auf der Hand. Der Europäische Gerichtshof für Menschenrechte hat staatliche Eingriffe in die Vertraulichkeit der Telekommunikation stets nur im Einzelfall zugelassen. Dass eine allgemeine, rein vorsorgliche Protokollierung des Telekommunikationsverhaltens aller Europäer in einer demokratischen Gesellschaft nicht erforderlich und verhältnismäßig ist, ist evident.

d) Fehlende Umsetzungspflicht nach Völkerrecht

Zum Umsetzung der Richtlinie 2006/24/EG wäre Deutschland selbst dann nicht verpflichtet oder berechtigt, wenn der Europäische Gerichtshof eine Umsetzungspflicht annähme. Normen des sekundären Gemeinschaftsrechts, die gegen primäres Gemeinschaftsrecht verstoßen, sind vom deutschen Zustimmungsgesetz zum EG-Vertrag nicht gedeckt[44], seien sie inexistent oder nicht. Die mit der Umsetzung befassten Staatsorgane sind aus verfassungsrechtlichen Gründen gehindert, diese Rechtsakte in Deutschland anzuwenden[45], etwa durch Umsetzung einer Richtlinie. Das Gutachten des Wissenschaftlichen Dienstes des Bundestages vom 03.08.2006 bestätigt:

> „*Die Umsetzungsverpflichtung dürfte nur in drei Fällen entfallen: [...] drittens, wenn sich die europäischen Organe bei Erlass der Richtlinie nicht in den Grenzen der Hoheitsbefugnisse bewegt haben, die ihnen von den Mitgliedstaaten eingeräumt worden sind*".[46]

Die Reichweite des deutschen Zustimmungsgesetzes ist eine Frage des deutschen Rechts. Dementsprechend entscheiden letztverbindlich nicht die Organe der Europäischen Gemeinschaft, sondern die deutschen Verfassungsorgane darüber, ob sich EG-Rechtsakte in den Grenzen der ihnen eingeräumten Hoheitsrechte halten oder aus ihnen ausbrechen.[47]

Dass die Richtlinie 2006/24/EG formell wie materiell gegen das primäre Gemeinschaftsrecht verstößt und damit die im EG-Vertrag übertragenen Hoheitsbefugnisse überschreitet, ist bereits dargelegt worden. Unabhängig davon, wie das Europarecht bzw. der Europäische Gerichtshof die Frage der Umsetzungspflicht beurteilt, ist Deutschland daher völkerrechtlich zur Umsetzung der Richtlinie 2006/24/EG nicht verpflichtet. Würden europäische Organe eine Umsetzungspflicht für einen Rechtsakt annehmen, der vom Zustimmungsgesetz nicht gedeckt ist, so handelten sie selbst außerhalb des Zustimmungsgesetzes.

---

43 EuGH, Urteil vom 30.05.2006, Az. C-317/04 und C-318/04.

44 BVerfGE 89, 155 (188).

45 BVerfGE 89, 155 (188).

46 http://www.bundestag.de/bic/analysen/2006/-zulaessigkeit_der_vorratsdatenspeicherung_nach_europaeischem_und_deutschem_recht.pdf, 21.

47 BVerfGE 89, 155 (188).

IV. Fazit

Die in dem Gesetz zur Neuregelung der Telekommunikationsüberwachung angeordnete Erfassung des Telekommunikations- und Bewegungsverhaltens der gesamten Bevölkerung ist offensichtlich verfassungswidrig. Dementsprechend appellieren wir an Sie, die Unterzeichnung dieses Gesetzes abzulehnen.

Bei Rückfragen stehen wir gerne zu Ihrer Verfügung.

Mit freundlichen Grüßen,