Arbeitskreis Vorratsdatenspeicherung • Netzwerk Neue Medien e.V. • Neue Richtervereinigung e.V.

Stellungnahme zum Regierungsentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG

Zusammenfassung

Der Regierungsentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung sieht vor, Telekommunikationsunternehmen ab 2008 zu verpflichten, Daten über die Kommunikation ihrer Kunden auf Vorrat zu speichern. 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.

Eine derart weitreichende Registrierung des Verhaltens der Menschen in Deutschland ist inakzeptabel. 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.

Einer Studie des Bundeskriminalamts vom November 2005 zufolge reichen die gegenwärtig verfügbaren Kommunikationsdaten zur effektiven Aufklärung von Straftaten ganz regelmäßig aus. Eine Vorratsdatenspeicherung würde nicht besser vor Kriminalität schützen, dafür aber Millionen von Euro kosten, die Privatsphäre Unschuldiger gefährden, vertrauliche Kommunikation beeinträchtigen und den Weg in eine immer weiter reichende Massenansammlung von Informationen über die gesamte Bevölkerung ebnen.

Im Einklang mit seiner bisherigen Rechtsprechung wird das Bundesverfassungsgericht die vorgesehene Pflicht zur verdachtslosen Vorratsspeicherung von Kommunikationsdaten für verfassungswidrig erklären. Der Europäische Gerichtshof wird nach der Fluggastdatenübermittlung in die USA auch die EG-Richtlinie zur Vorratsdatenspeicherung mangels Rechtsgrundlage für nichtig erklären. Bereits gegenwärtig ist Deutschland zur Umsetzung der mit schweren Fehlern behafteten Richtlinie zur Vorratsdatenspeicherung nicht verpflichtet.

Wir lehnen das Vorhaben einer Vorratsdatenspeicherung entschieden ab und appellieren an die Politik, sich von dem Vorhaben der umfassenden und verdachtsunabhängigen Speicherung von Daten zu distanzieren. Die Umsetzung der Richtlinie 2006/24/EG hat wenigstens bis auf weiteres zu unterbleiben, um den Ausgang der anhängigen Nichtigkeitsklage gegen die Richtlinie 2006/24/EG sowie der Verfassungsbeschwerde gegen die Vorratsspeicherung von Telekommunikations-Bestandsdaten abzuwarten.

Dem Gutachten des Wissenschaftlichen Dienstes des Bundestages vom 03.08.2006 zufolge droht bei Umsetzung der Richtlinie deren spätere Nichtigerklärung durch den Europäischen Gerichtshof und die Verwerfung des deutschen Umsetzungsgesetzes als verfassungswidrig durch das Bundesverfassungsgericht. Demgegenüber ist im Fall eines Moratoriums lediglich die Einleitung eines Vertragsverletzungsverfahrens durch die EG-Kommission ohne finanzielle Nachteile für Deutschland zu befürchten. Dieser Weg ist deswegen einzuschlagen.

Inhaltsverzeichnis

A. Allgemeines

I. Inhalt und Auswirkungen des Gesetzesentwurfs

Der vorliegende Gesetzesentwurf sieht vor, dass Anbieter von Telekommunikationsdiensten künftig sechs Monate lang auf Vorrat speichern müssen, wer wann mit wem per Telefon, Handy oder E-Mail kommuniziert hat, wer sich mit welcher Kennung im Internet bewegt hat und an welchem Ort sich Handynutzer bei Beginn einer Verbindung aufgehalten haben (§§ 113a, 113b TKG-E). Die Speicherung soll für den Fall erfolgen, dass die Daten für strafrechtliche Ermittlungsverfahren benötigt werden. Anonymisierungsdienste sollen ebenfalls zu einer Vorratsdatenspeicherung verpflichtet werden.[1] Zugriffe auf die gespeicherten Daten sollen nicht nur zur Verfolgung schwerer Straftaten erlaubt sein, sondern bereits zur Verfolgung „erheblicher" Straftaten sowie jeglicher mittels Telekommunikation begangener Straftaten (§ 100g StPO). Weiter soll der Gesetzesentwurf das Angebot von Anonymisierungsdiensten faktisch unmöglich machen (§ 113a Abs. 6 TKG-E).

Die Verwendungsmöglichkeiten der zu speichernden Kommunikationsdaten sind enorm: Mit ihrer Hilfe können grobe Bewegungsprofile erstellt, geschäftliche Kontakte rekonstruiert und Freundschaftsbeziehungen identifiziert werden. Das Wissen über die Person der Kommunikationspartner kann zudem Rückschlüsse auf den Inhalt der Kommunikation, auf persönliche Interessen und die Lebenssituation der Kommunizierenden zulassen. So braucht es nicht viel Fantasie, um die Bedeutung einer E-Mail an eine AIDS-Beratungsstelle oder eines Telefonats mit einem auf Steuerstrafrecht spezialisierten Rechtsanwalt zu erkennen. Daneben erlauben es Kommunikationsdaten, jeden Klick und jede Eingabe im Internet minuziös zu rekonstruieren.

Wegen der weitgehenden Verwendungs- und Missbrauchsmöglichkeiten von Kommunikationsdaten ist ihre Aufzeichnung und Aufbewahrung bisher nur insoweit zulässig, wie es zu Abrechnungszwecken unbedingt erforderlich ist (§ 97 Abs. 3 TKG). Standortdaten und E-Mail-Verbindungsdaten werden deswegen bisher nicht gespeichert. Der Kunde kann verlangen, dass Abrechnungsdaten mit Rechnungsversand gelöscht werden (§ 97 Abs. 4 TKG). Durch die Benutzung von Pauschaltarifen kann eine Speicherung zudem bisher gänzlich vermieden werden, was etwa für Journalisten und Beratungsstellen wichtig ist.

Die verdachtslose, systematische Protokollierung des Kommunikationsverhaltens jedes Bürgers greift unangemessen in die persönliche Privatsphäre der Betroffenen ein. Aus den gespeicherten Daten über das Kommunikations- und Bewegungsverhalten lassen sich sensible Informationen über das Privat- und Intimleben ablesen. Erfahrungsgemäß kommt es immer wieder zur unbefugten Offenlegung vertraulicher Daten durch Mitarbeiter des speichernden Unternehmens, Mitarbeiter der Eingriffsbehörden oder Unbefugte („Hacker"). Die Offenlegung der Kommunikationsdaten etwa von Prominenten kann schwerwiegende Folgen nach sich ziehen und auch für kriminelle Handlungen wie Erpressung oder politische Zwecke genutzt werden.

Eine Vorratsdatenspeicherung beeinträchtigt ferner berufliche Aktivitäten (z.B. in den Bereichen Medizin, Recht, Kirche, Journalismus) ebenso wie politische und unternehmerische Aktivitäten, die Vertraulichkeit voraussetzen. Wenn jeder Kontakt etwa zu Berufsgeheimnisträgern nachvollzogen werden kann, werden Menschen, die ein Bekanntwerden ihres Kontakts vermeiden möchten, eine Kontaktaufnahme unterlassen. Bei befürchteten Repressalien, bestimmten Krankheiten oder strafrechtlichen Vorwürfen wollen die Betroffenen ein Bekanntwerden oft um jeden Preis vermeiden. Selbst wenn sie sich trotz der Vorratsdatenspeicherung nicht von einer Kontaktaufnahme abschrecken lassen, höhlt die Datenspeicherung das Arzt- und Anwaltsgeheimnis sowie den Quellenschutz von Journalisten aus. Die Vorratsdatenspeicherung führt zu Kommunikationsstörungen und zu Verhaltensanpassungen. Sie schaden damit unserer freiheitlichen Gesellschaft insgesamt.

1 § 113a Abs. 6 TKG-E.

Eine Vorratsdatenspeicherung verhindert Terrorismus oder Kriminalität nicht. Die ohnehin verfügbaren Kommunikationsdaten genügen zur Gewährleistung einer effektiven Strafverfolgung. Eine Vorratsdatenspeicherung kann von Kriminellen leicht umgangen werden. Sie würde die Verfolgung von Straftaten insgesamt gesehen nicht nennenswert verbessern, erst recht nicht die Sicherheit der Bürger stärken.

Eine Vorratsdatenspeicherung verstößt gegen das Menschenrecht auf Privatsphäre und informationelle Selbstbestimmung. In seinem Urteil zur Rasterfahndung hat das Bundesverfassungsgericht „das außerhalb statistischer Zwecke bestehende strikte Verbot der Sammlung personenbezogener Daten auf Vorrat" ausgesprochen.[2] Bereits 2003 hat das Bundesverfassungsgericht geurteilt:

> *„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".*[3]

Eine Vorratsdatenspeicherung ist teuer und belastet Wirtschaft und Verbraucher. Sie zwingt zur Anschaffung neuer Anlagen, die zur Datenspeicherung in der Lage sind. Vor allem aber müssen die Unternehmen Personal für die zu erwartenden Auskunftsanfragen vorhalten. Jährliche Kosten in Millionenhöhe sind zu erwarten, gerade bei E-Mail-Anbietern, die bisher keine Verkehrsdaten speichern müssen. Die Entwurfsbegründung erkennt an, dass jedem größeren Anbieter Mehrkosten in Höhe von „mehreren Hunderttausend Euro" drohen (S. 7). Die Kosten einer Vorratsdatenspeicherung können kleinere und nichtkommerzielle Anbieter zur Aufgabe ihres Angebots zwingen und größere Anbieter zu Preiserhöhungen. Schätzungen gehen von drohenden Preiserhöhungen um 10-15% aus. Auch die Entwurfsbegründung erkennt negative Auswirkungen auf das Verbraucherpreisniveau (S. 7).

Eine Vorratsdatenspeicherung diskriminiert Nutzer von Telefon, Mobiltelefon und Internet gegenüber anderen Kommunikationsformen. Dass die anonyme Kommunikation per Post oder im Wege eines unmittelbaren Gesprächs möglich bleibt, während gerade die elektronische Kommunikation protokolliert werden soll, ist nicht zu rechtfertigen. Alleine die technische und finanzielle Realisierbarkeit einer Protokollierung der Kommunikation im Bereich der Telekommunikationsnetze rechtfertigt diese Diskriminierung nicht. Viele Menschen sind beruflich oder privat auf die Nutzung von Telekommunikation angewiesen und haben keine Möglichkeit, für vertrauliche Gesprächen auf andere Kommunikationsmöglichkeiten auszuweichen.

II. Rechtliche Problematik

Am 04.04.2006 hat das Bundesverfassungsgericht die deutsche Rasterfahndung nach dem 11. September 2001 für verfassungswidrig erklärt und „das außerhalb statistischer Zwecke bestehende strikte Verbot der Sammlung personenbezogener Daten auf Vorrat" ausgesprochen.[4] Bereits 2003 hatte das Bundesverfassungsgericht geurteilt: „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".[5]

Am 30.05.2006 hat der Europäische Gerichtshof EG-Rechtsakte für nichtig erklärt, welche die Übermittlung von Fluggastdaten in die USA genehmigten.[6] Zur Begründung führte der Gerichtshof an, es handele sich um „eine Datenverarbeitung, die nicht für die Erbringung einer Dienstleistung erforderlich ist, sondern zum Schutz der öffentlichen Sicherheit und zu Strafverfolgungszwecken als erforderlich angesehen wird."[7] Für den Bereich der öffentlichen Sicherheit und der Strafverfolgung sei die Europäische Gemein-

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

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

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

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

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

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

schaft nicht zuständig. Dies gelte auch dann, wenn eine Harmonisierung unterschiedlicher Regelungen in den Mitgliedsstaaten angestrebt werde.

Am 06.07.2006 hat Irland Nichtigkeitsklage gegen die Richtlinie 2006/24/EG eingereicht[8] mit der Begründung, die Vorratsdatenspeicherung diene einer verbesserten Strafverfolgung und habe deswegen nicht im Wege einer EG-Richtlinie beschlossen werden können. Die Entscheidung des Gerichtshofs wird 2008 erwartet.

Am 03.08.2006 hat der Wissenschaftliche Dienst des Bundestages ein Rechtsgutachten vorgelegt[9], in dem es heißt: „Es bestehen Bedenken, ob die Richtlinie in der beschlossenen Form mit dem Europarecht vereinbar ist. Dies betrifft zum einen die Wahl der Rechtsgrundlage, zum anderen die Vereinbarkeit mit den im Gemeinschaftsrecht anerkannten Grundrechten." Im Hinblick auf die deutschen Grundrechte sei „zweifelhaft, dass dem Gesetzgeber aufgrund der europarechtlichen Vorgaben eine verfassungsgemäße Umsetzung gelingen" könne.

Am 18.07.2007 gab die Generalanwältin am Europäischen Gerichtshof eine Stellungnahme ab, in der es heißt: „Man kann daran zweifeln, ob die Speicherung von Verkehrsdaten aller Nutzer – gewissermaßen auf Vorrat – mit Grundrechten vereinbar ist, insbesondere da dies ohne konkreten Verdacht geschieht."[10] In der Stellungnahme wird die Rechtsprechung des Bundesverfassungsgerichts zitiert.

Bei dem Bundesverfassungsgericht ist derzeit eine Verfassungsbeschwerde gegen Vorschriften des Telekommunikationsgesetzes (§§ 95 Abs. 3, 111-113 TKG) anhängig[11], die Telekommunikationsanbieter zur Erhebung und Vorratsspeicherung von Telekommunikations-Bestandsdaten verpflichten. Die Entscheidung des Bundesverfassungsgerichts wird in wenigen Monaten erwartet.

III. Überschießende Richtlinienumsetzung, Unverbindlichkeit der Richtlinie 2006/24/EG

Art. 2 des vorliegenden Gesetzesentwurfs ist nicht durch die Richtlinie 2006/24/EG vorgegeben.

1. Überschießende und richtlinienwidrige Umsetzung in Deutschland

Eine Umsetzungspflicht besteht jedenfalls insoweit nicht als der Regierungsentwurf weit über die in der Richtlinie vorgesehenen Regelungen hinaus geht:

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.[12]

8 Az. C-301/06.

9 http://www.bundestag.de/bic/analysen/2006/-zulaessigkeit_der_vorratsdatenspeicherung_nach_europaeischem_und_deutschem_recht.pdf.

10 Generalanwältin am EuGH, Schlussanträge vom 18. Juli 2007 in der Rechtssache C-275/06, Rn. 82.

11 1 BvR 1299/05, http://www.tkg-verfassungsbeschwerde.de.

12 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).

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 rechtfertigen. E-Mail-Anbieter sollen künftig in das Online-Abrufverfahren des § 112 TKG einbezogen werden. Auch die Film- und Musikindustrie und andere „Rechteinhaber“ sollen Auskunft über die Identität der Kommunizierenden verlangen dürfen, etwa um die Benutzung von Tauschbörsen im Internet verfolgen zu können. 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. Nach Art. 4 S. 1 der Richtlinie ist sicherzustellen, „dass die gemäß dieser Richtlinie auf Vorrat gespeicherten Daten nur [...] an die zuständigen nationalen Behörden weitergegeben werden.“[13]

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

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

13 Vgl. Generalanwältin am EuGH, Schlussanträge vom 18. Juli 2007 in der Rechtssache C-275/06, Rn. 123 und 127: „Selbst wenn die Richtlinie 2006/24 anwendbar wäre, würde sie eine direkte Weitergabe von personenbezogenen Verkehrsdaten an Promusicae nicht erlauben. Nach Art. 1 bezweckt die Vorratsspeicherung allein die Ermittlung, Feststellung und Verfolgung von schweren Straftaten. Dementsprechend dürfen diese Daten gemäß Art. 4 nur an die zuständigen Behörden weitergegeben werden. [...] Die Richtlinie 2006/24 könnte vielmehr dazu führen, den gemeinschaftsrechtlichen Datenschutz in Bezug auf Streitigkeiten wegen Verletzungen des Urheberrechts zu stärken. Es stellt sich dann nämlich selbst in strafrechtlichen Ermittlungsverfahren die Frage, inwieweit es mit dem gemeinschaftsrechtlichen Grundrecht auf Datenschutz vereinbar ist, geschädigten Rechteinhabern Einblick in die Ermittlungsergebnisse zu gewähren, wenn diese auf der Auswertung von auf Vorrat gespeicherten Verkehrsdaten im Sinne der Richtlinie 2006/24 beruhen.“

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 2008 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 nicht verpflichtet.

Der Regierungsentwurf vertritt unter Hinweis auf Art. 242 EG die Auffassung (S. 61), bis zur Entscheidung des Europäischen Gerichtshofs über Irlands Nichtigkeitsklage[14] 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.[15] 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.[16] 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.[17]

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[18] und des Rates[19] 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 wäre, weil Ziel der Datenspeicherung die Erleichterung der Strafverfolgung ist.[20] 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

14 Az. C-301/06

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

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

17 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.

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

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

20 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.“

Gerichtshofs zur Fluggastdatenübermittlung in die USA.[21] 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."*[22]

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.[23] 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.[24] Er hat sogar ausdrücklich auf die Vorratsdatenspeicherung Bezug genommen.[25] 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.[26]

Einen Teil des primären Gemeinschaftsrechts stellen die Gemeinschaftsgrundrechte dar, die der Europäische Gerichtshof als „allgemeine Grundsätze des Gemeinschaftsrechts"[27] aus den Rechtstraditionen der

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

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

23 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.

24 Abs-Nr. 160 der Schlussanträge vom 22.11.2005.

25 Abs-Nr. 160 der Schlussanträge vom 22.11.2005.

26 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.

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

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.[28] Entsprechend Art. 8 EMRK hat der Europäische Gerichtshof beispielsweise den Schutz der Privatsphäre als Gemeinschaftsgrundrecht anerkannt.[29]

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.[30] Das Interesse des Staates muss gegenüber den Interessen des Einzelnen an der Achtung seiner Privatsphäre abgewogen werden.[31] Eingriffe sind zwar nicht auf das unerlässliche Maß beschränkt, aber ein bloßes Nützlich- oder Wünschenswertsein genügt nicht.[32]

Die Abwägung ergibt, dass eine Speicherung des Kommunikationsverhaltens der gesamten Bevölkerung grob unverhältnismäßig ist.[33] Die staatlichen Behörden würden nur einen kleinen Bruchteil (etwa 0,0004%[34]) der anfallenden Kommunikationsdaten jemals nachfragen, während mehr als 99% der Betroffenen[35] 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 erforderlich 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.[36] Die dortigen Erwägungen sind wörtlich auf die Vorratsdatenspeicherung übertragbar. Die fehlende Rechtsgrundlage steht der Richtlinie 2006/24/EG „auf die Stirn geschrieben".

---

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

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

30 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.

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

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

33 Vgl. Belege in Fußnote 26 oben.

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

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

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

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[37], seien sie inexistent oder nicht. Die mit der Umsetzung befassten Staatsorgane sind aus verfassungsrechtlichen Gründen gehindert, diese Rechtsakte in Deutschland anzuwenden[38], 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*“.[39]

Die Reichweite des deutschen Zustimmungsgesetzes ist eine Frage des deutschen Rechts. Dementsprechend entscheidet letztverbindlich nicht der Europäische Gerichtshof, sondern das Bundesverfassungsgericht darüber, ob sich EG-Rechtsakte in den Grenzen der ihnen eingeräumten Hoheitsrechte halten oder aus ihnen ausbrechen.[40]

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.

e) Nichtigerklärung der Richtlinie

Selbst wenn gegenwärtig eine Umsetzungspflicht bestünde, wird spätestens der Europäische Gerichtshof auf die Klage Irlands die Richtlinie aus den genannten Gründen für nichtig erklären. Mit dem Urteil ist Mitte 2008 zu rechnen. Diese Nichtigerklärung wird zur Folge haben, dass ein deutsches Umsetzungsgesetz ohne Einschränkungen an den deutschen Grundrechten zu messen ist. Mit dem Grundgesetz ist die Vorratsdatenspeicherung offensichtlich unvereinbar.[41]

IV. Position des Deutschen Bundestags

Das geforderte Umsetzungsmoratorium steht in Übereinstimmung mit mehreren Beschlüssen des Deutschen Bundestages, in denen die Einführung einer Vorratsdatenspeicherung abgelehnt worden ist. So heißt es im Bundestagsbeschluss vom 27.01.2005 (BT-Drs. 15/4748):

> „*Der Deutsche Bundestag erinnert an seine bei der Novellierung des Telekommunikationsgesetzes zum Ausdruck gekommene Ablehnung einer Mindestspeicherungsfrist für Verkehrsdaten und fordert die Bundesregierung auf, dies zur Grundlage ihrer Verhandlungen auf EU-Ebene zu machen.*“

37 BVerfGE 89, 155 (188).

38 BVerfGE 89, 155 (188).

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

40 BVerfGE 89, 155 (188).

41 Siehe Nachweise auf Seite 37.

Am 17.02.2005 hat der Deutsche Bundestag erneut beschlossen (BT-Drs. 15/4597):

> *„Der Deutsche Bundestag bekräftigt seine bereits bei Novellierung des Telekommunikationsgesetzes zum Ausdruck gekommene Ablehnung einer Mindestspeicherungsfrist für Verkehrsdaten und fordert, vorbehaltlich einer Darlegung entsprechender Rechtstatsachen, die die Notwendigkeit einer solchen Regelung auf europäischer Ebene darlegen und eine neue Behandlung dieser Thematik erfordern, die Bundesregierung auf, einen etwaigen Beschluss in den Gremien der Europäischen Union, der eine solche Verpflichtung für Unternehmen in Deutschland vorsähe, nicht mitzutragen.“*

Die Bundesregierung erklärte schon 1996 (BT-Drs. 13/4438):

> *„Die Forderung des Bundesrates, neben den 'Höchstfristen' auch 'Mindestfristen' für die Speicherung von personenbezogenen Daten der an der Telekommunikation Beteiligten vorzusehen sowie neben den Interessen der Unternehmen und Betroffenen auch diejenigen der in Absatz 6 Nr. 1 genannten Stellen einzubeziehen, wird abgelehnt. Damit würde den in § 86 Abs. 1 Satz 2 normierten Grundsätzen der Verhältnismäßigkeit, Erforderlichkeit und Zweckbindung beim Erlaß von Datenschutzvorschriften widersprochen.“*

Soweit sich der Bundestag am 16.02.2006 für die Richtlinienumsetzung aussprach (BT-Drs. 16/545), hat sich die Lage durch das Urteil des Europäischen Gerichtshofs zur Fluggastdatenübermittlung in die USA vom Mai 2006 grundlegend geändert. Die noch im Bundestagsbeschluss vom Februar 2006 geäußerten Zweifel an der gewählten Rechtsgrundlage haben sich durch das Urteil bestätigt. Eine Nichtigkeitsklage gegen die Richtlinie ist erhoben worden. Hinzu gekommen ist das Urteil des Bundesverfassungsgerichts zur Unzulässigkeit der Rasterfahndung, die anhängige Verfassungsbeschwerde gegen die Vorratsdatenspeicherung von Telekommunikations-Bestandsdaten sowie das Rechtsgutachten des Wissenschaftlichen Dienstes des Bundestages vom 03.08.2006. In Anbetracht all dieser veränderten Umstände kann an dem Bundestagsbeschluss vom 16.02.2006 weder politisch noch rechtlich festgehalten werden.

Im Übrigen widerspricht der vorliegende Regierungsentwurf selbst diesem Bundestagsbeschluss, weil der Gesetzentwurf unter anderem in Bezug auf E-Mail- und Anonymisierungsdienste, vor allem aber hinsichtlich der Verwendung der gesammelten Daten weit über die Mindestvorgaben der Richtlinie 2006/24/EG hinaus geht.[42]

V. Rechtsprechung des Bundesverfassungsgerichts

Der Einführung von Speicherungspflichten für Verkehrsdaten in Deutschland stehen die Grundrechte der betroffenen Bürger und die dazu ergangene verfassungsgerichtliche Rechtsprechung entgegen.[43]

Dies gilt zum einen für das vom Bundesverfassungsgericht ausgesprochene „außerhalb statistischer Zwecke bestehende strikte Verbot der Sammlung personenbezogener Daten auf Vorrat“.[44] Entgegen der Ansicht der Verfasser des Regierungsentwurfs (S. 66) gilt dieses Verbot nicht nur für eine Vorratsdatenspeicherung „zu unbestimmten oder noch nicht bestimmbaren Zwecken“. Diese Einschränkung hat das Bundesverfassungsgericht in seinem Urteil zur Rasterfahndung aufgegeben und nicht mehr genannt.[45] 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.

---

42 Siehe im Einzelnen Seite 6 oben.

43 Ebenso Deutscher Anwaltverein, Stellungnahme vom August 2007, http://www.anwaltverein.de/03/05/2007/-41-07.pdf, 36 ff.

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

45 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.“*

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.[46] 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.

Im Urteil 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."*[47] *„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."*[48]

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".*[49]

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.[50] 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.[51] 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."*[52]

---

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

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

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

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

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

51 BVerfGE 107, 299 (314).

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

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 wäre es ein vorsätzlicher Verfassungsbruch, eine Vorratsspeicherung von Telekommunikations-Verkehrsdaten gleichwohl zu beschließen.

Schon 1967 hat das Bundesverwaltungsgericht entschieden:

> *„Ausgangspunkt hat die Feststellung zu sein, daß nach dem Menschenbild des Grundgesetzes die Polizeibehörde nicht jedermann als potentiellen Rechtsbrecher betrachten und auch nicht jeden, der sich irgendwie verdächtig gemacht hat ('aufgefallen ist') oder bei der Polizei angezeigt worden ist, ohne weiteres 'erkennungsdienstlich behandeln' darf. Eine derart weitgehende Registrierung der Bürger aus dem Bestreben nach möglichst großer Effektivität der Polizeigewalt und Erleichterung der polizeilichen Überwachung der Bevölkerung widerspräche den Prinzipien des freiheitlichen Rechtsstaates.“*[53]

Die Vorratsdatenspeicherung geht weit über die Aufnahme vom Lichtbildern und Fingerabdrücken im Rahmen einer erkennungsdienstlichen Behandlung hinaus. Sie betrifft sensible Daten über die Kommunikation der Menschen mit ihren nächsten Angehörigen sowie mit Beratungs- und Hilfsberufen, über die sozialen Beziehungen der Menschen zueinander, über ihre Internetnutzung und über ihr Bewegungsverhalten. Eine derart weitreichende Registrierung des Verhaltens aller 82 Mio. Menschen in Deutschland aus dem Bestreben nach möglichst großer Effektivität der Polizeigewalt und Erleichterung der Verfolgung von Straftaten widerspricht den Grundprinzipien des freiheitlichen Rechtsstaates.

Mit Beschluss vom 22.08.2006 hat das Bundesverfassungsgericht an den Gesetzgeber nochmals eine besondere Warnung gerichtet:

> *„Das Bundesministerium der Justiz hat mitgeteilt, seit längerem an einer Gesamtregelung der strafprozessualen heimlichen Ermittlungsmaßnahmen zu arbeiten [...] Es stellt sich auch die Frage, ob und in welchem Umfang von einer neuerlichen Ausdehnung heimlicher Ermittlungsmethoden im Hinblick auf Grundrechtspositionen unbeteiligter Dritter Abstand zu nehmen ist.“*[54]

Die Vorratsdatenspeicherung stellt eine schwerwiegende Ausdehnung der heimlichen Telekommunikationsüberwachung dar und beschädigt Grundrechtspositionen unbeteiligter Dritter massiv.

VI. Lösung

Die Einführung einer Vorratsspeicherung von Telekommunikations-Verkehrsdaten in Deutschland zur Umsetzung der Richtlinie 2006/24/EG hat bis auf weiteres zu unterbleiben, um zunächst den Ausgang der anhängigen Nichtigkeitsklage gegen die Richtlinie 2006/24/EG sowie der Verfassungsbeschwerde gegen die Vorratsspeicherung von Telekommunikations-Bestandsdaten abzuwarten.

Dem Gutachten des Wissenschaftlichen Dienstes des Bundestages vom 03.08.2006 zufolge droht bei Umsetzung der Richtlinie deren spätere Nichtigerklärung durch den Europäischen Gerichtshof und die Verwerfung des deutschen Umsetzungsgesetzes als verfassungswidrig durch das Bundesverfassungsgericht. Demgegenüber ist im Fall eines Moratoriums lediglich die Einleitung eines Vertragsverletzungsverfahrens durch die EG-Kommission ohne finanzielle Nachteile für Deutschland zu befürchten. Dieser Weg ist deswegen einzuschlagen.

53 BVerwG, 1 C 57.66 vom 09.02.1967.

54 BVerfG, 2 BvR 1345/03 vom 22.08.2006, MMR 2006, 805 (810), Abs. 84.

VII. Einordnung des Gesetzesentwurfs in die Sicherheitspolitik der letzten Jahre

Der vorliegende Gesetzesentwurf und insbesondere die darin vorgesehene Vorratsdatenspeicherung geben Anlass zu grundsätzlichen Anmerkungen zur Innen- und Justizpolitik der letzten Jahre und Jahrzehnte.

Nach dem Zusammenbruch des totalitären Dritten Reichs haben sich die Deutschen ein Grundgesetz gegeben, das die Würde des Menschen in den Mittelpunkt alles staatlichen Handelns stellt (Art. 1 GG) und an zweiter Stelle das Menschenrecht auf ein freies, selbstbestimmtes Leben nennt (Art. 2 GG). Dieses Recht begründet einen Anspruch der Menschen auf ein Leben frei von staatlicher Einmischung und Überwachung. Jeder Mensch hat ein Recht darauf, vom Staat in Ruhe gelassen zu werden, solange er nicht die Rechte anderer stört (Art. 2 i.V.m. Art. 1 GG). Dieser Schutz gilt für unsere Privatsphäre (Art. 8 EMRK) ebenso wie für unsere Kommunikation (Art. 10 GG) und für unser Verhalten in der Öffentlichkeit.

Seit 1968 erfolgt demgegenüber eine stetige Aushöhlung des Rechts auf Selbstbestimmung im Wege immerwährender vorgeblich „maßvoller Ausweitungen“ der Überwachungs-, Kontroll- und sonstigen Machtbefugnisse staatlicher Behörden. Der vorliegende Gesetzesentwurf ist symptomatisch für diese Entwicklung. Dabei zeigen wissenschaftliche Vergleichsstudien, dass die Kriminalitätsrate von den Befugnissen der Eingriffsbehörden unabhängig ist.[55] Insgesamt betrachtet nützt die beständige Aufrüstung der Sicherheitsbehörden der Gesellschaft also nicht. Dagegen hat sie dazu geführt, dass wir inzwischen in einer Überwachungsgesellschaft angekommen sind.[56]

Wenn wir unseren Kindern auch nur einen Teil des Menschenrechts auf Selbstbestimmung erhalten wollen, müssen Regierung, Parlament und Gerichte Grenzen setzen und rote Linien ziehen, die auch im Eifer der Sicherheitspolitik nicht überschritten werden dürfen. Der vorliegende Gesetzesentwurf überschreitet eine solche rote Linie, nämlich das Verbot der anlasslosen Sammlung personenbezogener Daten auf Vorrat. Eine weitere rote Linie verläuft dort, wo Personen massenweise und ohne besonderen Anlass kontrolliert und abgeglichen werden. Diese Grenze wird etwa bei einem automatisierten Abgleich von Kfz-Kennzeichen oder von Gesichtern mit Fahndungsdatenbanken überschritten.

Wir fordern einen grundlegenden Wandel der Innen- und Justizpolitik. Alle seit 1968 zugunsten der staatlichen Eingriffsbehörden erfolgten Grundrechtsbeschränkungen müssen einer unabhängigen Überprüfung unterzogen werden. Schwerwiegende Grundrechtseingriffe, von denen kein messbarer gesamtgesellschaftlicher Nutzen ausgeht, müssen aufgehoben werden. Eine weitere Ausweitung der Machtbefugnisse der Eingriffsbehörden darf erst erfolgen, wenn nachgewiesen ist, dass von dem jeweiligen Gesetz ein messbarer gesamtgesellschaftlicher Nutzen ausgeht. Zur unabhängigen Durchführung der Überprüfungen fordern wir die Einrichtung einer Deutschen Grundrechteagentur. Außerdem muss es möglich werden, bereits vor dem Beschluss eines Gesetzes ein Gutachten des Bundesverfassungsgerichts über die Verfassungsmäßigkeit des Gesetzesvorhabens einzuholen.

55 Rohe, Verdeckte Informationsgewinnung mit technischen Hilfsmitteln zur Bekämpfung der Organisierten Kriminalität (1998), 47.

56 Surveillance Studies Network, Bericht vom September 2006, http://www.privacyconference2006.co.uk/files/report_ger.pdf.

B. Zu einzelnen Vorschriften des Gesetzesentwurfs

I. § 53b StPO-E [Schutz von Berufsgeheimnisträgern]

Es ist nicht nachvollziehbar, warum § 53b Abs. 1 StPO nur Geistliche, Strafverteidiger und Abgeordnete verlässlich vor verdeckten Ermittlungsmaßnahmen schützen soll, Beratungsstellen, Ärzte, Rechtsanwälte, Journalisten und andere Berufsgeheimnisträger dagegen nicht. Diese Unterscheidung ist sachlich nicht gerechtfertigt und beschädigt das Vertrauensverhältnis von Angehörigen dieser Berufe zu ihren Kommunikationspartnern.[57] Eine vertrauliche Beratung ist essentiell für Menschen, die sich in Not befinden und darauf angewiesen sind, dass niemand – auch nicht der Staat – von ihrer Notlage erfährt. Auch der Schutz von Presseinformanten vor Enttarnung ist von besonderer gesellschaftlicher Bedeutung.

Weiter ist es nicht gerechtfertigt, die verdeckte Überwachung besonders eng verbundener Familienmitglieder (§ 52 StPO) uneingeschränkt zuzulassen. Nicht einmal die Einschränkung des § 53b Abs. 2 StPO-E soll gelten, obwohl auf der Hand liegt, dass etwa zum eigenen Ehegatten ein sehr viel engeres Vertrauensverhältnis besteht als zu Geistlichen, Strafverteidigern oder gar Abgeordneten.

Wir fordern, das Erhebungs- und Verwertungsverbot des § 53b Abs. 1 StPO einheitlich auf alle Zeugnisverweigerungsberechtigten nach den §§ 52-53a StPO zu erstrecken.

II. §§ 100a, 100b StPO-E [Telekommunikationsüberwachung]

1. Fehlende Einbeziehung von Verkehrs- und Bestandsdaten

Wir fordern, den staatlichen Zugriff auf Informationen über die Kommunikation und die Kommunizierenden („Verkehrsdaten“, „Bestandsdaten“) den gleichen Voraussetzungen zu unterwerfen wie den Zugriff auf die Inhalte der Kommunikation.[58] Dazu sind Verkehrs- und Bestandsdaten in den Anwendungsbereich der §§ 100a, 100b StPO einzubeziehen.

Wenn verbreitet angenommen wird, der Zugriff auf Kommunikationsinhalte sei eingriffsintensiver als der Zugriff auf Verkehrsdaten, beruht dies auf einem Irrtum.[59] Die Eingriffstiefe bestimmt sich laut Bundesverfassungsgericht nicht nach der Art der Daten, sondern nach deren Nutzbarkeit und Verwendungsmöglichkeiten.[60] Die Verwendungsmöglichkeiten von Verkehrsdaten sind enorm und größer als von Inhaltsdaten. Die automatisierte Verarbeitung und Verknüpfung der computerlesbaren Verkehrsdaten ermöglicht die Abbildung von Freundschafts- und Beziehungsnetzwerken, die Erstellung von Bewegungsprofilen, die Identifizierung von Interessen und politischer Einstellungen anhand der Kommunikationspartner eines Menschen (z.B. Anruf bei politischer Partei, Telefonat mit Arzt für Geschlechtskrankheiten). Auch können Verkehrsdaten in großen Mengen mit geringem finanziellen oder personellen Aufwand erhoben und analysiert werden. All dies ist bei Inhaltsdaten nicht möglich. Insgesamt sind Verkehrsdaten nicht weniger schutzwürdig als Kommunikationsinhalte und bedürfen des gleichen gesetzlichen Schutzniveaus.[61] Die österreichische Strafprozessordnung verfolgt diesen richtigen Ansatz bereits (§ 149a öStPO).

Auch für Bestandsdaten muss die gleiche Eingriffsschwelle gelten, denn Bestandsdaten ermöglichen erst die Zuordnung bekannter Kommunikationsinhalte zur Person der Beteiligten oder die Erhebung weiterer Kommunikationsinhalte (durch Überwachungsmaßnahmen oder – bei PINs und Passwörtern – durch un-

57 Ebenso Deutscher Anwaltverein, Stellungnahme vom August 2007, http://www.anwaltverein.de/03/05/2007/-41-07.pdf, 5 ff.

58 Ebenso Bundesrechtsanwaltskammer, Stellungnahme vom August 2007, http://brak.de/seiten/pdf/-Stellungnahmen/2007/Stn31.pdf, 45.

59 Ebenso Bundesrechtsanwaltskammer a.a.O.

60 BVerfGE 65, 1 (45).

61 Näher Breyer, Vorratsspeicherung (2005), www.vorratsspeicherung.de.vu, 211 ff.

mittelbaren Zugriff). Die Identität der Kommunikationspartner ist integraler Bestandteil der Kommunikation selbst. Dies wird näher erläutert auf Seite 32 dieser Stellungnahme.

2. Unzureichende Eingriffsvoraussetzungen

§ 100a StPO-E sieht eine erhebliche Ausweitung der Straftaten vor, deren Verdacht eine Überwachung der Telekommunikation rechtfertigen soll.

Das Ziel des Gesetzesentwurfs, den Jahr für Jahr zu beobachtenden rasanten Anstieg der Zahl von Überwachungsanordnungen einzudämmen, wird so verfehlt. Wenn wenig praxisrelevante Straftaten aus dem Katalog der Anlasstaten gestrichen werden, gleichzeitig aber sehr häufig verwirklichte Straftatbestände neu aufgenommen werden, wird es zu einem sprunghaften Anstieg der Anzahl von Überwachungsmaßnahmen kommen. Außerdem wird der Gesetzgeber den Anlasstatenkatalog weiterhin in regelmäßigen Zeitabständen erweitern, wie es in den vergangenen Jahren geschehen ist.

Zweckmäßig ist stattdessen eine Bestimmung der Eingriffsvoraussetzungen anhand der konkreten Straferwartung des Beschuldigten. Durch eine solche Eingrenzung kann eine einzelfallgerechte Lösung gefunden und auf den Anlasstatenkatalog verzichtet werden.

In Anbetracht der zunehmenden Telekommunikationsüberwachung ist eine erhebliche Heraufsetzung der Eingriffsschwelle erforderlich. Der im zeitlichen und internationalen Vergleich starke Anstieg der Telekommunikationsüberwachung in den letzten Jahren lässt sich nicht mit dem Argument rechtfertigen, Straftäter benutzten mehrere Anschlüsse (z.B. Handys). Denn auch wenn man anstelle der Überwachungsanordnungen die Strafverfahren zählt, in denen eine Telekommunikationsüberwachung erfolgt ist, stellt man Jahr für Jahr einen Anstieg der Fälle um durchschnittlich 10% fest. Alle sieben Jahre kommt es zu einer Verdoppelung der Verfahren mit Telekommunikationsüberwachung.[62]

Um dieser Entwicklung gegenzusteuern, sollte der heimliche Zugriff auf die Telekommunikation zwecks Strafverfolgung generell auf Fälle organisierter oder gewerbsmäßiger Kriminalität, in denen eine höhere Strafe als vier Jahre Freiheitsstrafe zu erwarten ist, beschränkt werden. Die in § 100a StPO-E vorgesehenen Anlasstaten stellen zu einem großen Teil keine schweren Straftaten dar, sondern Straftaten im unteren und mittleren Kriminalitätsbereich. Solche Taten rechtfertigt nicht den schwerwiegenden Eingriff einer heimlichen Überwachung der Telekommunikation, die eine Vielzahl Unschuldiger betrifft, etwa die nicht an einer Straftat beteiligten Gesprächspartner.

In Schweden setzte eine Telekommunikationsüberwachung bis vor kurzem generell eine zu erwartende Freiheitsstrafe von mindestens drei Jahren voraus. Erst im Zuge der terroristischen Anschläge des 11.9.2001 wurde diese Schwelle auf zwei Jahre abgesenkt. In Großbritannien ist eine Telekommunikationsüberwachung bei gewerbs- oder bandenmäßig begangenen Straftaten oder alternativ bei einer zu erwartenden Freiheitsstrafe von mindestens zwei Jahren zulässig, wobei die Straferwartung unter Außerachtlassung von Vorstrafen bemessen wird. Bei vorbestraften Tätern entspricht dies somit eher einer Straferwartung von drei Jahren. In Deutschland ist der Vergleich zur akustischen Wohnraumüberwachung angebracht, weil abgehörte Telekommunikation typischerweise in Wohnungen stattfindet und Gespräche betrifft, die ohne Telekommunikation im Schutz von Wohnungen geführt werden würden.

Maßgeblich für die Eingriffsschwelle muss neben der Schwere der Straftat sein, welches Maß an Rechtsgüterschutz die Strafverfolgung für die Zukunft gewährleisten kann. Der schwerwiegende Eingriff einer heimlichen Telekommunikationsüberwachung ist nur zu rechtfertigen, wenn er dem Rechtsgüterschutz dient. Voraussetzung muss danach sein, dass aufgrund bestimmter Tatsachen im Einzelfall zu befürchten ist, dass der Beschuldigte Straftaten dieser Art erneut begehen wird (z.B. bei gewerbs- oder bandenmäßiger Begehung, organisierte Kriminalität).

Wir fordern, den Anwendungsbereich des § 100a StPO anhand der zu erwartenden Strafe zu regeln. Der heimliche Zugriff auf die Telekommunikation zwecks Strafverfolgung ist auf Fälle organisierter oder

62 Breyer, Vorratsspeicherung (2005), www.vorratsspeicherung.de.vu, 23 m.w.N.

gewerbsmäßiger Kriminalität zu beschränken, in denen eine höhere Strafe als vier Jahre Freiheitsstrafe zu erwarten ist.

3. Fehlende Erfolgskontrolle (§ 100b Abs. 6 StPO-E)

§ 100b Abs. 6 StPO sah in der Fassung des Referentenentwurfs noch Ansätze einer aussagekräftigen Evaluierung und Selbstkontrolle vor. Danach sollte in die amtliche Statistik eingehen

> *4. die Anzahl der Beteiligten der überwachten Telekommunikation;*
>
> *5. ob die Überwachung Ergebnisse erbracht hat, die für das Verfahren relevant sind oder voraussichtlich relevant sein werden;*
>
> *6. ob die Überwachung Ergebnisse erbracht hat, die für andere Strafverfahren relevant sind oder voraussichtlich relevant sein werden.*

Die Notwendigkeit einer umfassenden Evaluierung staatlicher Eingriffsermächtigungen macht schon der Zweite Sicherheitsbericht der Bundesregierung aus dem Jahr 2006 deutlich. Darin heißt es zutreffend:

> *„Ohne gesichertes Wissen lässt sich alles irgendwie rechtfertigen. Solange also verlässliche und abgesicherte Erkenntnisse darüber fehlen, welches Problem besteht, mit welchen Mitteln und unter welchen Bedingungen die besten Ergebnisse erzielt und schädliche Nebenwirkungen am ehesten vermieden werden können, ist eine rationale Entscheidung zwischen Alternativen nicht möglich. [...] Die inzwischen vorliegenden Hilfen zur Evaluation polizeilicher Arbeitsformen müssten ergänzt werden durch eine breite Evaluation strafrechtlicher Maßnahmen; hier liegt ein großes Evaluationsdefizit vor. Denn weder dürfen Evaluationen nur auf nichtstrafrechtliche Interventionen beschränkt bleiben; Wirkungsforschung muss schon aus verfassungsrechtlichen Vorgaben alle staatlichen Maßnahmen betreffen. […] Auch gibt es immer wieder Situationen, in denen gehandelt werden muss, ohne dass die verfügbaren Strategien bereits evaluiert sind. Allerdings: Ehe sie in Allgemeinpraxis überführt werden, müssen sie sich erfolgreich einer externen Evaluation gestellt haben. Dies entspricht auch dem verfassungsrechtlichen Gebot, staatliche – insbesondere auch strafende staatliche Eingriffe – nach Art und Maß am Gebot der Erforderlichkeit (und damit auch zwingend der Wirksamkeit) auszurichten und zu begrenzen. Die Forderung nach mehr oder härteren strafenden Eingriffen findet in den – national wie international – vorliegenden Befunden jedenfalls keine Rechtfertigung. Umso wichtiger ist die systematische Evaluation sowohl präventiver wie auch klassisch-strafrechtlicher Reaktionsformen.“*[63]

Voraussetzung jeder aussagekräftigen Evaluierung ist eine ausreichende Datenlage. Welche Angaben auf dem Gebiet der Telekommunikationsüberwachung sinnvollerweise statistisch erhoben werden können, zeigt die folgende Aufstellung, die sich an einer Ausarbeitung der Internationalen Arbeitsgruppe über den Datenschutz in der Telekommunikation[64] orientiert:

1. Anlass eines Eingriffs in das Fernmeldegeheimnis und die Angabe, ob die erlangten Erkenntnisse anschließend nur zu diesem oder gegebenenfalls zu welchen anderen Zwecken (auch mittelbar) genutzt wurden.
2. Anzahl der angeordneten oder verlängerten Maßnahmen und gegebenenfalls die Dauer der Anordnung oder Verlängerung sowie die Anzahl der abgelehnten Anträge.
3. Anzahl der Kommunikationsvorgänge, in die eingegriffen wurde, unterteilt in solche mit und solche ohne Bedeutung für das Ermittlungsverfahren (aufgrund nachträglicher Auswertung).

63 http://www.bmi.bund.de/nn_121560/Internet/Content/Common/Anlagen/Broschueren/2006/-2__Periodischer__Sicherheitsbericht/2__PSB__Kapitel__1,templateId=raw,property=publicationFile.pdf/2_PSB_Kapitel_1.pdf

64 IWGDPT, Öffentliche Verantwortung bei Abhörmaßnahmen, www.datenschutz-berlin.de/doc/int/iwgdpt/inter_de.htm.

4. Anzahl der identifizierten Einzelpersonen, nicht nur der in der gerichtlichen Anordnung genannten, unter gesondertem Ausweis der Anzahl von Personen, die zeugnisverweigerungsberechtigt waren (Vertrauensverhältnisse).
5. Art der Kommunikationsdienste, in die eingegriffen wurde (etwa Telefon, Fax, E-Mail, Pager, Sprachbox-Dienste) und Art der Daten, auf die zugegriffen wurde (wie Kommunikationsinhalte, Telekommunikations-Verbindungsdaten, Standortdaten, Internet-Nutzungsdaten, Bestandsdaten).
6. Art der untersuchten Straftaten.
7. Resultate und Effektivität von Maßnahmen, wie z.B. die Anzahl der Fälle, in denen keine Hinweise für Straftaten gefunden wurden; die Anzahl der Fälle, in denen aufgrund der Maßnahme Verhaftungen erfolgen konnten; die Anzahl der Fälle, in denen aufgrund der Maßnahme Anklage erhoben wurde; die Anzahl der Fälle, in denen aufgrund der Maßnahme erlangte Daten als Beweismittel verwendet wurden; die Anzahl der Fälle, in denen aufgrund der Maßnahme ein Schuldspruch erfolgte, sowie das Maß der ausgesprochenen Strafe; die Anzahl der Fälle, in denen aufgrund der Maßnahme die Unschuld einer Person nachgewiesen werden konnte.
8. Kosten der Maßnahme (Sach- und Personalmittel von Behörden und Dritten).

Dass die Erstellung derartiger Statistiken keinen übermäßigen Aufwand verursacht, verdeutlichen die US-amerikanischen „Wiretap-Reports“, in denen über viele der genannten Punkte Rechenschaft abgelegt wird.[65]

Bezüglich der Wirkung von Evaluierungsmaßnahmen ist anzumerken, dass die Anzahl von Maßnahmen der Telefonüberwachung in den USA nach Einführung der Berichtspflicht erheblich zurückging[66]. Sicherlich kostet eine Berichtspflicht Zeit und Geld der Entscheidungsträger. Gerade hierdurch kann aber gewährleistet werden, dass Eingriffe nur dort vorgenommen werden, wo sie wirklich erforderlich sind. Dies gewährleistet zugleich die effektivere Nutzung finanzieller und personeller Ressourcen der Strafverfolgungsbehörden.

Wir fordern, zumindest die noch im Referentenentwurf vorgesehenen Informationen über Umfang und Ergebnis der Überwachungsmaßnahmen in die Statistik nach § 100b Abs. 6 StPO-E aufzunehmen. Informationen über die Effektivität der Maßnahmen braucht der Gesetzgeber, um die Verhältnismäßigkeit der Norm überprüfen zu können, wie es verfassungsrechtlich geboten ist.

III. § 100g StPO-E [Erhebung von Verkehrsdaten]

1. Fehlende Beschränkung auf schwere Straftaten

Soweit vorratsgespeicherte Telekommunikationsdaten betroffen sind, verstößt § 100g StPO-E und die §§ 112, 113 TKG gegen die Richtlinie 2006/24/EG. Nach der Richtlinie erfolgt die Vorratsspeicherung allein für die Verfolgung „schwerer Straftaten“ (Art. 1 Abs. 1 RiL 2006/24/EG). Die Generalanwältin beim Europäischen Gerichtshof weist zurecht darauf hin, dass diese Regelung die Verwendung der gesammelten Daten verbindlich beschränkt.[67]

Zeitgleich mit dem Richtlinienentwurf hat der Rat zwar eine „Erklärung“ verabschiedet, der zufolge die Mitgliedsstaaten „[b]ei der Definition des Begriffs 'schwere Straftat' im einzelstaatlichen Recht [...]

65 DSB-Konferenz, Datenschutzbeauftragte des Bundes und der Länder: Effektive parlamentarische Kontrolle von Lauschangriffen durch aussagekräftige jährliche Berichte der Bundesregierung, Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 26.06.2000, BT-Drs. 14/5555, 226.

66 taz vom 18.12.2000, 11.

67 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).

Straftaten unter Einsatz von Telekommunikationseinrichtungen angemessen zu berücksichtigen“ haben.[68] Dieser Beschluss will die Richtlinie allerdings bereits seinem Wortlaut nach nicht abändern, sondern richtet sich ausschließlich an die Mitgliedsstaaten. Ohnehin kann der Rat nicht durch einseitigen Beschluss eine Richtlinie abändern, die der Mitentscheidung des Europäischen Parlaments unterliegt. Die Erklärung des Rates kann daher nur so verstanden werden, dass die Mitgliedsstaaten unter allen schweren Straftaten auch die mittels Telekommunikation begangenen angemessen berücksichtigen sollen, wenn sie den Zugriff auf vorratsgespeicherte Daten regeln.

Nicht überzeugend ist es jedenfalls, wenn das Bundesjustizministerium kurzerhand erklärt: „*Zweck der Speicherung ist die Ermittlung, Aufdeckung und Verfolgung schwerer Straftaten, zu denen auch alle mittels Telekommunikation begangene Straftaten gehören.*“[69] Eine am Telefon ausgesprochene Beleidigung ist ebenso wenig eine schwere Straftat wie jede andere Beleidigung. Auch die in der Begründung des Regierungsentwurfs angeführten Zweckmäßigkeitsargumente gegen eine Beschränkung auf die Verfolgung schwerer Straftaten (S. 116) überzeugen nicht, zumal der Regierungsentwurf selbst darlegt, dass eine solche Beschränkung möglich ist.

Der Begriff der „schweren Straftaten“ beschreibt, in die Terminologie des Bundesverfassungsgerichts übersetzt, Straftaten im oberen Kriminalitätsbereich.[70] Demgegenüber erlaubt § 100g StPO-E den Zugriff auf Verkehrsdaten bereits zur Verfolgung „erheblicher“ Straftaten des mittleren Kriminalitätsbereiches sowie zur Verfolgung jeder mittels Telekommunikation begangener Tat. Selbst der Verdacht einer am Telefon oder im Internet begangenen Bagatellstraftat soll also eine Durchleuchtung des Kommunikationsverhaltens rechtfertigen können. Die Identifizierung von Telefon- und Internetnutzern wird sogar zur Verfolgung jeder Straftat oder Ordnungswidrigkeit zugelassen (§§ 112, 113 TKG). Dass all dies mit der vom Europaparlament mühsam errungenen und als Erfolg präsentierten Beschränkung auf die Verfolgung „schwerer Straftaten“ nicht in Einklang zu bringen ist, liegt auf der Hand. Die vorgesehenen Zugriffsregelungen sind mit der Vorratsspeicherungsrichtlinie folglich nicht vereinbar.

Die weiter gehenden deutschen Regelungen lassen sich auch nicht auf Art. 15 RiL 2002/58/EG stützen.[71] Insoweit ist der neue Absatz 1a dieses Artikels zu beachten. Danach sind diejenigen Datentypen vor weiter gehenden Zugriffsbefugnissen geschützt, für welche in der Richtlinie 2006/24/EG „eine Vorratsspeicherung zu den in Artikel 1 Absatz 1 der genannten Richtlinie aufgeführten Zwecken ausdrücklich vorgeschrieben ist“. Für sämtliche der in der Vorratsspeicherungsrichtlinie genannten Verkehrs- und Bestandsdaten ist „eine Vorratsspeicherung zu den in Artikel 1 Absatz 1 der genannten Richtlinie aufgeführten Zwecken ausdrücklich vorgeschrieben“, so dass sämtliche in der Vorratsspeicherungsrichtlinie genannte Daten vor Zugriffen zu anderen Zwecken geschützt sind.

Abweichend vom klaren Wortlaut des Art. 15 Abs. 1a RiL 2002/58/EG geht Erwägungsgrund 12 der Vorratsspeicherungsrichtlinie davon aus, dass ein Zugriff auf vorratsgespeicherte Daten auch „zu anderen – einschließlich justiziellen – Zwecken als denjenigen, die durch die vorliegende Richtlinie abgedeckt werden“, eröffnet werden könne. Allerdings entfalten die Erwägungsgründe keine Rechtskraft und können lediglich zur Auslegung herangezogen werden. Einer Auslegung des Art. 15 Abs. 1a RiL 2002/58/EG steht dessen eindeutiger Wortlaut entgegen. Im Übrigen stellt die Verfolgung mittlerer und leichter Straftaten sowie von Ordnungswidrigkeiten keinen „anderen Zweck“ dar als die Verfolgung schwerer Strafta-

68 Ratsdokument 5777/06 ADD 1 REV 1 vom 17.02.2006, http://register.consilium.europa.eu/pdf/de/06/st05/st05777-ad01re01.de06.pdf.

69 Pressemitteilung vom 21.02.2006, http://www.bmj.bund.de.

70 Vgl. S. 115 der Entwurfbegründung: „nur bei schweren Straftaten i. S. v. § 100a Abs. 1 Nr. 2, Abs. 2 StPO-E“.

71 Art. 15 Abs. 1 S. 1 lautet: „Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für die nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist.“

ten. Die repressive Verfolgung rechtswidriger Taten ist als einheitlicher Zweck anzusehen, weil die Beschränkung der Vorratsspeicherungsrichtlinie auf schwere Straftaten ansonsten jegliche Bedeutung verlöre.

Die Bundesregierung weist zwar zurecht darauf hin, dass der Richtliniengeber die Definition des Begriffs der „schweren Straftaten" in das Ermessen der Mitgliedsstaaten gestellt hat. Der deutsche Gesetzgeber überschreitet aber dieses Ermessen, wenn er bereits „erhebliche" Straftaten, jegliche mittels Telekommunikation begangene Straftaten und – im Bereich vorratsgespeicherter Bestandsdaten – gar Ordnungswidrigkeiten genügen lasst, um die Abfrage anlasslos gespeicherter Vorratsdaten zu rechtfertigen. Zudem hat das Bundesverfassungsgericht in seiner Entscheidung zum Europäischen Haftbefehl deutlich gemacht, dass der deutsche Gesetzgeber Umsetzungsspielräume möglichst grundrechtsfreundlich nutzen muss.[72] Dem wird § 100g StPO nicht annähernd gerecht.

Falls die Richtlinie zur Vorratsdatenspeicherung überhaupt umgesetzt wird, fordern wir, den Zugriff auf vorratsgespeicherte Verkehrs- und Bestandsdaten auf die Verfolgung schwerer Straftaten zu beschränken,[73] wie es die Richtlinie vorsieht. Als schwere Straftaten sind Fälle organisierter oder gewerbsmäßiger Kriminalität anzusehen, in denen eine höhere Strafe als vier Jahre Freiheitsstrafe zu erwarten ist.

2. Fehlende Bestimmung der maßgeblichen Straftaten

Ferner versäumen es § 100g StPO und die §§ 112, 113 TKG, die Straftaten zu „bestimmen", zu deren Verfolgung der Datenzugriff zulässig sein soll, wie es Art. 1 Abs. 1 der Vorratsspeicherungsrichtlinie verlangt. Eine katalogartige Aufzählung der Straftatbestände wie in § 100a StPO wird zwar nicht unbedingt erforderlich sein, aber doch eine Umschreibung, anhand derer sich eindeutig und unzweifelhaft die Straftaten bestimmen lassen, deren Aufklärung einen Datenzugriff rechtfertigt. Dies kann etwa auch durch Bezugnahme auf den Strafrahmen oder die Straferwartung geschehen.

Dass die allgemeine Umschreibung in § 100g StPO, welche die Bestimmung der „erheblichen Straftaten" letztlich der Rechtsprechung überlässt, nicht ausreicht, ergibt sich auch aus dem deutschen Verfassungsrecht. Der aus den Grundrechten folgende Parlamentsvorbehalt fordert eine eindeutige Bestimmung der maßgeblichen Straftaten durch den Bundestag selbst, zumal bei einem so schwerwiegenden Eingriff wie einer systematischen und anlasslosen Vorratsspeicherung von Kommunikationsdaten.

Wir fordern eine klare Umschreibung der maßgeblichen Straftaten durch Bezugnahme auf die jeweils zu erwartende Strafe.

3. Unzureichende Eingriffsschwelle

Die in § 100g StPO-E vorgesehene Eingriffsschwelle ist zu niedrig. Der Zugriff auf Verkehrsdaten muss den gleichen Voraussetzungen unterliegen wie der Zugriff auf Inhalte der Telekommunikation (§ 100a StPO). Entsprechende Regelungen finden sich in etlichen anderen europäischen Ländern.

Aus den deutschen Grundrechten und dem Verhältnismäßigkeitsgebot ist abzuleiten, dass in die Vertraulichkeit der Telekommunikation nur ausnahmsweise zur Abwehr schwerer Gefahren und zur Verfolgung schwerer Straftaten eingegriffen werden darf. Dies gilt für Kommunikationsinhalte, Kommunikationsumstände und Kommunikationsbeteiligte gleichermaßen, denn die technische Differenzierung in Inhalts-, Verkehrs- und Bestandsdaten ist ohne Bedeutung für Nutzbarkeit und Verwendungsmöglichkeiten. Gera-

72 BVerfGE 113, 273, Rn. 80: „Der Gesetzgeber war jedenfalls verpflichtet, die Umsetzungsspielräume, die der Rahmenbeschluss den Mitgliedstaaten belässt, in einer grundrechtsschonenden Weise auszufüllen."

73 Ähnlich Gola/Klug/Reif, NJW 2007, 2599 (2602): Beschränkung auf die Verfolgung der in § 139 Abs. 3 StGB genannten Straftaten. Vgl. auch Bundesrechtsanwaltskammer, Stellungnahme vom August 2007, http://brak.de/seiten/pdf/Stellungnahmen/2007/Stn31.pdf, 34: „Sofern eine verdachts- und anlassunabhängige Vorratsdatenspeicherung überhaupt verfassungsgemäß ist, wäre für die Erhebung solcher Daten zur Strafverfolgung die gleiche Schwelle wie für die Erhebung von Inhaltsdaten zu fordern."

de die jeweiligen Nutzungs- und Verwendungsmöglichkeiten bestimmen nach der Rechtsprechung des Bundesverfassungsgerichts die Schutzwürdigkeit eines Datums.[74]

Die verbreitete Annahme, der staatliche Zugriff auf die näheren Umstände der Telekommunikation wiege weniger schwer als der Zugriff auf Telekommunikationsinhalte, ist unzutreffend.[75] Im Vergleich zu Inhaltsdaten sind die Verarbeitungsmöglichkeiten von Verkehrsdaten weit höher. Verkehrsdaten können automatisch analysiert, mit anderen Datenbeständen verknüpft und auf bestimmte Suchmuster hin durchkämmt sowie nach bestimmten Kriterien geordnet und ausgewertet werden. Diese Möglichkeiten bestehen bei Inhaltsdaten nicht. Während die Strafverfolgungsbehörden oftmals nur oder jedenfalls zunächst nur an Verkehrsdaten interessiert sind, kommt der umgekehrte Fall praktisch nicht vor. Das Bundesverfassungsgericht betonte vor einigen Monaten:

> *„Immer mehr Lebensbereiche werden von modernen Kommunikationsmitteln gestaltet. Damit erhöht sich nicht nur die Menge der anfallenden Verbindungsdaten, sondern auch deren Aussagegehalt. Sie lassen in zunehmendem Maße Rückschlüsse auf Art und Intensität von Beziehungen, auf Interessen, Gewohnheiten und Neigungen und nicht zuletzt auch auf den jeweiligen Kommunikationsinhalt zu und vermitteln – je nach Art und Umfang der angefallenen Daten – Erkenntnisse, die an die Qualität eines Persönlichkeitsprofils heranreichen können.“*[76]

Ein Grundsatz, wonach Verkehrsdaten typischerweise weniger schutzbedürftig seien als Inhaltsdaten, lässt sich somit nicht aufstellen; ein unterschiedliches Schutzniveau für Inhaltsdaten einerseits und Verkehrsdaten andererseits ist nicht gerechtfertigt.

Wir fordern, den staatlichen Zugriff auf Informationen über die Kommunikation und die Kommunizierenden („Verkehrsdaten“, „Bestandsdaten“) den gleichen Voraussetzungen zu unterwerfen wie den Zugriff auf die Inhalte der Kommunikation.[77] Der Zugriff zwecks Strafverfolgung sollte dabei beschränkt sein auf Fälle organisierter oder gewerbsmäßiger Kriminalität, in denen eine höhere Strafe als vier Jahre Freiheitsstrafe zu erwarten ist.

4. Bewegungsprofile bei betriebsbereiten Mobiltelefonen

Die Ausweitung des § 100g StPO auf Verkehrsdaten eines nur betriebsbereiten Mobiltelefons wird strikt abgelehnt.

§ 100g Abs. 3 StPO erlaubt den Zugriff auf Verkehrsdaten bisher nur „im Falle einer Verbindung“. Insbesondere die Aufzeichnung der Bewegungen von Nutzern eines nur eingeschalteten Handys ist bisher allenfalls unter den Voraussetzungen des § 100a StPO zulässig.

Diese Einschränkung ist in § 100g StPO-E nicht mehr enthalten. Damit würde eine 24-stündige Überwachung des Bewegungsverhaltens schon wegen jedes Verdachts einer „erheblichen“ Straftat erlaubt. Ein derart schwerwiegender Eingriff muss weiterhin mindestens den Voraussetzungen des § 100a StPO unterliegen. Die Erhebung von Verkehrsdaten unter den geringen Voraussetzungen des § 100g StPO-E muss – wenn überhaupt – auf die näheren Umstände tatsächlicher Verbindungen beschränkt bleiben.

Die Bundesregierung hat zu § 100g StPO zutreffend ausgeführt:

> *„Auch gegenwärtig können die Strafverfolgungsbehörden den Aufenthaltsort eines Beschuldigten in der Vergangenheit, beispielsweise zur Tatzeit, nicht durch ein auf § 12 FAG gestütztes Auskunftsverlangen über die Standortkennung eines Mobiltelefons im „Stand by“-Betrieb ermitteln. Dies folgt daraus, dass eine solche Kennung mit jedem Wechsel des eingeschalteten Mobiltelefons in eine neue Funkzelle „über-*

74 BVerfGE 65, 1 (45).

75 Ebenso Bundesrechtsanwaltskammer, Stellungnahme vom August 2007, http://brak.de/seiten/pdf/-Stellungnahmen/2007/Stn31.pdf, 45; näher Breyer, Vorratsspeicherung (2005), www.vorratsspeicherung.de.vu, 211 ff.

76 BVerfG, 2 BvR 2099/04 vom 02.03.2006, NJW 2006, 976 (980), Abs. 91.

77 Ebenso Bundesrechtsanwaltskammer, Stellungnahme vom August 2007, http://brak.de/seiten/pdf/-Stellungnahmen/2007/Stn31.pdf, 45.

schrieben“ und nicht gespeichert wird. Aus diesem Grund ist auch die Erstellung nachträglicher Bewegungsprofile ausgeschlossen. Soweit der Vorschlag des Bundesrates dazu führen soll, dass im Falle einer Auskunftsanordnung über zukünftige Telekommunikation die jeweils gespeicherte Standortkennung des betriebsbereiten Mobiltelefons vor ihrer Löschung mitzuteilen wäre, bedarf es einer solchen Regelung nicht. Diese Informationen, mittels derer sich so genannte Bewegungsprofile erstellen lassen, können die Strafverfolgungsbehörden bereits heute im Rahmen einer Telekommunikationsüberwachung nach den §§ 100a, 100b StPO erlangen. Die insoweit erhöhten Anordnungsvoraussetzungen rechtfertigen sich aus der Eingriffsintensität der Maßnahme.“[78]

Falls § 100g StPO neben § 100a StPO überhaupt beibehalten wird, fordern wir, diesen weiterhin auf die im Falle einer Verbindung anfallenden Verkehrsdaten zu beschränken.

5. Erweiterung in Datenerhebungsbefugnis

Die Ausweitung des § 100g StPO von einem Auskunftsanspruch in eine Datenerhebungsbefugnis wird abgelehnt.

§ 100g StPO erlaubt bisher nur die Erhebung von Verkehrsdaten, die bei einem Anbieter ohnehin zu geschäftlichen Zwecken gespeichert sind. Auch soweit Auskunft über künftige Verkehrsdaten verlangt werden kann, gilt dies ausweislich der Gesetzesbegründung nur für solche Daten, die der Anbieter im Zuge der Bereitstellung und Abrechnung des Dienstes ohnehin speichert. Die Erhebung weiterer Verkehrsdaten, auch in Echtzeit, ist bisher nur unter den Voraussetzungen des § 100a StPO zulässig. Die Begründung des Regierungsentwurfs räumt ein, dass diese Gesetzeslage auch unter Berücksichtigung der Cybercrime-Konvention beibehalten werden kann (S. 57 und 112).

Die Bundesregierung hat zu § 100g StPO zutreffend ausgeführt:

„Ebenso wie bei der Auskunft über Verbindungsdaten aus der Vergangenheit soll auch bei einer Anordnung der Auskunft über zukünftig anfallende Verbindungsdaten der Auskunftsanspruch auf solche Daten beschränkt bleiben, die seitens der Diensteanbieter aufgrund bestehender Regelungen zulässigerweise erhoben und gespeichert werden. [...] Eine Verpflichtung, auch sonstige Verbindungsdaten aufzuzeichnen, soll mit der Neuregelung demgegenüber nicht begründet werden. Eine solche Verpflichtung ginge sogar über den Regelungsgehalt der Telekommunikationsüberwachung (§§ 100a, 100b StPO) hinaus, da selbst dort die Diensteanbieter gemäß § 100b Abs. 3 StPO nicht zur Aufzeichnung, sondern ausschließlich dazu verpflichtet werden können, die Überwachung und Aufzeichnung der Telekommunikation durch die Strafverfolgungsbehörden zu ermöglichen. Auch zukünftig sollen die Diensteanbieter hinsichtlich solcher Verbindungsdaten, die sie nach dem Telekommunikationsrecht nicht erheben und speichern dürfen, lediglich zur Ermöglichung der Überwachung und Aufzeichnung unter den Voraussetzungen der §§ 100a, 100b StPO verpflichtet bleiben.“[79]

§ 100g StPO-E soll demgegenüber künftig auch für nicht zu Geschäftszwecken gespeicherte Daten gelten mit der Folge, dass deren Erhebung nicht nur bei dem Verdacht schwerer Straftaten, sondern bereits bei Ermittlungen wegen „erheblicher“ oder jeglicher mittels Telekommunikation begangener Straftat zulässig wäre. Dies widerspricht der bewussten Entscheidung des Gesetzgebers, die in § 100g StPO vorgesehene niedrige Eingriffsschwelle eben nicht für die Erhebung weiterer Verkehrsdaten genügen zu lassen.

Der Regierungsentwurf begründet diese beabsichtigte Änderung allein mit einer Angleichung an § 100a StPO, also im Grunde mit einer Vereinfachung des Wortlauts. Solche Gesichtspunkte rechtfertigen aber offensichtlich keine derart schwerwiegende Herabsetzung der Eingriffschwelle.

Falls § 100g StPO überhaupt beibehalten wird, fordern wir, dass die Vorschrift weiterhin auf Verkehrsdaten beschränkt bleibt, die der Anbieter ohnehin im Zuge der Bereitstellung und Abrechnung des Dienstes speichert.

78 BT-Drs. 14/7258, 4.

79 BT-Drs. 14/7258, 4.

6. Ausweitung auf inhaltsbezogene Verkehrsdaten

Die Ausweitung des § 100g StPO auf „sonstige [...] Verkehrsdaten“ (§ 96 Abs. 1 Nr. 5 TKG) wird strikt abgelehnt.

§ 100g Abs. 3 StPO enthält bisher eine abschließende Definition der Verkehrsdaten, auf die unter den niedrigen Voraussetzungen des § 100g StPO zugegriffen werden darf. Auf andere Verkehrsdaten darf bisher nur nach Maßgabe des § 100a StPO zugegriffen werden. Unter § 100a StPO fallen insbesondere Verkehrsdaten, die genauen Aufschluss über den Inhalt der Telekommunikationsvorgänge zulassen. Unter anderem sind zu nennen die genaue Bezeichnung (URL) aufgerufener Internetseiten einschließlich Nutzereingaben (z.B. in Suchmaschinen eingegebene Suchwörter) sowie die Kennziffer von Newsgroup-Nachrichten (posted message ID). Diese Daten enthalten Kommunikationsinhalte (Nutzereingaben) oder ermöglichen jedenfalls den Abruf des Kommunikationsinhalts. Die Erhebung solcher Verkehrsdaten darf nicht bereits bei dem Verdacht einer „erheblichen“ oder jeglicher mittels Telekommunikation begangener Straftat zulässig sein. Auch der Regierungsentwurf nennt keine praxisrelevanten Beispiele „sonstiger Verkehrsdaten“, für welche die Eingriffsvoraussetzungen des § 100g StPO-E angemessen wären (S. 115).

Wir fordern, die niedrigere Eingriffsschwelle des § 100g StPO – wenn überhaupt – weiterhin nur für die in § 100g Abs. 3 StPO abschließend bestimmten Verkehrsdaten beizubehalten.

7. Fehlende Erfolgskontrolle

Die Erfolgskontrolle nach § 100b Abs. 4 S. 2 StPO-E muss auch für den Zugriff auf die näheren Umstände der Telekommunikation gelten. Deren Vertraulichkeit ist nicht minder schutzwürdig als die Vertraulichkeit der Kommunikationsinhalte.

Die Rückmeldungen analog § 100b Abs. 4 S. 2 StPO-E müssen auch in die Statistik nach § 100g Abs. 4 StPO-E einfließen. Die laut Entwurf in die Statistik aufzunehmenden Angaben lassen keinen Rückschluss auf die Effektivität der Maßnahmen zu. Entsprechende Kenntnisse braucht der Bundestag aber, um die Verhältnismäßigkeit der Norm überprüfen zu können. Eine solche Überprüfung ist verfassungsrechtlich geboten; gerade zu diesem Zweck ist die Geltungsdauer der §§ 100g, 100h StPO befristet worden. Auch § 100b Abs. 6 Nrn. 5 und 6 StPO in der Fassung des Referentenentwurfs sah die Erhebung von Daten über das Ergebnis der Zugriffe vor. Diese Erhebung muss ebenso für den Zugriff auf die näheren Umstände der Telekommunikation nach § 100g StPO erfolgen.

8. Verkehrsdaten über Unbeteiligte

Nach § 100g Abs. 1 S. 2 StPO darf Auskunft über Verkehrsdaten nur erteilt werden, „soweit diese Verbindungsdaten den Beschuldigten oder die sonstigen in § 100a Satz 2 bezeichneten Personen betreffen.“ Die geplante Neufassung enthält eine entsprechende Einschränkung nicht. Der geplante Verweis auf § 100a Abs. 3 StPO-E ist zu unbestimmt. § 100a Abs. 3 StPO-E regelt nur, gegen wen sich die Anordnung richten darf, nicht aber, wessen Verkehrsdaten erhoben werden dürfen.

§ 100g Abs. 1 S. 2 StPO muss daher beibehalten werden.

IV. § 101 StPO-E [Allgemeine Verfahrensregelungen bei verdeckten Ermittlungsmaßnahmen]

1. Benachrichtigung der von Telekommunikationsüberwachung Betroffenen

Wir fordern die Sicherstellung der Benachrichtigung der Betroffenen durch Aufnahme einer Regelung der folgenden Art:

„Auf Ersuchen der Staatsanwaltschaft veranlasst die Bundesnetzagentur die Benachrichtigung der Inhaber von Telekommunikationsanschlüssen. In dem Ersuchen der Staatsanwaltschaft sind die Kennungen der betroffenen Anschlüsse anzugeben. Auf Verlangen der Bundesnetzagentur sind Diensteanbieter im Sinne des § 100b der Strafprozessordnung verpflichtet, ihren Kunden eine Benachrichtigung zu übermitteln. Den Diensteanbietern sind die hierzu erforderlichen Aufwendungen nach Maßgabe des Justizver-

gütungs- und -entschädigungsgesetzes zu erstatten. Zur Ermittlung der Diensteanbieter der zu benachrichtigenden Personen darf die Bundesnetzagentur das automatisierte Auskunftsverfahren nach § 112 TKG nutzen.“

Benachrichtigungen bereiten heutzutage keinen nennenswerten Aufwand mehr, wenn man die technischen Möglichkeiten einsetzt, die man sich auch für die Telekommunikationsüberwachung selbst zunutze macht. Möglich ist erstens eine Benachrichtigung an den überwachten Anschluss selbst (per SMS, E-Mail, Telefonautomat). Möglich ist zweitens eine Benachrichtigung in der Telefonrechnung. Diese Möglichkeiten machen auch Massenbenachrichtigungen praktikabel, gerade, wenn das Verfahren automatisiert wird.

Sinnvoll erscheint die folgende Vorgehensweise: Die Staatsanwaltschaft übermittelt der Bundesnetzagentur eine Liste der betroffenen Anschlüsse, deren Inhaber zu benachrichtigen sind. Dies verursacht keinen erheblichen Aufwand, da derartige Listen der Staatsanwaltschaft aufgrund der Überwachungsmaßnahme bereits vorliegen. Die Bundesnetzagentur nimmt sodann die Benachrichtigung entweder selbst vor (per Brief, SMS, E-Mail oder Telefonautomat) oder ersucht den jeweiligen Diensteanbieter, die Benachrichtigung in die nächste Rechnung aufzunehmen. Dies kann automatisiert erfolgen und verursacht ebenfalls keinen erheblichen Aufwand. Die Diensteanbieter der Betroffenen können im Wege des automatisierten Auskunftsverfahren nach § 112 TKG ermittelt werden, auf das die Bundesnetzagentur ohnehin Zugriff hat. Es darf nicht bei dem bisherigen Missstand bleiben, dass die Staatsanwaltschaften wegen des damit verbundenen Aufwands regelmäßig von einer Benachrichtigung absehen.

Daneben fordern wir eine Pflicht zur Benachrichtigung der Betroffenen auch von Auskünften über ihre Bestandsdaten (§§ 112, 113 TKG, Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums).

In die falsche Richtung gehen die vielfältigen Einschränkungen der Benachrichtigungspflicht in § 101 StPO-E. Während der Gesetzentwurf den Anspruch hat, den Rechtsschutz der Betroffenen zu stärken, tut er in Wahrheit das Gegenteil. § 101 StPO sieht in der geltenden Fassung einen einschränkungslosen Anspruch auf Benachrichtigung vor, wie er auch verfassungsrechtlich vorgegeben ist.

Der Gesetzentwurf will dagegen Ausnahmen zulassen, wenn die betroffene Person „von der Maßnahme nur unerheblich betroffen wurde und anzunehmen ist, dass sie kein Interesse an einer Benachrichtigung hat“ (§ 101 Abs. 4 S. 4 StPO-E). Tatsächlich sind die von verdeckter staatlicher Informationserhebung Betroffenen immer gravierend betroffen und haben stets ein verfassungsrechtlich geschütztes Interesse an einer Benachrichtigung. Falsch ist die in der Begründung aufgestellte Behauptung, bei Verkehrsdatenerhebungen fehle es regelmäßig an einem Interesse der Betroffenen, von der Überwachung ihres Kommunikationsverhaltens zu erfahren (S. 136). Zur Stützung dieser Behauptung werden keinerlei empirische Anhaltspunkte angeführt. Eine empirische Auswertung würde vielmehr ergeben, dass die meisten Menschen sehr wohl erfahren möchten, wann ihr Kommunikationsverhalten ohne ihr Wissen ermittelt worden ist und zu welchem Zweck.

Weiter soll die Ermittlung der Betroffenen als Voraussetzung ihrer Benachrichtigung nur in bestimmten Fällen erforderlich sein (§ 101 Abs. 4 S. 5 StPO-E). Diese Einschränkung steht mit den verfassungsrechtlichen Vorgaben nicht im Einklang. Vielmehr besteht nach der Rechtsprechung des Bundesverfassungsgerichts grundsätzlich ein Anspruch auf Benachrichtigung. Dieser kann nur im Wege der Abwägung zurücktreten. Der durch die Benachrichtigung verursachte Arbeitsaufwand hat ohne Einfluss auf den Benachrichtigungsanspruch zu sein. Der Benachrichtigungsaufwand lässt sich nicht von dem Aufwand für die Durchführung der Überwachungsmaßnahme selbst trennen. Oben sind praktikable und einfache Möglichkeiten der elektronischen Benachrichtigung aufgezeigt worden.

Wir fordern die Streichung des § 101 Abs. 4 S. 4 und 5 StPO und die Sicherstellung der Benachrichtigung der Betroffenen durch Aufnahme einer Regelung über elektronische Benachrichtigungen.

2. Frist zur gerichtlichen Überprüfung

Die in § 101 Abs. 9 StPO-E vorgesehene Frist von zwei Wochen, innerhalb derer die gerichtliche Überprüfung einer verdeckten Ermittlungsmaßnahme beantragt werden kann, ist zu kurz.

Ein Antrag auf Überprüfung der Rechtmäßigkeit der Maßnahme oder der Art und Weise ihres Vollzugs kann sinnvollerweise erst gestellt werden, wenn der Betroffene über die Maßnahme und die Art und Weise ihres Vollzugs informiert ist. Die Benachrichtigung nach § 101 StPO-E enthält darüber keine ausreichenden Angaben. Der Betroffene muss regelmäßig erst einen Anwalt beauftragen und Akteneinsicht beantragen, bevor er über einen Antrag auf gerichtliche Überprüfung entscheiden kann. Bis die beantragte Akteneinsicht gewährt wird, wird lange Zeit vergehen, falls mehrere Benachrichtigte gleichzeitig die Akte einsehen wollen. Die Zweiwochenfrist gewährleistet daher keinen effektiven Rechtsschutz. Sie führt auch zu einer übermäßigen Beanspruchung der Gerichte, weil Betroffene rein vorsorglich einen Antrag auf Überprüfung stellen werden, um sich diese Möglichkeit offen zu halten. Der bisher analog angewandte § 98 StPO sieht ebenfalls keine Frist vor.

Die Entwurfsbegründung führt an, die Befristung stelle sicher, dass die erhobenen Daten zeitnah gelöscht werden könnten (S. 129). Dies lässt sich aber bereits dadurch gewährleisten, dass dem Betroffenen mitgeteilt wird, wann die Daten gelöscht werden sollen. Erwägt der Betroffene das Beschreiten des Rechtswegs, so kann er dies der Behörde rechtzeitig mitteilen und dadurch eine Löschung verhindern. Eine Befristung des Rechtsbehelfs ist dazu nicht erforderlich und – trotz vergleichbarer Problematik – auch in § 98 StPO nicht vorgesehen. Im Übrigen ist Voraussetzung einer gerichtlichen Prüfung keineswegs immer, dass die erhobenen Daten noch vorliegen. Oft wird lediglich in Frage stehen, ob die Anordnung der Maßnahme rechtmäßig war. Die Ergebnisse der Maßnahme sind dann ohne Bedeutung. Schließlich wäre zumindest eine Verlängerung der Frist zur gerichtlichen Überprüfung etwa auf drei Monate möglich.

Wir fordern die Streichung der vorgesehenen Zweiwochenfrist.

3. Folgen rechtswidriger Ermittlungsmaßnahmen

Der Gesetzesentwurf regelt die Folgen rechtswidriger Ermittlungsmaßnahmen nicht.

Die Rechtsprechung entscheidet über die Folgen rechtswidriger Ermittlungsmaßnahmen bisher im Wege einer Abwägung. Ein Verwertungsverbot nimmt sie nur an, wenn das Gewicht der Rechte des Betroffenen das staatliche Strafverfolgungsinteresse überwiegt. Bei verdeckten Ermittlungsmaßnahmen ist demgegenüber zu beachten, dass es sich um schwerwiegende Grundrechtseingriffe handelt. Hier wird ohne das Wissen der Betroffenen in deren Privatsphäre eingedrungen. Die Begründung des vorliegenden Gesetzesentwurfs führt zu § 100a StPO zutreffend aus, dass von den Gerichten „weitergehende Ermittlungen nur in den Fällen für zulässig gehalten werden, in denen die Maßnahme nach § 100a StPO rechtmäßig war“ (S. 148). Dasselbe gilt für andere verdeckte Ermittlungsmaßnahmen.

Wir fordern eine Pflicht zur sofortigen Vernichtung sowie ein Verwertungsverbot für Informationen, die durch rechtswidrige verdeckte Ermittlungsmaßnahmen erlangt worden sind. Ferner fordern wir die Aufnahme eines ausdrücklichen Anspruchs der von rechtswidrigen Ermittlungsmaßnahmen Betroffenen auf angemessene Entschädigung.

V. § 110 StPO-E [Durchsicht von Papieren]

Nach § 110 Abs. 3 StPO-E soll sich die Durchsuchung von Festplatten, DVDs usw. künftig auf weitere Medien erstrecken dürfen, zu denen der Betroffene zugangsberechtigt ist. Die Regelung soll der Umsetzung der Cybercrime-Konvention (CCC) des Europarats dienen.

Diese regelt in Art. 19 Abs. 2: „*Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um sicherzustellen, dass ihre Behörden, wenn sie ein bestimmtes Computersystem oder einen Teil davon nach Absatz 1 Buchstabe a durchsuchen oder in ähnlicher Weise darauf Zugriff nehmen und Grund zu der Annahme haben, dass die gesuchten Daten in einem anderen Computersystem oder einem Teil davon im Hoheitsgebiet der betreffenden Vertragspartei gespeichert sind, und diese Daten von dem ersten System aus rechtmäßig zugänglich oder verfügbar sind, die Durchsuchung oder den ähnlichen Zugriff rasch auf das andere System ausdehnen können.*“

§ 110 Abs. 3 StPO-E ist erstens zu unbestimmt und geht zweitens erheblich über Art. 19 Abs. 2 CCC hinaus.[80]

Unbestimmt ist die Regelung, soweit von „Betroffenen" die Rede ist.[81] Hier muss klargestellt werden, dass es sich um die Person handelt, gegen die sich die Durchsuchungsanordnung richtet. Ferner ist klarzustellen, dass die Erstreckung der Durchsuchung auf andere Systeme eine besonderen Anordnung bedarf, über die im Regelfall der Richter entscheidet.[82]

Über die Konvention hinaus geht § 110 Abs. 3 StPO-E in mehrfacher Hinsicht.[83] Art. 19 Abs. 2 CCC gilt nur in einer bestimmten Situation, nämlich wenn die Strafverfolgungsbehörden ein Computersystem durchsuchen und dabei feststellen, dass die gesuchten Daten auf einem anderen Computersystem gespeichert sind. Die Regelung gilt damit erstens nur für Fälle, in denen die Strafverfolgungsbehörde nach bestimmten Daten sucht. Diese Einschränkungen sucht man in § 110 Abs. 3 StPO-E vergeblich. § 110 Abs. 3 StPO-E soll zweitens für alle „elektronischen Speichermedien" gelten und nicht nur für „Computersysteme". Die Ermächtigung würde also beispielsweise auch Audio-CDs abdecken. § 110 Abs. 3 StPO-E soll drittens allgemein und nicht nur dann gelten, wenn die Behörden vergeblich nach bestimmten Daten gesucht haben. Schließlich erlaubt Art. 19 Abs. 2 CCC viertens nur die Durchsuchung von Datenbeständen, die „von dem ersten System aus rechtmäßig zugänglich" sind. Hieran wird deutlich, dass etwa die Durchsuchung externer Speichermedien keinen Zugriff auf weitere Systeme erlaubt.

Unzutreffend ist die Annahme, eine Online-Durchsuchung sei weniger eingriffsintensiv als die Beschlagnahme von Datenträgern (S. 145 f.). Richtig ist, dass eine Online-Durchsuchung in Abwesenheit und ohne das Wissen des Betroffenen erfolgen kann, so dass es sich um die eingriffsintensivere Ermittlungsmaßnahme handelt.[84]

Wir fordern eine normenklare und vor allem nicht überschießende Umsetzung der Cybercrime-Konvention in § 110 Abs. 3 StPO-E.[85]

VI. § 96 TKG-E [Verkehrsdaten]

Wir fordern, die ursprüngliche Fassung des § 96 Abs. 2 S. 1 TKG wieder herzustellen.[86]

§ 96 Abs. 2 S. 1 TKG lautete bis Herbst 2006: „*Die gespeicherten Verkehrsdaten dürfen über das Ende der Verbindung hinaus nur verwendet werden, soweit sie zum Aufbau weiterer Verbindungen oder für die in den §§ 97, 99, 100 und 101 genannten Zwecke erforderlich sind.*" Diese Vorschrift lautet aufgrund des Gesetzes zur Änderung telekommunikationsrechtlicher Vorschriften nun wie folgt: „*Die gespeicherten Verkehrsdaten dürfen über das Ende der Verbindung hinaus nur verwendet werden, soweit sie zum Aufbau weiterer Verbindungen oder für die in den §§ 97, 99, 100 und 101 genannten oder für die durch andere gesetzliche Vorschriften begründeten Zwecke erforderlich sind.*" Zur Begründung ist angeführt worden, die bisherige Formulierung führe „*zu dem nicht beabsichtigten Rückschluss, dass die Daten nicht für die durch die §§ 100g, 100h StPO, § 8 Abs. 8 und 10 BVerfSchG, § 10 Abs. 3 MAD-Gesetz und*

80 Ebenso Deutscher Anwaltverein, Stellungnahme vom August 2007, http://www.anwaltverein.de/03/05/2007/-41-07.pdf, 25 ff.

81 Ebenso Deutscher Anwaltverein, Stellungnahme vom August 2007, http://www.anwaltverein.de/03/05/2007/-41-07.pdf, 27.

82 Ebenso Deutscher Anwaltverein, Stellungnahme vom August 2007, http://www.anwaltverein.de/03/05/2007/-41-07.pdf, 28.

83 Ebenso Deutscher Anwaltverein, Stellungnahme vom August 2007, http://www.anwaltverein.de/03/05/2007/-41-07.pdf, 26.

84 Bundesgerichtshof, StB 18/06 vom 31.01.2007.

85 Ebenso Deutscher Anwaltverein, Stellungnahme vom August 2007, http://www.anwaltverein.de/03/05/2007/-41-07.pdf, 31 f.

86 Ebenso Gola/Klug/Reif, NJW 2007, 2599 (2601).

§ 8 Abs. 3a BND-Gesetz sowie durch Landesrecht geregelte Erteilung von Auskünften über Verkehrsdaten an die Strafverfolgungs- und Sicherheitsbehörden verwendet werden dürften."

So legitim das Anliegen ist, diese Frage klarzustellen, so ungeeignet und gefährlich ist die erfolgte Umformulierung. Es ist vollkommen unklar und unbestimmt, was „durch andere gesetzliche Vorschriften begründete Zwecke" sein sollen. Diese Formulierung erlaubt die Auslegung, dass jegliche gesetzliche Auskunfts- oder Übermittlungsregelungen auch auf Telekommunikationsdaten Anwendung finden. Dies darf aber mitnichten der Fall sein, weil Verkehrsdaten dem Fernmeldegeheimnis unterliegen. § 88 Abs. 3 TKG erlaubt eine Verwendung zu anderen Zwecken deshalb nur, „soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht."

Auch erlaubt es die gewählte Formulierung undifferenziert, Daten zu spezialgesetzlichen Zwecken zu „verwenden", also auch etwa zu speichern. Dies würde die Interpretation erlauben, dass Daten, die an sich zu löschen wären, für den Fall auf Vorrat gespeichert werden dürfen, dass sie irgendwann einmal für „durch andere gesetzliche Vorschriften begründete Zwecke erforderlich sind". Schließlich steht mit der Entscheidung des Bundesverfassungsgerichts zum automatisierten Kontenabruf[87] nicht im Einklang, dass der Kreis der zugriffsberechtigten Behörden nicht bestimmt ist.[88]

§ 96 Abs. 2 TKG sollte stattdessen in seiner ursprünglichen Fassung wieder hergestellt oder aber wie folgt neu gefasst werden: „*Die gespeicherten Verkehrsdaten dürfen über das Ende der Verbindung hinaus nur verwendet werden, soweit sie zum Aufbau weiterer Verbindungen oder für die in den §§ 97, 99, 100 und 101 genannten Zwecke erforderlich sind. Im Übrigen sind Verkehrsdaten vom Diensteanbieter nach Beendigung der Verbindung unverzüglich zu löschen. Vorschriften in anderen Gesetzen, die sich ausdrücklich auf Telekommunikationsvorgänge beziehen, bleiben unberührt.*"

Mit dieser Formulierung wird ohne Weiteres das Ziel erreicht, klarzustellen, dass spezialgesetzliche Vorschriften unberührt bleiben. Gleichzeitig wird die Übereinstimmung mit § 88 Abs. 3 TKG gewährleistet und sichergestellt, dass Verkehrsdaten nur insoweit zu anderen Zwecken gespeichert oder übermittelt werden, wie es spezialgesetzlich auch vorgesehen ist.

VII. § 110 TKG-E [Umsetzung von Überwachungsmaßnahmen, Erteilung von Auskünften]

§ 110 TKG-E soll die Exekutive ermächtigen, künftig auch die „Erteilung von Auskünften" zu normieren und zu standardisieren. Die vorgesehene Ermächtigung beschränkt sich nicht auf die Erhebung von Verkehrsdaten in Echtzeit, wie die Begründung suggeriert (S. 169). Vielmehr kann damit jede Auskunft über Verkehrsdaten oder Bestandsdaten (§ 113 TKG) normiert und standardisiert werden.

§ 110 TKG-E ist zu unbestimmt, weil er nicht angibt, welche Auskünfte gemeint sind. Er ist ferner inhaltlich abzulehnen, weil die Standardisierung von Auskünften sogenanntes „Data Mining" in weitem Umfang ermöglicht und erleichtert. Der Bundesrat fordert in Ziff. 16 seiner Stellungnahme bereits „ein einheitliches Dateiformat und eine einheitliche Schnittstelle" für die „Anlieferung der Verkehrsdaten" durch die Diensteanbieter. Im Ausland stellen Behörden bereits heute Telekommunikations-Verkehrsdaten in große Datenbanken ein („Datawarehouse"), um sie automatisiert analysieren zu können. Kommerziell erhältliche Software etwa der Firma „Harlequin" ermöglicht es, verfahrensübergreifend Kommunikationsdaten auf vermeintliche Verbindungen oder Auffälligkeiten zu analysieren sowie Kommunikationsnetzwerke grafisch offenzulegen. Diese Verfahren entfernen sich von dem rechtsstaatlichen Leitbild einer gezielten Ermittlung in konkreten Verfahren mit anschließender Löschung der nicht mehr benötigten Daten. Sie führen in Richtung der amerikanischen Praxis, gigantische Datenbanken mit personenbezogenen Daten über Jahrzehnte hinweg aufzubauen, um sie automatisiert durchsuchen und Ver-

87 BVerfG NJW 2007, 2464.

88 Gola/Klug/Reif, NJW 2007, 2599 (2601).

dachtsmomente schöpfen zu können. Gerade Telekommunikationsdaten betreffen überwiegend unverdächtige Personen, nämlich unbeteiligte Gesprächspartner.

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

Wir fordern, die vorgesehene Ausweitung des § 110 TKG zu streichen.

VIII. § 111 TKG-E [Daten für Auskunftsersuchen der Sicherheitsbehörden]

1. Identifizierungspflicht für Telefon, Handy und Internet (§ 111 Abs. 1 TKG)

§ 111 Abs. 1 TKG zufolge setzt die Nutzung eines Telefon- oder Handyanschlusses sowie künftig auch von Internetanschlüssen zwingend die Angabe von Name, Anschrift und Geburtsdatum voraus, und zwar selbst dann, wenn die Erhebung von Kundendaten zu betrieblichen Zwecken nicht erforderlich ist (z.B. bei vorausbezahlten Mobiltelefonkarten oder kostenlosen Internettelefonie-Diensten).

Das Grundgesetz lässt solche Grundrechtseingriffe nur aus überwiegenden Interessen der Allgemeinheit zu. Hiervon kann bei der Identifizierungspflicht für Telefon, Handy und Internet keine Rede sein. Es ist unverhältnismäßig, die anonyme Inanspruchnahme der Telekommunikation für die gesamte Bevölkerung zu verbieten, obwohl diese Möglichkeit nur in einem Bruchteil aller Fälle missbraucht wird. Wenn Menschen aus Furcht vor sozialer Stigmatisierung, vor Nachteilen am Arbeitsplatz, vor Strafverfolgungsmaßnahmen oder vor geheimdienstlicher Beobachtung auf Kommunikation mit anderen verzichten, schadet dies nicht nur ihnen, sondern der demokratischen Gesellschaft insgesamt. Die demokratische Gemeinschaft ist darauf angewiesen, dass die Bürgerinnen und Bürger unbefangen von ihren Grundrechten Gebrauch machen. Die vielfältigen Möglichkeiten zur Umgehung der Bestandsdatenerhebung, angefangen mit dem Tausch vorausbezahlter Telefonkarten, lassen den vermeintlichen Nutzen der Regelung weiter hinter den mit ihr verbundenen Schaden zurücktreten. Das Gewicht des Eingriffs vergrößert sich ferner durch die ausufernden gesetzlichen Zugriffsrechte (§§ 112, 113 TKG), zu denen in Kürze noch ein zivilrechtlicher Auskunftsanspruch wegen Urheberrechtsverletzungen hinzu treten soll.[89]

Eine Verfassungsbeschwerde gegen § 111 TKG ist anhängig (1 BvR 1299/05). Zu Recht wird darin gerügt, dass § 111 TKG unverhältnismäßig in das Fernmeldegeheimnis und in das Grundrecht auf informationelle Selbstbestimmung eingreift. Eine solche verdachtslose und systematische „Vorratsdatenerhebung" ist ebenso unverhältnismäßig wie eine Vorratsdatenspeicherung.

§ 111 TKG findet auch in der Richtlinie über die Vorratsdatenspeicherung keine Entsprechung. Die Richtlinie sieht eine Pflicht zur Erhebung von Bestandsdaten nicht vor, sondern nur Mindestspeicherfristen für ohnehin von den Anbietern erhobene Daten. In Art. 3 Abs. 1 der Richtlinie heißt es, „dass die in Artikel 5 der vorliegenden Richtlinie genannten Daten" nur zu speichern sind, „soweit sie [...] im Zuge der Bereitstellung der betreffenden Kommunikationsdienste von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes erzeugt oder verarbeitet werden". Bei vorausbezahlten oder kostenlosen Diensten fallen dagegen oft keine Bestandsdaten an. Dass die Richtlinie 2006/24/EG die anonyme Bereitstellung von Telekommunikation zulässt, ergibt sich auch aus Art. 5 Abs. 1 Buchst. e Nr. 2 vi, der den Fall „vorbezahlter anonymer Dienste" ausdrücklich regelt.

Wir fordern die Aufhebung des § 111 Abs. 1 TKG.

89 Entwurf eines Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums, BT-Drs. 16/5048.

2. Zwangserhebung auch von Internet-Kundendaten und von Gerätenummern (§ 111 Abs. 1 S. 1 Nr. 1 und 5 TKG-E)

Die vorgesehene Erweiterung der Zwangserhebung von Bestandsdaten (§ 111 Abs. 1 TKG) auf die Gerätenummern von Mobiltelefonen und auf Internet-Dienste hätte im Internetbereich weitreichende Folgen.

§ 111 TKG-E soll neben der Vergabe von Rufnummern nun auch die Vergabe „anderer Anschlusskennungen" erfassen. Es fehlt jedoch eine Definition des Begriffs der „Anschlusskennung". Dieser Begriff wird im Bundesrecht bislang nur im Zusammenhang mit der Telekommunikationsüberwachung verwendet, etwa in den §§ 110b, 110h StPO. Im Sinne dieser Vorschriften soll etwa eine Internetprotokolladresse (IP-Adresse) als Anschlusskennung anzusehen sein.[90] Im Zusammenhang mit § 111 TKG würde dies bedeuten, dass jeder, der geschäftsmäßig IP-Adressen vergibt, verpflichtet wäre, die Personalien der Nutzer zu erheben und zum elektronischen Abruf nach § 112 TKG bereit zu halten.

Dies aber würde das Ende einer Vielzahl von Angeboten bedeuten. So müssten sämtliche kostenlosen öffentlichen WLAN-Internetzugänge wie „Freifunk" oder „FON" eingestellt werden, weil die – meist privaten – Anbieter eine Identifizierung der Nutzer und die Online-Bereitstellung von Teilnehmerdaten (§ 112 TKG) nicht leisten können. Gleiches gilt für die Anbieter von Proxy-Servern und Anonymisierungsdiensten, die ebenfalls IP-Adressen bereitstellen.[91] Ferner könnte der Benutzername bei Inanspruchnahme von Internettelefonie (z.B. „Skype"), von Chat-Diensten oder von Instant Messaging-Diensten als „Anschlusskennung" anzusehen sein.

Insgesamt ist der Begriff „andere Anschlusskennungen" in § 111 TKG-E ist unbestimmt und ausufernd weit. Die Pflichten der §§ 111, 112 TKG sind schon jetzt europaweit nahezu einzigartig. Ihre Ausweitung auf sämtliche IP-basierten Internetdienste würde Deutschland vollends international isolieren und technologisch weit zurückwerfen. International selbstverständliche Dienste wie kostenlose WLAN-Internetzugänge oder Anonymisierungsdienste könnten einzig in Deutschland nicht mehr angeboten werden.

Die vorgesehene Erweiterung der Zwangserhebung von Bestandsdaten in § 111 Abs. 1 TKG ist ohnehin in mehrfacher Hinsicht widersinnig.

Sie widerspricht erstens der Vorgabe des Bundestagsbeschlusses vom 16.02.2006, wonach die Speicherpflichten der Richtlinie 2006/24/EG nur in ihren Mindestanforderungen umgesetzt werden sollen. Die Richtlinie sieht eine Pflicht zur Erhebung von Bestandsdaten nicht vor, sondern nur Mindestspeicherfristen für ohnehin von den Anbietern erhobene Daten.

Weiter widerspricht die vorgesehene Ausdehnung des § 111 TKG der eigenen Erkenntnis der Bundesregierung, *„dass die §§ 111 bis 113 TKG Gegenstand eines derzeit beim Bundesverfassungsgericht anhängigen Verfassungsbeschwerdeverfahrens sind (1 BvR 1299/05). Während der Anhängigkeit eines solchen Verfahrens erscheint es ratsam, Änderungen der betroffenen Vorschriften nur dann vorzunehmen, wenn hierzu ein unabweisbares Bedürfnis besteht."*[92]

Ein solches Bedürfnis wird im Hinblick auf die vorgesehenen Erweiterungen nicht auch nur im Ansatz dargelegt, geschweige denn durch eine Untersuchung belegt. Die Regelungen entspringen offenbar einer „Wunschliste" der Eingriffsbehörden, ohne dass konkret überprüft wurde, ob damit in der Praxis nennenswerte Erfolge erzielt werden können.

Ernstzunehmende Kriminelle geben beim Kauf eines Mobiltelefons und bei der Anmeldung eines Internetzugangs nicht ihren echten Namen an. Es genügt schon die Angabe eines Namens aus dem Telefonbuch, um die geplanten Regelungen zu umgehen. Diese sind mithin von vornherein untauglich. Sie schädigen im Wesentlichen nur die Privatsphäre rechtstreuer Bürger, denen die Möglichkeit genommen wird, anonym per Internet zu kommunizieren, und sei es mit Anwälten, Ärzten, Beratungsstellen und Journa-

90 KK-Nack, § 100b StPO, Rn. 4.

91 Zur Bedeutung von Anonymisierungsdiensten siehe Seite 38.

92 Ziff. 18 der Gegenäußerung der Bundesregierung, BT-Drs. 16/5846, 231.

listen. Die anhängige Verfassungsbeschwerde gegen § 111 TKG (Az. 1 BvR 1299/05) rügt zu Recht, dass die Vorschrift unverhältnismäßig in das Fernmeldegeheimnis und in das Grundrecht auf informationelle Selbstbestimmung eingreift.

Schließlich widerspricht die geplante Ausdehnung des § 111 TKG der Warnung des Bundesverfassungsgerichts, von einer neuerlichen Ausdehnung von Grundrechtseingriffen zulasten unbeteiligter Dritter abzusehen.[93]

Für den Fall, dass § 111 TKG nicht gänzlich gestrichen wird, fordern wir dessen unveränderte Beibehaltung bis zur Entscheidung des Bundesverfassungsgerichts über die anhängige Verfassungsbeschwerde.

3. Online-Identifizierung auch von E-Mail-Nutzern (§§ 111 Abs. 1 S. 3, 112 TKG-E)

§ 111 Abs. 1 S. 3 TKG-E soll nun auch E-Mail-Dienste verpflichten, Daten zur Identifizierung ihrer Kunden in die Datenbank einzustellen, auf die eine Vielzahl von Behörden Onlinezugriff haben (§ 112 TKG). Diese Erweiterung des automatischen Abrufverfahrens auf E-Mail-Dienste ist in mehrfacher Hinsicht widersinnig.

Sie widerspricht erstens wiederum der eigenen Erkenntnis der Bundesregierung, *„dass die §§ 111 bis 113 TKG Gegenstand eines derzeit beim Bundesverfassungsgericht anhängigen Verfassungsbeschwerdeverfahrens sind (1 BvR 1299/05). Während der Anhängigkeit eines solchen Verfahrens erscheint es ratsam, Änderungen der betroffenen Vorschriften nur dann vorzunehmen, wenn hierzu ein unabweisbares Bedürfnis besteht.“*[94]

Ein solches Bedürfnis wird im Hinblick auf die vorgesehenen Erweiterungen nicht auch nur im Ansatz dargelegt, geschweige denn durch eine Untersuchung belegt. Die Regelungen entspringen offenbar einer „Wunschliste“ der Eingriffsbehörden, ohne dass konkret überprüft wurde, ob damit in der Praxis nennenswerte Erfolge erzielt werden können.

Ernstzunehmende Kriminelle geben bei der Anmeldung eines E-Mail-Kontos nicht ihren echten Namen an. Es genügt schon die Angabe eines Namens aus dem Telefonbuch oder aber die Nutzung eines kostenlosen ausländischen Dienstes (z.B. Yahoo Mail, Gmail), um die geplanten Regelungen zu umgehen. Diese sind mithin von vornherein untauglich. Sie schädigen im Wesentlichen nur die Privatsphäre rechtstreuer Bürger, denen die Möglichkeit genommen wird, anonym per Internet zu kommunizieren, und sei es mit Anwälten, Ärzten, Beratungsstellen und Journalisten. Die anhängige Verfassungsbeschwerde gegen § 111 TKG (Az. 1 BvR 1299/05) rügt zu Recht, dass die Vorschrift unverhältnismäßig in das Fernmeldegeheimnis und in das Grundrecht auf informationelle Selbstbestimmung eingreift.

Schließlich widerspricht die geplante Ausdehnung des Online-Abrufverfahrens der Warnung des Bundesverfassungsgerichts, von einer neuerlichen Ausdehnung von Grundrechtseingriffen zulasten unbeteiligter Dritter abzusehen.[95]

Die geplante Änderung wird erhebliche wirtschaftliche Auswirkungen haben. Laut Gesetzesbegründung wird eine „Verfünffachung der anzuschließenden Unternehmen“ die Folge der Einbeziehung von E-Mail-Diensten in den Anwendungsbereich des § 111 TKG sein (S. 6 f.). Jeder E-Mail-Dienst für die Öffentlichkeit soll erfasst sein. Selbst kleinste Dienste werden verpflichtet, an dem Online-Verfahren teilzunehmen. E-Mail-Dienste werden verbreitet kostenlos und werbefinanziert angeboten. Die Kosten des automatisierten Abrufverfahrens werden viele Anbieter nicht tragen können. § 111 Abs. 1 S. 3 TKG-E vernichtet deswegen nicht nur wirtschaftliche Existenzen, sondern beeinträchtigt auch den Wettbewerb und das Angebot von E-Mail-Diensten an Verbraucher und Unternehmen in Deutschland.

Für den Fall, dass § 111 TKG nicht gänzlich gestrichen wird, fordern wir dessen unveränderte Beibehaltung bis zur Entscheidung des Bundesverfassungsgerichts über die anhängige Verfassungsbeschwerde.

93 BVerfG, 2 BvR 1345/03 vom 22.08.2006, MMR 2006, 805 (810), Abs. 84.

94 Ziff. 18 der Gegenäußerung der Bundesregierung, BT-Drs. 16/5846, 231.

95 BVerfG, 2 BvR 1345/03 vom 22.08.2006, MMR 2006, 805 (810), Abs. 84.

4. Vorratsspeicherung von Bestandsdaten (§ 111 Abs. 4 TKG-E)

§ 111 Abs. 4 TKG-E ordnet, wie auch § 95 Abs. 3 TKG, die Vorratsspeicherung von Bestandsdaten über die betrieblich erforderliche Dauer hinaus an.

Diese Vorratsdatenspeicherung ist ebenso verfassungswidrig wie die Vorratsspeicherung von Verkehrsdaten (§ 113a TKG-E). Zur Begründung wird auf die obigen Ausführungen Bezug genommen (Seite 33). Die vorbenannte Verfassungsbeschwerde (Az. 1 BvR 1299/05) richtet sich zu Recht auch gegen § 111 Abs. 4 TKG.

Die in § 111 Abs. 4 TKG-E vorgesehene Speicherdauer von bis zu zwei Jahren geht überdies weit über die Mindestvorgaben der Richtlinie hinaus. Das Gleiche gilt für die in der Richtlinie nicht vorgesehene Einbeziehung nichtöffentlicher Dienste.

Wir fordern die Streichung des § 95 Abs. 3 TKG und des § 111 Abs. 4 TKG-E, andernfalls jedenfalls die Beschränkung der Speicherdauer auf sechs Monate.

5. Kostenerstattung (§ 111 Abs. 5 TKG-E)

Der Ausschluss einer Entschädigung für die Vorratsdatenerhebung ist verfassungswidrig. Auf die diesbezüglichen Ausführungen zu § 113a TKG-E wird verwiesen (Seite 42).

IX. §§ 112, 113 TKG [Auskünfte über Bestandsdaten]

Die §§ 112 und 113 TKG räumen den verschiedensten öffentlichen Stellen Zugriffsrechte auf Telekommunikations-Bestandsdaten ein. Diese Bestandsdaten geben insbesondere Aufschluss darüber, wer an bestimmten Telekommunikationsvorgängen beteiligt war, und ermöglichen die Erhebung von Kommunikationsinhalten (durch nachfolgende Überwachungsmaßnahmen oder – bei PINs und Passwörtern – durch unmittelbaren Zugriff). Die Identität der Kommunikationspartner ist integraler Bestandteil der Kommunikation selbst. Ohne die Kenntnis der Identität der Kommunikationsbeteiligten ist die Kenntnis der sonstigen Kommunikationsumstände und des Inhalts der Telekommunikation nutzlos. Dies verdeutlicht die besondere Sensibilität von Bestandsdaten.

Nach der Rechtsprechung setzt eine Auskunftsanforderung nach den §§ 112, 113 TKG nicht voraus, dass Name oder Anschlusskennung der Zielperson angegeben wird. Es genügt bereits die Angabe der näheren Umstände eines Kommunikationsvorgangs (z.B. eines Telefonanrufs, eines Internet-Seitenabrufs), um gemäß § 113 TKG Auskunft über den „dahinter stehenden“ Anschlussinhaber zu verlangen. Praxisrelevant ist die Vorschrift vor allem bei der Verfolgung von Urheberrechtsverstößen im Internet (in „Tauschbörsen“) anhand der Sitzungskennung (dynamisch vergebenen IP-Adresse) des Nutzers.

Durch die geplante Vorratsspeicherung von Verkehrsdaten wird § 113 TKG erheblich an Bedeutung gewinnen. Denn die Identifizierung von Internetnutzern setzt voraus, dass die Internetzugangsanbieter die Vergabe von IP-Adressen protokollieren. Zu Abrechnungszwecken ist dies nicht erforderlich, weswegen eine solche Protokollierung bislang unzulässig ist. Im Fall von T-Online haben die Gerichte dies bestätigt.[96] Mit der geplanten Vorratsspeicherung der jeweils genutzten IP-Adressen wird eine Vervielfachung der Auskunftsanforderungen nach § 113 TKG einhergehen. Der vorliegende Gesetzesentwurf sieht nicht einmal eine statistische Erfassung der Anzahl der Auskunftsanforderungen nach § 113 TKG vor.

Die geltenden Regelungen der §§ 112, 113 TKG sind verfassungswidrig und dringend überarbeitungsbedürftig. Unter anderem sehen sie keinerlei Erheblichkeitsschwelle vor. Den Zugriff auf Bestandsdaten eröffnen die §§ 112, 113 TKG letztlich allen Behörden, die irgend ein Interesse an diesen Daten haben könnten. Schon die Verfolgung von Ordnungswidrigkeiten und von Schwarzarbeit soll einen Zugriff rechtfertigen. Dies wird der Aussagekraft und Sensibilität der Auskünfte in keiner Weise gerecht. Die anhängige Verfassungsbeschwerde (Az. 1 BvR 1299/05) richtet sich daher zu Recht auch gegen die §§ 112, 113 TKG.

96 Landgericht Darmstadt vom 25.01.2006, Az. 25 S 118/05, MMR 2006, 330, rechtskräftig nach BGH vom 28.10.2006, Az. III ZR 40/06.

Verhältnismäßig sind Zugriffsrechte vor dem Hintergrund der hohen Nutzbarkeit und Verwendungsmöglichkeiten von Bestandsdaten nur zur Verfolgung schwerer Straftaten. Eben dies sieht auch die Richtlinie zur Vorratsdatenspeicherung vor, die auch auf vorratsgespeicherte Bestandsdaten Anwendung findet. Die Richtlinie 2006/24/EG gilt für Verkehrs- und Bestandsdaten gleichermaßen. Dies übersieht der vorliegende Gesetzesentwurf. Während § 113b TKG-E die Verwendung vorratsgespeicherter Verkehrsdaten beschränkt, versäumt der Gesetzesentwurf dies für Bestandsdaten.

Wir fordern, die Abfrage von Bestandsdaten nach den §§ 112, 113 TKG auf die Verfolgung schwerer Straftaten zu beschränken, wie es die Richtlinie 2006/24/EG und das deutsche Verfassungsrecht vorgeben. Außerdem fordern wir, die Anzahl der Auskunftsanforderungen nach § 113 TKG statistisch erfassen zu lassen.

X. § 113a TKG-E [Speicherungspflichten für Verkehrsdaten] und § 113b TKG-E [Verwendung der nach § 113a gespeicherten Daten]

1. Verfassungswidrigkeit

Die vorgesehene Vorratsspeicherung von Verkehrsdaten verstößt gegen das Fernmeldegeheimnis, das Grundrecht auf informationelle Selbstbestimmung, die Meinungs- und Rundfunkfreiheit sowie das Gleichbehandlungsgebot.

a) Mangelnde Effektivität

Es fehlt bereits die Erforderlichkeit einer Vorratsspeicherung von Verkehrsdaten. Schon heute haben Ermittler Zugriff auf Verbindungsdaten (§§ 100g, 100h StPO), die zu Abrechnungszwecken gespeichert sind (§ 97 Abs. 3 TKG). Im Bedarfsfall kann zusätzlich die Aufzeichnung der Kommunikationsdaten Verdächtiger angeordnet werden (§ 100g Abs. 1 S. 3 StPO bzw. §§ 100a, 100b StPO). Die erfolgreiche Aufklärung der terroristischen Anschläge in Madrid weist darauf hin, dass die gegenwärtige Verfügbarkeit von Kommunikationsdaten ausreicht und eine systematische, vorsorgliche Protokollierung des Telekommunikationsverhaltens der gesamten Bevölkerung nicht erforderlich ist. Eine Vorratsdatenspeicherung würde fast durchweg die Kommunikation unschuldiger und unverdächtiger Menschen treffen. Es gibt kein Bedürfnis einer Protokollierung der Kommunikation und des Bewegungsverhaltens der Ärztin, des Steuerberaters oder der Rentnerin von nebenan.

Nach einer Studie des Bundeskriminalamts vom November 2005[97] konnten in den letzten Jahren 381 Straftaten wegen fehlender Telekommunikationsdaten nicht aufgeklärt werden, vor allem in den Bereichen Internetbetrug, Austausch von Kinderpornografie und Diebstahl. Die 381 Fälle beziehen sich auf einen Zeitraum von mehreren Jahren, konnten teilweise auch auf anderem Wege aufgeklärt werden und hätten selbst mit einer sechsmonatigen Vorratsdatenspeicherung teilweise nicht aufgeklärt werden können. Vor allem machen diese 381 Fälle nur 0,01% der 2,8 Mio. Straftaten aus, die laut Kriminalstatistik Jahr für Jahr nicht aufgeklärt werden können.

Stellt man sich die 2,8 Mio. jährlich nicht aufklärbarer Straftaten zur besseren Veranschaulichung als eine mit Wasser gefüllte Literflasche vor, so entsprechen die Fälle fehlender Verkehrsdaten gerade einmal der Menge eines Wassertropfens. Auf diese Weise kann der „Durst“ nach verbesserter Strafverfolgung nicht gelöscht werden. Eine Vorratsdatenspeicherung käme dem sprichwörtlichen Tropfen auf den heißen Stein gleich. Schon jetzt ist die Aufklärungsquote im Bereich mittels Telekommunikation begangener Straftaten den einschlägigen Statistiken zufolge nicht niedriger, sondern höher als im Durchschnitt (55%). In den Bereichen Internetbetrug und Softwarepiraterie liegt die Aufklärungsquote etwa bei über 80%. Eine Vorratsdatenspeicherung würde die durchschnittliche Aufklärungsquote von bisher 55% im besten Fall auf 55,006% erhöhen, wenn man von 381 pro Jahr zusätzlich aufgeklärten Straftaten ausgeht.

97 Mindestspeicherungsfristen für Telekommunikationsverbindungsdaten – Rechtstatsachen zum Beleg der defizitären Rechtslage, http://www.vorratsdatenspeicherung.de/images/bka_vorratsdatenspeicherung.pdf

Auf Vorrat gespeicherte Kommunikationsdaten können den Strafverfolgern vereinzelt zwar nützlich sein. Dies wird in der Regel allerdings nur bei unvorsichtigen Kleinkriminellen der Fall sein. Der Präsident des Europäischen Verbands der Polizei Heinz Kiefer warnte 2005: „*Für Kriminelle bliebe es einfach, mit relativ simplen technischen Mitteln eine Entdeckung zu verhindern, z.B. durch den Einsatz und häufigen Wechsel im Ausland gekaufter, vorausbezahlter Mobiltelefonkarten. Das Ergebnis wäre ein enormer Aufwand mit wenig mehr Wirkung auf Kriminelle und Terroristen, als sie etwas zu verärgern.*“[98]

Eine Vorratsdatenspeicherung wirkt sogar kontraproduktiv, weil sie die Entwicklung und den Einsatz von Anonymisierungstechniken fördert und der Polizei auf diese Weise selbst in Fällen schwerster Gefahr die Möglichkeit erfolgversprechender Ermittlungen abschneidet. Klaus Jansen, Vorsitzender des Bundes Deutscher Kriminalbeamter, klagt bereits heute: „*Da es sich herumgesprochen hat, dass Telefongespräche relativ leicht abgehört werden können, reden die Verdächtigen nur noch selten offen am Telefon*“.[99] Wenn eine Vorratsdatenspeicherung eingeführt wird, werden sich Kriminelle auch darauf bald eingerichtet haben. Im Volkszählungsurteil hat das Bundesverfassungsgericht schon einmal eine Regelung über die Weiterverwertung von Daten zu anderen Zwecken verworfen. Es hat dies begründet mit dem Argument, die Regelung beeinträchtige die „Bereitschaft, wahrheitsgemäße Angaben zu machen“ und gefährde damit die „Funktionsfähigkeit der amtlichen Statistik“.[100] In ähnlicher Weise gefährdet die Vorratsspeicherung von Verkehrsdaten die Funktionsfähigkeit der Strafverfolgung, die auf die Möglichkeit einer erfolgreichen Telekommunikationsüberwachung angewiesen ist und durch ein zunehmendes Ausweichen auf Anonymisierungstechniken gefährdet wäre.

Dass die Massenspeicherung von Kommunikationsdaten den Ermittlungsbehörden in einzelnen Fällen nützlich sein könnte, bedeutet zudem nicht, dass sie den Schutz der Bürger vor Straftaten verbessern würde. Insoweit ist zunächst eine realistische Einordnung der „Bedrohung“ durch Kriminalität erforderlich. Eurostat zufolge sterben weniger als 0,002% der Europäer jährlich als Opfer einer Straftat, terroristische Anschläge eingeschlossen. Weiter führt die Weltgesundheitsorganisation eine Statistik, die den Verlust gesunder Lebenszeit durch vorzeitigen Tod, Krankheit oder Behinderung misst. Dieser Statistik zufolge beruht der Verlust gesunder Lebenszeit für Westeuropäer zu 92% auf Krankheiten, zu 2% auf Verkehrsunfällen, zu 1% auf Stürzen, zu 1,7% auf Suizid und nur zu 0,2% auf Gewalt und Straftaten. Die großen Gesundheitsrisiken sind andere als Kriminalität: Bluthochdruck, Tabak, Alkohol, Cholesterin, Übergewicht, Fehlernäherung und Bewegungsmangel sind die Hauptrisikofaktoren. Auch dass uns Lebensrisiken wie Armut, Arbeitslosigkeit oder Naturkatastrophen treffen, ist weitaus wahrscheinlicher als das Risiko, Opfer einer Straftat zu werden.

Die europäischen Strafverfolgungsbehörden gewährleisten also bereits heute einen guten Schutz vor Straftaten, ohne dass Informationen über die Kommunikation der gesamten Bevölkerung zur Verfügung stehen müssten. Die Telekommunikationsüberwachung im Bedarfsfall hat in der Vergangenheit stets genügt. Selbst die USA kennen keine Vorratsspeicherungspflicht. Erst in den letzten Jahren haben einzelne europäische Staaten wie Irland generelle Speicherungspflichten eingeführt, ohne dass dies aber einen Einfluss auf die Kriminalitätsrate dieser Staaten gehabt hätte. Somit ist nicht erkennbar, dass eine Vorratsdatenspeicherung die Sicherheit der Bevölkerung stärkt.

Aus Sicht der Strafverfolger fehlen bei Verfolgung ernsthafter Krimineller im Übrigen regelmäßig nicht Verkehrsdaten in Deutschland, sondern Zugriffsmöglichkeiten auf ausländische Verkehrsdaten.[101] Es ist bekannt, dass 89% der Fälle organisierter Kriminalität einen internationalen Bezug aufweisen.[102] In 80% der von der deutschen „Zentralstelle für anlassunabhängige Recherchen in Datennetzen” eingeleiteten strafrechtlichen Ermittlungsverfahren sind Zugriffe auf im Ausland gespeicherte Verkehrsdaten erforder-

98 Pressemitteilung vom 02.06.2005, http://snipurl.com/m82z.

99 http://daserste.ndr.de/panorama/archiv/2005/t_cid-2843438_.html.

100 BVerfGE 65, 1 (50 und 64).

101 Näher Breyer, Vorratsspeicherung (2005), www.vorratsspeicherung.de.vu, 349 f. m.w.N.

102 Holznagel/Nelles/Sokol, Die neue TKÜV (2002), 63 (71).

lich.[103] Derzeit dauert es Monate bis Jahre, bis Daten aus anderen EU-Staaten übermittelt werden; der Zugriff auf Verkehrsdaten außerhalb der EU ist nahezu komplett unmöglich.[104] Angesichts dessen wäre es zur Verfolgung ernsthafter Straftäter um vieles nützlicher, die internationale Sicherung und Übermittlung von Verkehrsdaten zu ermöglichen sowie Mechanismen zur internationalen Erhebung von Verkehrsdaten im Einzelfall einzuführen als leicht zu umgehende Regelungen zur generellen Verkehrsdatenspeicherung im europäischen Alleingang zu schaffen.

b) Risiko falscher Verdächtigung

Die Unverhältnismäßigkeit einer generellen Protokollierung des Telekommunikationsverhaltens ergibt sich auch aus den negativen Auswirkungen dieser Maßnahme auf die Sicherheit der Bürger. Als „Verdachtsschöpfungsinstrument“ erhöht eine Vorratsspeicherung das Risiko, zu Unrecht einer Straftat verdächtigt zu werden. Zur Aufklärung einer Brandstiftung in Schleswig-Holstein beispielsweise wurden anhand von Telekommunikationsdaten alle Besitzer eines Mobiltelefons ermittelt, die sich zur Tatzeit in der Nähe des Brandorts aufhielten. Die Polizei kündigte eine Vernehmung all dieser Personen an.[105] Auch sind Fälle bekannt, in denen Mobiltelefone gestohlen oder Internetzugänge „gehackt“ wurden und dadurch die Anschlussinhaber in den falschen Verdacht einer Straftat gerieten. Eine generelle Speicherung von Telekommunikationsdaten erhöht die allgemeine Gefahr falscher Verdächtigungen erheblich, weil Kommunikationsdaten inhaltlich nur beschränkt aussagekräftig sind und der jeweilige Benutzer des Geräts nicht sicher feststellbar ist. Die Vorratsdatenspeicherung wird dadurch selbst zum Sicherheitsrisiko.

c) Abschreckung erwünschten Verhaltens

Hinzu kommt das Risiko eines Missbrauchs der Daten durch Polizeibeamte, staatliche Behörden, Mitarbeiter von Telekommunikationsunternehmen oder Dritte. Eine Reihe von Vorfällen in der Vergangenheit (z.B. Bonusmeilenaffäre) hat gezeigt, dass ein Missbrauch sensibler Daten immer wieder vorkommt. Um die Bürger effektiv vor Datenmissbrauch zu schützen, sollte die Aufzeichnung von Kommunikationsdaten von vornherein so weit wie möglich untersagt werden.

Andernfalls werden sich manche, die auf die Hilfe eines Arztes, eines Rechtsanwalts, eines Psychologen oder einer Beratungsstelle angewiesen sind, dadurch abschrecken lassen, dass ihr Kontakt noch monatelang nachvollzogen werden könnte und sensible Informationen über ihr Privatleben in die falschen Hände geraten könnten. Das Gleiche gilt für regierungskritische Aktivisten und Demonstranten, die ihre Aktivitäten per Telefon oder Internet koordinieren. Informanten von Journalisten, die anonym staatliche Missstände aufdecken möchten, werden es in Zukunft ebenfalls schwer haben. Die Nachvollziehbarkeit von Geschäftskontakten wird schließlich auch zur Wirtschaftsspionage genutzt werden.

Das Bundesverfassungsgericht hat wiederholt davor gewarnt, dass eine exzessive Kommunikationsüberwachung die Unbefangenheit der Kommunikation beeinträchtigt und dadurch letztlich unserer Gesellschaft insgesamt schadet: „*Die Befürchtung einer Überwachung mit der Gefahr einer Aufzeichnung, späteren Auswertung, etwaigen Übermittlung und weiteren Verwendung durch andere Behörden kann schon im Vorfeld zu einer Befangenheit in der Kommunikation, zu Kommunikationsstörungen und zu Verhaltensanpassungen [...] führen.*“[106] Die ehemalige Präsidentin des Bundesverfassungsgerichts Jutta Limbach wird noch deutlicher: „*Eine demokratische politische Kultur lebt von der Meinungsfreude und dem Engagement der Bürger. Das setzt Furchtlosigkeit voraus. Diese dürfte allmählich verloren gehen, wenn der Staat seine Bürger biometrisch vermisst, datenmäßig durchrastert und seine Lebensregungen elektronisch verfolgt.*“[107]

---

103 BMI/BMJ, Sicherheitsbericht 2001, 203.

104 Breyer, Vorratsspeicherung (2005), www.vorratsspeicherung.de.vu, 349 f. m.w.N.

105 Segeberger Zeitung vom 02.08.2005, http://segeberg.nordclick.de/news/archiv/?id=1688548.

106 BVerfG, 1 BvR 2226/94 vom 14.07.1999, NJW 1996, 114 (114), Abs. 234.

107 Ist die kollektive Sicherheit Feind der individuellen Freiheit? Rede vom 10.05.2002, http://www.zeit.de/reden/deutsche_innenpolitik/200221_limbach_sicherheit?page=all.

d) Dammbruch

Irreführend ist die Behauptung, Verbindungsdaten würden bereits heute gespeichert. Tatsächlich dürfen gegenwärtig nur abrechnungsrelevante Verbindungsdaten gespeichert werden (§ 97 Abs. 3 TKG). Nicht zulässig ist damit unter anderem die Aufzeichnung von Daten über die Internet- oder E-Mail-Nutzung oder über den Standort von Mobiltelefonen. Durch die Benutzung von Pauschaltarifen kann eine Datenspeicherung bisher zudem gänzlich vermieden werden. Auch sonst können Kunden die sofortige Löschung der gewählten Zielrufnummern mit Rechnungsversand wählen (§ 97 Abs. 4 TKG). All diese Mechanismen zum Schutz sensibler Kontakte und Aktivitäten würde eine Vorratsdatenspeicherung beseitigen.

Falsch ist auch die Behauptung, den Strafverfolgungsbehörden stünden heute weniger Kommunikationsdaten zur Verfügung als früher. Das Gegenteil ist der Fall. Vorausbezahlte Mobiltelefonkarten konnten bis vor wenigen Jahren noch vollständig anonym erworben werden, während heute eine Identifizierungspflicht besteht. Bis in die 90er Jahre hat es im Telefonnetz keine digitalen Vermittlungsstellen und folglich auch keine Speicherung von Einzelverbindungsdaten gegeben, während diese Daten den Ermittlern heute meist zur Verfügung stehen. Schließlich bringt die Informationsgesellschaft mit sich, dass ein immer größerer Teil des täglichen Lebens in die Telekommunikationsnetze und das Internet verlagert wird (z.B. Online-Shopping, Telemedizin, Internet-Zeitungen), während früher vergleichbare Tätigkeiten im Schutz von Wohnungen oder Gebäuden stattgefunden haben. Die heutige Gesellschaft ist also viel leichter überwachbar als es noch vor wenigen Jahren der Fall war.

Wenn von Regierungsseite betont wird, der Zugriff auf die gespeicherten Kommunikationsdaten werde nur sehr eingeschränkt zulässig sein, so widerlegen dies die vielfältigen vorgesehenen Zugriffsrechte. Der Zugriff durch Geheimdienste sowie auf Bestandsdaten ist bereits heute ohne richterliche Anordnung möglich. Darüber hinaus zeigen die Erfahrungen der Vergangenheit, dass man die nützlichen Datenbestände sukzessive zu weiteren Zwecken freigeben wird. Schon heute werden Verbindungsdaten zehntausende Male im Jahr abgefragt, die Identität von Telefon-, Handy-, E-Mail- und Internetnutzern (Bestandsdaten) sogar mehrere Millionen Mal jährlich (3,4 Mio. mal im Jahr 2005 oder 9.000mal am Tag). Eine Vorratsdatenspeicherung würde die Zahl der Abfragen noch einmal sprunghaft ansteigen lassen. In Anbetracht dessen kann keine Rede davon sein, dass der Zugriff auf die gespeicherten Daten engen Voraussetzungen unterliege.

Die verdachtslose Massenspeicherung von Kommunikationsdaten stellt im Kern einen Präzedenzfall einer verdachtsunabhängigen, flächendeckenden maschinellen Überwachung der Bevölkerung dar. Der Kampf gegen den Terror wird so zunehmend zum Kampf gegen den Bürger. Während der freiheitliche Rechtsstaat im Grundsatz der Gesetzestreue seiner Bürger vertraute, ist im „Sicherheitsstaat“ prinzipiell jeder verdächtig, ein „Gefährder“ zu sein. Mit den Argumenten der Befürworter einer Vorratsdatenspeicherung ließen sich sogar George Orwells „Telescreens“ (Videokameras) in jeder Wohnung rechtfertigen, solange auf die Aufnahmen nur im Fall schwerer Gefahren zugegriffen werden dürfte. Daran wird deutlich, dass die Vorratsspeicherung der Kommunikation der gesamten Bevölkerung einen Dammbruch der traditionellen Grenzen staatlicher Eingriffe in die Rechte unbescholtener Bürger darstellt. Selbst die Bundesjustizministerin erklärte am 19.09.2006 zur Eröffnung des Deutschen Juristentages: *„Wir können auch nicht über eine Vielzahl von Bürgerinnen und Bürgern immer mehr Daten anhäufen, um so einem Verdacht auf die Spur zu kommen.“*

Die vermeintliche „Speicherung mit Augenmaß“ würde schon bald ausgeweitet werden. Die Justiz- und Innenpolitik der vergangenen Jahre zwingt zu der Prognose, dass eine Verlängerung der Speicherfristen, die Einbeziehung weiterer Datentypen sowie die Einführung von Auskunftsrechten für weitere Behörden und private „Rechteinhaber“ nicht lange auf sich warten lassen würden. Die Vorratsspeicherung von Bewegungen mit nur empfangsbereitem Handy, die Protokollierung von Internetnutzungsdaten und die Aufbewahrung von Inhaltsdaten (z.B. Betreffzeilen, SMS) ist absehbar. Aber auch in anderen Bereichen würde das Beispiel der Vorratsdatenspeicherung Schule machen. Die Vorratsspeicherung von Flugreisen und Nahverkehrsfahrten, von Fahrzeugbewegungen auf Autobahnen, von Aufzeichnungen privater Überwa-

chungskameras, von Einkäufen in Geschäften und Ausleihvorgängen in Büchereien sind Beispiele einer Vorratsspeicherung, die im Ausland geplant oder bereits realisiert sind.

Spektakuläre Straftaten, die zuvor Undenkbares als wünschenswert erscheinen lassen, werden auch in Deutschland immer wieder neue Forderungen laut werden lassen. Die vorsorgliche Protokollierung personenbezogener Daten ist für den Staat stets und in allen Bereichen nützlich. Aus jedem personenbezogenen Datum können sich im Einzelfall einmal Schlüsse bezüglich einer begangenen oder geplanten schweren Straftat 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 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.

e) Ergebnis

Die Abwägung des Nutzens mit den Gefahren einer systematischen Protokollierung des Telekommunikationsverhaltens ergibt, dass das Interesse an der verbesserten strafrechtlichen Verfolgung von Einzelfällen hinter die Grundrechte der Vielzahl rechtmäßig handelnder Nutzer zurücktreten muss. Das Verbot einer Vorratsdatenspeicherung dient nämlich dem – gegenüber einer möglichen verbesserten Strafverfolgung höherwertigen – Zweck, sensible Daten der unzähligen rechtmäßig handelnden Nutzer vor unberechtigten und missbräuchlichen Zugriffen zu schützen und deren unbefangenes Gebrauchmachen von ihren grundrechtlich geschützten Freiheiten zu ermöglichen. Die Strafverfolgungsbehörden würden nur einen kleinen Bruchteil (etwa 0,0004%[108]) der gespeicherten Kommunikationsdaten jemals nachfragen, während mehr als 99% der von einer Vorratsspeicherung Betroffenen vollkommen unschuldig wären.[109] Eine solche Vorratsdatenspeicherung ist evident unverhältnismäßig.[110] Das Bundesverfassungsgericht wird dementsprechend die §§ 113a, 113b TKG-E für verfassungswidrig erklären, falls sie Gesetz werden. Der Entwurf einer entsprechenden Verfassungsbeschwerde, verbunden mit einem Antrag auf einstweilige Aussetzung des Gesetzes wegen offensichtlicher Verfassungswidrigkeit, liegt bereits vor.[111] Schon mehrere tausend Bürger haben einen Rechtsanwalt mit der Erhebung der Verfassungsbeschwerde beauftragt.[112]

---

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

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

110 Bäumler/v. Mutius-Bäumler, Anonymität im Internet (2003), 8; Gitter/Schnabel, MMR 2007, 411 (414); Gola/Klug/Reif, NJW 2007, 2599 (2600 und 2602); Krader, DuD 2001, 344 (347); Kugelmann, DuD 2001, 215 (220); Uhe/Herrmann, Überwachung im Internet, http://ig.cs.tu-berlin.de/oldstatic/da/2003-08/UheHerrmann-Diplomarbeit-082003.pdf, 164 m.w.N.; Ulmer/Schrief, DuD 1994, 591 (596); Weßlau, ZStW 113 (2001), 681 (703); 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.

111 http://wiki.vorratsdatenspeicherung.de/images/Verfassungsbeschwerde_Vorratsdatenspeicherung.pdf.

112 http://www.vorratsdatenspeicherung.de/index.php?option=com_content&task=view&id=64&Itemid=70.

In den nächsten Monaten ist überdies die Entscheidung des Bundesverfassungsgerichts zur Vorratsspeicherung von Telekommunikations-Bestandsdaten (§§ 95 Abs. 3, 111 TKG) zu erwarten.[113] Diese Entscheidung wird jeden Zweifel an der Verfassungswidrigkeit auch der Vorratsspeicherung von Telekommunikations-Verkehrsdaten endgültig beseitigen.

Wir fordern, Artikel 2 des vorliegenden Gesetzentwurfs zu streichen und die anstehende Entscheidung des Bundesverfassungsgerichts zur Vorratsspeicherung von Telekommunikations-Bestandsdaten sowie die Entscheidung des Europäischen Gerichtshofs über die Wirksamkeit der Richtlinie 2006/24/EG abzuwarten, bevor der massive Grundrechtseingriff einer Protokollierung des Telekommunikationsverhaltens der gesamten Bevölkerung beschlossen wird.

2. Überschießender Umfang der Speicherung von E-Mail-Verbindungsdaten (§ 113a Abs. 3 TKG-E)

Der Regierungsentwurf geht in Bezug auf E-Mail-Dienste über die Richtlinie 2006/24/EG hinaus und widerspricht insoweit den Vorgaben des Bundestagsbeschlusses vom 16.02.2006.

In Deutschland soll bei jedem Versenden und Abrufen von E-Mail die Kennung (IP-Adresse) des Nutzers gespeichert werden, bei jedem Empfangen von E-Mails die IP-Adresse des Absenders (§ 113a Abs. 3 TKG-E). Dadurch hebelt der Regierungsentwurf die in § 111 Abs. 1 S. 3 TKG-E vorgesehene und auch in der Richtlinie vorausgesetzte Möglichkeit der anonymen Nutzung von E-Mail-Diensten wieder aus. Denn Internet-Zugangsanbieter müssen die Vergabe von IP-Adressen künftig auf Vorrat protokollieren. Über die vorratsgespeicherte IP-Adresse kann die Person des E-Mail-Nutzers letztlich doch festgestellt werden. Dies gilt selbst dann, wenn Deutsche E-Mails über anonyme Dienste versenden, die von Drittstaaten aus angeboten werden. Denn die deutsche IP-Adresse ist auch in über Drittstaaten versandten E-Mails enthalten und kann über den Zugangsprovider zugeordnet werden. Insofern geht § 113a Abs. 3 TKG-E weit über die noch im Referentenentwurf vorgesehene Identifizierungspflicht für E-Mail-Nutzer hinaus. Die Datensammlung ist auch wirkungslos, weil professionelle Kriminelle sie durch den Einsatz internationaler Anonymisierungsdienste leicht umgehen können. In der EU-Richtlinie ist keine Rede davon, dass E-Mail-Anbieter IP-Adressen speichern sollen.

Falls eine Vorratsdatenspeicherung trotz ihrer Verfassungswidrigkeit beschlossen wird, fordern wir, die Speicherung von IP-Adressen in § 113a Abs. 3 TKG-E nicht vorzusehen.

3. Überschießendes Verbot von Anonymisierungsdiensten (§ 113a Abs. 6 TKG-E)

Der Regierungsentwurf geht in Bezug auf Anonymisierungsdienste über die Richtlinie 2006/24/EG hinaus und widerspricht insoweit den Vorgaben des Bundestagsbeschlusses vom 16.02.2006. Eine vergleichbare Vorschrift ist zudem weltweit in keinem anderen demokratischen Staat bekannt.

Ausweislich § 113a Abs. 6 TKG-E und der Entwurfsbegründung (S. 167) sollen auch Anonymisierungsdienste zur Vorratsdatenspeicherung verpflichtet werden. § 113a Abs. 6 TKG-E läuft jedoch bereits seinem Wortlaut nach leer. Er soll nur für den Anbieter gelten, der „die nach Maßgabe dieser Vorschrift zu speichernden Angaben verändert“. Anbieter von Anonymisierungsdiensten haben nach § 113a TKG aber keine Daten zu speichern, solange sie nicht gleichzeitig Internet-Zugangsanbieter sind. Außerdem verändern sie keine Daten, sondern sie leiten Anfragen lediglich weiter.

113 1 BvR 1299/05, http://www.tkg-verfassungsbeschwerde.de.

Die Einbeziehung von Anonymisierungsdiensten ist vor allem der Sache nach inakzeptabel, weil Menschen in bestimmten Situationen (z.B. Notlagen, Krankheiten) auf die Möglichkeit der anonymen Beratung und Hilfe über das Internet angewiesen sind. Die Richtlinie 2006/24/EG erfasst Anonymisierungsdienste nicht. Dies wäre auch sinnlos, weil im Ausland betriebene Internet-Anonymisierungsdienste kostenfrei zur Verfügung stehen (z.B. „TOR-Netzwerk“) und Straftäter eine Vorratsdatenspeicherung in Deutschland ohne Weiteres umgehen könnten. In Erwägungsgrund 33 der Richtlinie 2002/58/EG heißt es zutreffend:

> *„Um die Privatsphäre des Nutzers zu schützen, müssen die Mitgliedstaaten daher darauf hinwirken, dass bei den elektronischen Kommunikationsdiensten beispielsweise alternative Funktionen entwickelt werden, die den anonymen oder rein privaten Zugang zu öffentlich zugänglichen elektronischen Kommunikationsdiensten ermöglichen*“.

In Deutschland würde eine Protokollierungspflicht das Aus für die allermeisten Anonymisierungsdienste bedeuten. Anonymisierungsdienste werden regelmäßig kostenlos von Privatpersonen angeboten, die weder technisch noch finanziell in der Lage sind, Daten auf Vorrat zu speichern und die Vorgaben des Telekommunikationsgesetzes einzuhalten. Kommerzielle Anonymisierungsdienste, die in Deutschland belegen sind, haben bereits angekündigt, ihren Dienst in das Ausland verlagern, weil sie nicht glaubwürdig einen Anonymisierungsdienst anbieten und gleichzeitig jede Benutzung protokollieren können.

Das weitgehende Ende deutscher Anonymisierungsdienste würde sich auf die Nutzer dieser Dienste sehr nachteilig auswirken. Anonymisierungsdienste sind für viele Menschen unverzichtbar:

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

Gefängnisstrafen und Folter ausgesetzt; Anonymisierungsdienste schützen also Leben und Freiheit dieser Personen. Beispielsweise in Burma ist die demokratische Opposition auf die anonyme Kommunikation per Internet angewiesen.

Mit einer Protokollierungspflicht für Anonymisierungsdienste, die faktisch wie ein Verbot wirken würde, würde sich Deutschland in der Gemeinschaft demokratischer Staaten isolieren.

Wir fordern, § 113a Abs. 6 TKG zu streichen.

4. Überschießende Speicherfrist (§ 113a Abs. 2 TKG-E)

§ 113a TKG-E geht auch in einem weiteren Punkt über die Anforderungen der Richtlinie 2006/24/EG hinaus und widerspricht insoweit den Vorgaben des Bundestagsbeschlusses vom 16.02.2006: § 113a Abs. 2 TKG-E erweitert die Speicherfrist überschießend von 6 auf bis zu 7 Monate. Eine unverzügliche Löschungspflicht ist den Anbietern demgegenüber durchaus zumutbar. Sie ist schon heute in den §§ 96 Abs. 2 S. 2, 97 Abs. 3 S. 2 TKG vorgesehen.

Falls eine Vorratsdatenspeicherung trotz ihrer Verfassungswidrigkeit beschlossen wird, fordern wir die unverzügliche Löschung der gespeicherten Daten nach Ablauf von sechs Monaten.

5. Richtlinienwidrige Verwendung der Vorratsdaten (§ 113b TKG-E)

§ 113b TKG-E gibt die noch im Referentenentwurf vorgesehene Beschränkung der Verwendung vorratsgespeicherter Daten auf Zwecke der Strafverfolgung auf. Stattdessen sollen die Daten auch zur Gefahrenabwehr und für Zwecke der Nachrichtendienste bereit stehen.

Nach Art. 1 des Richtlinie 2006/24/EG erfolgt die Vorratsdatenspeicherung dagegen nur für die Verfolgung schwerer **Straftaten**, weswegen konsequenterweise auch die Verwendung der gespeicherten Daten auf die Verfolgung schwerer Straftaten beschränkt werden muss. Dies hat die Generalanwältin am Europäischen Gerichtshof jüngst bestätigt.[114] Es ist inakzeptabel, dass eine Regelung zuerst mit der Begründung der Bekämpfung schwerer Straftaten oder gar Terrorismus durchgesetzt wird, dann aber vor allem zur Verfolgung von Bagatellvergehen wie dem Austausch von Musik im Internet genutzt wird. Zumal das Europaparlament die Beschränkung auf die Verfolgung schwerer Straftaten als besonderen Verhandlungserfolg herausgestellt hat.

§ 113b TKG-E ist auch mit Art. 15 RiL 2002/58/EG unvereinbar.[115] Insoweit ist der neue Absatz 1a dieses Artikels zu beachten. Danach sind diejenigen Datentypen vor weiter gehenden Zugriffsbefugnissen geschützt, für welche in der Richtlinie 2006/24/EG „eine Vorratsspeicherung zu den in Artikel 1 Absatz 1 der genannten Richtlinie aufgeführten Zwecken ausdrücklich vorgeschrieben ist“. Für sämtliche der in der Vorratsspeicherungsrichtlinie genannten Verkehrs- und Bestandsdaten ist „eine Vorratsspeicherung zu den in Artikel 1 Absatz 1 der genannten Richtlinie aufgeführten Zwecken ausdrücklich vorgeschrieben“, so dass sämtliche in der Vorratsspeicherungsrichtlinie genannte Daten vor Zugriffen zu anderen Zwecken geschützt sind.

Abweichend vom klaren Wortlaut des Art. 15 Abs. 1a RiL 2002/58/EG geht Erwägungsgrund 12 der Vorratsspeicherungsrichtlinie davon aus, dass ein Zugriff auf vorratsgespeicherte Daten auch „zu anderen

114 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).

115 Art. 15 Abs. 1 S. 1 lautet: „Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für die nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist.“

– einschließlich justiziellen – Zwecken als denjenigen, die durch die vorliegende Richtlinie abgedeckt werden", eröffnet werden könne. Allerdings entfalten die Erwägungsgründe keine Rechtskraft und können lediglich zur Auslegung herangezogen werden. Einer Auslegung des Art. 15 Abs. 1a RiL 2002/58/EG steht dessen eindeutiger Wortlaut entgegen. Dass frühere Entwürfe zur Vorratsdatenspeicherung auf EU-Ebene noch ausdrücklich eine Datennutzung zu anderen Zwecken zuließen, verdeutlicht, dass das Europäische Parlament die Verwendung der Daten abweichend hiervon strikt auf die Verfolgung schwerer Straftaten beschränken wollte. Im Übrigen stellt die Verfolgung mittlerer und leichter Straftaten sowie von Ordnungswidrigkeiten keinen „anderen Zweck" dar als die Verfolgung schwerer Straftaten. Die repressive Verfolgung rechtswidriger Taten ist als einheitlicher Zweck anzusehen, weil die Beschränkung der Vorratsspeicherungsrichtlinie auf schwere Straftaten ansonsten jegliche Bedeutung verlöre.

Dasselbe muss für **Auskunftsrechte von Inhabern gewerblicher Schutzrechte** gelten, zu deren Erfüllung der Bundesrat die Nutzung vorratsgespeicherter Verkehrsdaten zulassen will (Ziff. 20 der Stellungnahme des Bundesrats). Auch diese Auskunftsansprüche bezwecken im Kern die Verfolgung strafbarer Verletzungen gewerblicher Schutzrechte. Da es sich dabei jedoch nicht um schwere Straftaten handelt, dürfen vorratsgespeicherte Daten nicht zur Erteilung von Auskünften an Private verwendet werden. Es wäre auch mit dem Verhältnismäßigkeitsgebot unvereinbar, das Telekommunikationsverhalten der Bevölkerung mit der Begründung der Verfolgung schwerer Straftaten erfassen zu lassen (Art. 1 RiL 2006/24/EG), die Daten in der Praxis aber in über 90% der Fälle zur Geltendmachung von Schadensersatzansprüchen durch die Medienindustrie nutzen zu lassen, wie es Konsequenz der Forderung des Bundesrats wäre. Falls man die Richtlinie zur Vorratsdatenspeicherung überhaupt für verbindlich hielte, so hat sie der deutsche Gesetzgeber jedenfalls möglichst grundrechtsfreundlich umzusetzen.[116] Mit den betroffenen Grundrechten besonders unvereinbar wäre es, die anlasslos gespeicherten Kommunikationsdaten für die Verwendung zum Profit der Inhaber gewerblicher Schutzrechte preiszugeben.

Zugriffsrechte der **Nachrichtendienste** und der **Gefahrenabwehrbehörden** verstoßen ebenfalls gegen Art. 1 Abs. 1 RiL 2006/24/EG in Verbindung mit Art. 15 Abs. 1a RiL 2002/58/EG. Aufgabe der Nachrichtendienste und der Gefahrenabwehr ist nicht die Verfolgung schwerer Straftaten. Auf diesen Zweck hat das Europaparlament die Vorratsdatenspeicherung bewusst beschränkt. Im Gegensatz zu früheren Entwürfen hat Art. 1 Abs. 1 RiL 2006/24/EG die präventive „Vorbeugung" oder „Verhütung" von Straftaten nicht mehr zum Gegenstand. Ein Zugriff durch die Nachrichtendienste ist besonders eingriffsintensiv und unangemessen, weil er eine richterliche Prüfung und Anordnung nicht voraussetzt.

§ 113b TKG-E verstößt außerdem dadurch gegen Art. 1 S. 1 der Richtlinie, dass er nur die Verwendung der Daten durch die Telekommunikationsanbieter regelt. Nicht angeordnet ist, dass die Daten auch von den Empfängerbehörden nur zu dem Übermittlungszweck verwendet werden dürfen (**Zweckbindung**). Vorratsgespeicherte Verkehrs- und Bestandsdaten sind dadurch nicht vor einer späteren Kenntnisnahme beispielsweise durch gewerbliche Rechteinhaber oder sonstige Privatpersonen geschützt. Im Wege der Datenübermittlung, der Akteneinsicht oder gemeinsamer Dateien erlaubt das Fachrecht eine Weitergabe und Weiterverwendung übermittelter Daten zu vielfältigen anderen Zwecken. Die Anordnung einer strengen Zweckbindung für vorratsgespeicherte Daten ist wegen der Tiefe des Grundrechtseingriffs jedoch unabdingbar und im Übrigen auch durch die Richtlinie vorgegeben. Die Generalanwältin beim Europäischen Gerichtshof weist zurecht darauf hin, dass sich aus Art. 1 Abs. 1 der Richtlinie ergibt, dass auf Vorrat gespeicherte Daten nur für die Verfolgung schwerer Straftaten verwendet werden dürfen, und dass dies nicht nur für die erstmalige Übermittlung der Daten gilt, sondern auch für ihre weitere Verwendung.[117] Der Gesetzgeber hat daher anzuordnen, dass Empfängerstellen die Daten nur für den Übermittlungszweck nutzen, weitergeben und Dritten zugänglich machen dürfen.

---

116 BVerfGE 113, 273, Rn. 80: „Der Gesetzgeber war jedenfalls verpflichtet, die Umsetzungsspielräume, die der Rahmenbeschluss den Mitgliedstaaten belässt, in einer grundrechtsschonenden Weise auszufüllen."

117 Generalanwältin am EuGH, Schlussanträge vom 18. Juli 2007 in der Rechtssache C-275/06, Rnrn. 124 und 127: „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. [...] Die Richtlinie

Wenn man trotz Art. 1 Abs. 1 RiL 2006/24/EG einen Ermessensspielraum des deutschen Gesetzgebers bei der Bestimmung der zulässigen Verwendungszwecke annehmen wollte, so wäre der Gesetzgeber jedenfalls zur möglichst grundrechtsschonenden Umsetzung der Richtlinie 2006/24/EG verpflichtet.[118] Dies hat das Bundesverfassungsgericht in seiner Entscheidung zum Europäischen Haftbefehl sehr deutlich gemacht.[119] Das Grundgesetz zwingt mithin zu einer möglichst engen Regelung der Verwendung von Vorratsdaten, zumal bereits deren Sammlung verfassungswidrig ist.

Für den Fall, dass die verfassungswidrige Vorratsdatenspeicherung überhaupt eingeführt wird, fordern wir, die Verwendung vorratsgespeicherter Daten auf die Verfolgung schwerer Straftaten zu beschränken.[120] Als schwere Straftaten sind Fälle organisierter oder gewerbsmäßiger Kriminalität anzusehen, in denen eine höhere Strafe als vier Jahre Freiheitsstrafe zu erwarten ist. Wir fordern außerdem ein Verbot der Weiterverwendung übermittelter Vorratsdaten zu anderen Zwecken.

Der Vorschlag der Bundesregierung, die Verwendung der Vorratsdaten zur Erteilung von Auskünften nach **§ 113 TKG** zu erlauben,[121] ist abzulehnen. § 113 TKG erlaubt die Identifizierung von Telekommunikations- und Internetnutzern, aber auch die Abfrage etwa der Passwörter zu E-Mail-Konten. Schon zur Verfolgung von Ordnungswidrigkeiten sowie zu vielfältigen anderen Zwecken dürfen Auskünfte eingeholt werden; eine Eingriffsschwelle ist nicht vorgesehen. Die Bundesregierung erkennt, *„dass die §§ 111 bis 113 TKG Gegenstand eines derzeit beim Bundesverfassungsgericht anhängigen Verfassungsbeschwerdeverfahrens sind (1 BvR 1299/05). Während der Anhängigkeit eines solchen Verfahrens erscheint es ratsam, Änderungen der betroffenen Vorschriften nur dann vorzunehmen, wenn hierzu ein unabweisbares Bedürfnis besteht.*“[122] Die Verwendung der neuen Vorratsdaten auch zur Erteilung von Auskünften nach § 113 TKG freizugeben, würde die praktische Bedeutung des § 113 TKG gerade im Internetbereich vervielfachen, ohne dass ein entsprechendes „unabweisbares Bedürfnis“ behauptet oder gar nachgewiesen wäre. Vielmehr sind die ausufernden Zwecke des § 113 TKG offensichtlich ungeeignet, die Heranziehung anlasslos gespeicherter Kommunikationsdaten der gesamten Bevölkerung zu rechtfertigen.

6. Kosten der Vorratsdatenspeicherung

Der Ausschluss einer Entschädigung für die Kosten der Vorratsdatenspeicherung ist verfassungswidrig.

Die wirtschaftlichen Auswirkungen einer Vorratsspeicherungspflicht sind enorm. Ihre Kosten werden etwa für Internetprovider auf einmalig 25 Mio. Euro und jährlich weitere zehn Mio. Euro Betriebskosten geschätzt.[123] Diese Zusatzkosten könnten die Internetnutzung für den Verbraucher um 15-20% verteuern[124] und zur Einstellung bisher kostenloser Angebote führen. Die Pflicht zur Vorratsdatenspeicherung soll nämlich auch für nichtkommerzielle und private Dienste gelten. Die in der TKÜV vorgesehenen Ausnahmen für kleinere Anbieter sollen keine Anwendung finden. Erfasst werden damit etwa auch öffentliche drahtlose Internetzugänge (sog. WLANs), die von Privatpersonen kostenlos zur Verfügung ge-

---

2006/24 könnte vielmehr dazu führen, den gemeinschaftsrechtlichen Datenschutz in Bezug auf Streitigkeiten wegen Verletzungen des Urheberrechts zu stärken. Es stellt sich dann nämlich selbst in strafrechtlichen Ermittlungsverfahren die Frage, inwieweit es mit dem gemeinschaftsrechtlichen Grundrecht auf Datenschutz vereinbar ist, geschädigten Rechteinhabern Einblick in die Ermittlungsergebnisse zu gewähren, wenn diese auf der Auswertung von auf Vorrat gespeicherten Verkehrsdaten im Sinne der Richtlinie 2006/24 beruhen.“

118 Gola/Klug/Reif, NJW 2007, 2599 (2601).

119 BVerfGE a.a.O.

120 Ähnlich Gola/Klug/Reif, NJW 2007, 2599 (2602): Beschränkung auf die Verfolgung der in § 139 Abs. 3 StGB genannten Straftaten. Vgl. auch Bundesrechtsanwaltskammer, Stellungnahme vom August 2007, http://brak.de/seiten/pdf/Stellungnahmen/2007/Stn31.pdf, 34: „Sofern eine verdachts- und anlassunabhängige Vorratsdatenspeicherung überhaupt verfassungsgemäß ist, wäre für die Erhebung solcher Daten zur Strafverfolgung die gleiche Schwelle wie für die Erhebung von Inhaltsdaten zu fordern.“

121 Ziff. 20 der Gegenäußerung der Bundesregierung, BT-Drs. 16/5846, 234.

122 Ziff. 18 der Gegenäußerung der Bundesregierung, BT-Drs. 16/5846, 231.

123 Rotert, http://www.heise.de/newsticker/meldung/66367.

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

stellt werden. Die vorgeschriebene Datenspeicherung können diese Anbieter nicht leisten; die dazu erforderlichen Einrichtungen werden sie aus finanziellen Gründen nicht anschaffen. Die Vorratsdatenspeicherung wird dadurch zu einer deutlichen Verschlechterung der telekommunikativen Infrastruktur in Deutschland führen, auch im internationalen Vergleich. Projekte wie FON, die zum Aufbau eines flächendeckenden Netzes kostenloser Internetzugänge in Deutschland führen sollten, stehen vor dem Aus.

Viele Anbieter von Internetzugängen speichern bislang keinerlei Verkehrsdaten und müssen die erforderlichen Vorrichtungen erst neu anschaffen. Sie haben zudem mit einer Vielzahl von Auskunftsanforderungen wegen leichter Straftaten im Internet zu rechnen, was erhebliche Personalkosten nach sich ziehen wird. Daneben werden sie eine Vielzahl privater Anfragen wegen (angenommener) Urheberrechtsverletzungen bearbeiten müssen.[125]

Die Verfassungsgerichte Österreichs und Frankreichs haben bereits entschieden, dass eine entschädigungslose Inpflichtnahme der Wirtschaft zu Strafverfolgungszwecken verfassungswidrig ist.[126] In der Tat sind Telekommunikationsunternehmen für den Missbrauch ihrer Dienste durch Straftäter nicht verantwortlich. Sie kontrollieren die Kommunikation ihrer Kunden nicht und dürfen dies wegen des Fernmeldegeheimnisses auch nicht. Die Telekommunikationsüberwachung erfolgt nicht zu ihren Gunsten, sondern ist eine öffentliche Angelegenheit, deren Lasten die Allgemeinheit der Steuerzahler zu tragen hat. In Deutschland ist deshalb aus Art. 12 und Art. 3 GG abzuleiten, dass der Staat Telekommunikationsunternehmen die Mehrkosten einer staatlich angeordneten Vorratsdatenspeicherung voll zu erstatten hat.[127]

Auch der Bundestag hat mit Beschluss vom 16.02.2006 (BT-Dr. 16/545) *„eine angemessene Entschädigung der Telekommunikationsunternehmen für die Inanspruchnahme im Rahmen der Erfüllung hoheitlicher Ermittlungsmaßnahmen im Bereich der Telekommunikation*“ gefordert. Die Verfasser des vorliegenden Regierungsentwurfs räumen in anderem Zusammenhang ein: *„Diese Statistik dient damit in erster Linie hoheitlichen Zwecken, so dass es geboten ist, die Daten von öffentlichen Stellen erheben und übermitteln zu lassen*“ (S. 158). Die Vorratsdatenspeicherung dient ebenfalls „hoheitlichen Zwecken“, soll aber von den Telekommunikationsanbietern vorgenommen werden.

Bislang ist in Deutschland eine (teilweise) Entschädigung für die Mitwirkung an der Telekommunikationsüberwachung nur für Mehrkosten infolge einzelner Überwachungsanordnungen vorgesehen (§ 23 Abs. 1 S. 1 Nr. 2 JVEG, § 20 G10). Diese Entschädigung deckt nur 2% der Kosten ab, die Telekommunikationsunternehmen durch ihre gesetzlich angeordnete Mitwirkung an der Telekommunikationsüberwachung entstehen.[128] Insbesondere eine Entschädigung für gesetzlich vorgeschriebene Überwachungsvorrichtungen und für sonstige Vorhaltekosten (z.B. Personalkosten) ist gegenwärtig ausgeschlossen (§ 110 Abs. 1 und Abs. 9 S. 2 TKG). Viele Anbieter haben nicht einmal eine Überwachungsmaßnahme pro Jahr durchzuführen.

Müsste der Staat für die enormen Kosten der Vorratsdatenspeicherung aufkommen, so würde offenbar, dass der damit verbundene Aufwand zulasten anderer, gezielter Maßnahmen zur Gewährleistung der Sicherheit geht. Es würde sich schon aus Haushaltssicht die Frage stellen, ob die für die Vorratsdatenspeicherung aufgewandten Mittel nicht sinnvoller und effektiver eingesetzt werden könnten. Zum Schutz vor Netzkriminalität beispielsweise versprechen technische Schutzmaßnahmen und Aufklärungskampagnen einen weitaus größeren Erfolg als repressive Maßnahmen.[129]

---

125 Siehe Entwurf eines Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums.

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

127 Näher Breyer, Vorratsspeicherung (2005), www.vorratsspeicherung.de.vu, 277 ff. und 357 ff.

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

129 Näher Breyer, Vorratsspeicherung (2005), www.vorratsspeicherung.de.vu, 338 ff.

Eine Verfassungsbeschwerde gegen den Ausschluss der Kostenerstattung ist anhängig.[130]

XI. § 150 TKG-E [Übergangsvorschrift]

1. Verfrühte Vorratsdatenspeicherung im Internetbereich (§ 150 Abs. 12b TKG-E)

Es ist inakzeptabel und geht über die Vorgaben der Richtlinie 2006/24/EG hinaus, Anbieter von Internetdiensten schon vor dem 15.03.2009 zur Vorratsspeicherung von Verkehrsdaten zu ermächtigen und zu verpflichten.

Nach einer Entscheidung des Bundesgerichtshofs im Fall T-Online (Az. III ZR 40/06) steht rechtskräftig fest, dass das geltende Recht eine Vorratsspeicherung abrechnungsirrelevanter Daten verbietet. Es ist nicht hinnehmbar, dass ohne Umsetzungspflicht schon vor dem 15.03.2009 eine Vorratsspeicherung im Internetbereich erfolgen soll. Dies ist auch nicht erforderlich, um den Anbietern rechtzeitige Investitionen in neue Anlagen zu ermöglichen. Vorratsspeicherungsfähige Anlagen können ohne Weiteres so eingerichtet werden, dass sie eine Vorratsdatenspeicherung erst zum 15.03.2009 aufnehmen. Andere Staaten wie Großbritannien schöpfen die Umsetzungsfrist im Internetbereich voll aus.

Wenn man überhaupt eine Pflicht zur Umsetzung der Richtlinie 2006/46/EG annehmen wollte, so ist der deutsche Gesetzgeber jedenfalls zur möglichst grundrechtsschonenden Umsetzung der Richtlinie verpflichtet.[131] Dies hat das Bundesverfassungsgericht in seiner Entscheidung zum Europäischen Haftbefehl sehr deutlich gemacht.[132] Das Grundgesetz zwingt mithin zu einer Ausschöpfung der europarechtlichen Umsetzungsfristen. Zumal Gerichtsverfahren auf europäischer und deutscher Ebene erwarten lassen, dass die Vorratsdatenspeicherung bis zum 15.03.2009 wieder aufgehoben sein wird und es somit zumindest im Internetbereich nie zu einer Vorratsdatenspeicherung kommen wird.

Wenn überhaupt eine Vorratsdatenspeicherung beschlossen wird, fordern wir, diese im Internetbereich erst ab dem 15.03.2009 zuzulassen.

2. Verfallklausel bei Nichtigerklärung der Richtlinie 2006/24/EG

Für den Fall, dass eine Vorratsdatenspeicherung trotz ihrer Verfassungswidrigkeit eingeführt wird, fordern wir die Aufnahme einer Bestimmung, der zufolge Artikel 2 des vorliegenden Gesetzesentwurfs außer Kraft tritt, sobald der Europäische Gerichtshof die Richtlinie 2006/24/EG für nichtig erklärt hat. Spätestens mit dieser Nichtigerklärung entfällt jeder Anschein einer Legitimität der vorgesehenen Vorratsdatenspeicherung.

XII. Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums

Der Entwurf eines Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums[133] räumt Rechteinhabern zur zivilrechtlichen Verfolgung von Urheber- und anderen Rechtsverletzungen einen Auskunftsanspruch unter anderem gegen Telekommunikationsunternehmen ein. Dazu ist dazu Folgendes anzumerken:

1. Fehlende Beschränkung auf gerichtliche Verfahren

Die umzusetzende Durchsetzungsrichtlinie sieht zur Gewährleistung der Privatsphäre der Betroffenen und der Verhältnismäßigkeit eine Auskunftserteilung ausdrücklich nur im Rahmen gerichtlicher Verfahren

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

131 Gola/Klug/Reif, NJW 2007, 2599 (2601).

132 BVerfGE 113, 273, Rn. 80: „Der Gesetzgeber war jedenfalls verpflichtet, die Umsetzungsspielräume, die der Rahmenbeschluss den Mitgliedstaaten belässt, in einer grundrechtsschonenden Weise auszufüllen."

133 BT-Drs. 16/5048.

und auf gerichtliche Anordnung vor.[134] Der deutsche Gesetzesentwurf verzichtet demgegenüber auf diese Einschränkungen und will jede „offensichtliche Rechtsverletzung“ genügen lassen. Zur Begründung heißt es, *„dass Rechtsinhaber durchaus ein berechtigtes Interesse auf Auskunft haben können, um den Verletzer überhaupt erst ermitteln zu können.“* Rechtsinhabern soll also ein allgemeiner Auskunftsanspruch zum Aufspüren von „Rechtsverletzern“ eingeräumt werden.

Das geht zu weit. Mit guten Gründen haben sowohl das Oberlandesgericht Frankfurt a. M.[135] wie auch das Oberlandesgericht Hamburg[136] eine Auskunftspflicht von Internet-Zugangsvermittlern verneint. Allenfalls, wenn schon ein gerichtliches Verfahren gegen den Verletzer anhängig ist, ist ein Auskunftanspruch angemessen. So regelt es auch die Durchsetzungsrichtlinie. Ein allgemeiner Auskunftanspruch würde dazu führen, dass Verbraucher mit Abmahnungen und Prozessen überzogen werden, wenn sie – selbst in Unkenntnis der Rechtslage – eine „offensichtliche Rechtsverletzung” begehen.

Die geplante Auskunftsregelung geht ohnehin regelmäßig fehl, weil es in der Praxis meist um Urheberrechtsverletzungen geht, zu deren Ahndung Rechteinhaber die Auskunft benötigen, welchem Nutzer eine bestimmte IP-Adresse zugewiesen war. Internet-Zugangsprovider dürfen diese Information nach geltender Rechtslage aber nicht speichern, weil sie abrechnungsirrelevant ist. Der vorliegende Gesetzesentwurf zur Neuregelung der Telekommunikationsüberwachung sieht zwar eine Vorratsspeicherung dieser Daten vor, beschränkt die zulässigen Verwendungszwecke aber auf öffentliche Zwecke (§ 113b TKG-E). Der zivilrechtliche Auskunftsanspruch macht hier also ebenfalls keinen Sinn.

Wir fordern, aus dem Entwurf des „Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums“ die Passage „In Fällen offensichtlicher Rechtsverletzung oder” zu streichen, so dass nur „in Fällen, in denen der Verletzte gegen den Verletzer Klage erhoben hat” verbleibt (§§ 140b Patentgesetz-E, 24b Gebrauchsmustergesetz-E, 19 MarkenG-E, 101 UrhG-E, 46 Geschmacksmustergesetz-E, 37b Sortenschutzgesetz-E).

2. Fehlende Beschränkung auf Rechtsverletzungen in gewerblichem Ausmaß

In der Begründung des vorbenannten Gesetzentwurfs heißt es: *„Auch der in Absatz 2 geregelte Auskunftsanspruch gegenüber Dritten setzt voraus, dass die Rechtsverletzung im geschäftlichen Verkehr erfolgt ist. Damit wird auch hier dem Erwägungsgrund 14 der Richtlinie Rechnung getragen, wonach ein Auskunftsanspruch auf jeden Fall dann vorgesehen werden muss, wenn die Rechtsverletzung in gewerblichem Ausmaß vorgenommen worden ist.“* (Seite 49).

Die Beschränkung der Richtlinie auf Rechtsverletzungen in gewerblichem Ausmaß ist richtig und notwendig, um den erheblichen Grundrechtseingriff zugunsten privater Vermögensinteressen zu rechtfertigen. Man sucht sie im Gesetzentwurf der Bundesregierung aber vergeblich. Der vorgeschlagene Gesetzestext lässt insbesondere im Urheberrecht jegliche Einschränkung vermissen, so dass auch private „Rechtsverletzer“, selbst wenn sie gelegentlich und unabsichtlich handeln, mit Hilfe des Auskunftsanspruchs „aufgespürt“ werden dürften. Auch dies würde dazu führen, dass Verbraucher massenhaft mit Abmahnungen und Prozessen überzogen werden.

Der Gesetzestext reflektiert nicht einmal die Absicht der Bundesregierung, dass nur Rechtsverletzungen „im geschäftlichen Verkehr“ Anlass zu einer Auskunft geben sollen; diese Einschränkung findet sich im Gesetzestext nicht. Darüber hinaus ist die Beschränkung auf den geschäftlichen Verkehr unzureichend. Ein „Handeln im geschäftlichen Verkehr“ ist nach der Rechtsprechung bei allen wirtschaftlichen Tätigkeiten gegeben, die der Förderung eines eigenen oder fremden Geschäftszweckes dienen. Eine Gewinner-

134 Art. 8 Abs. 1 RiL 2004/48/EG lautet: „Die Mitgliedstaaten stellen sicher, dass die zuständigen Gerichte im Zusammenhang mit einem Verfahren wegen Verletzung eines Rechts des geistigen Eigentums auf einen begründeten und die Verhältnismäßigkeit wahrenden Antrag des Klägers hin anordnen können, dass Auskünfte [...] erteilt werden [...]“.

135 Urteil vom 25.1.2005 – 11 U 51/04, GRUR-RR 2005, 147.

136 Urteil vom 28.4.2005 – 5 U 156/04, GRUR-RR 2005, 209.

zielung ist nicht erforderlich, nicht einmal ein Handeln gegen Entgelt. Damit geht der Begriff erheblich weiter als der Tatbestand einer „Rechtsverletzung in gewerblichem Ausmaß“.

Eine Rechtsverletzung in gewerblichem Ausmaß setzt erstens ein gewerbsmäßiges Handeln voraus und zweitens, dass die jeweilige Rechtsverletzung für sich genommen ein gewerbsmäßiges Ausmaß erreicht. Diese Einschränkung ist gerade vor dem Hintergrund unverzichtbar, dass der Auskunftsanspruch bereits im Vorfeld eines Gerichtsverfahrens eingeräumt werden soll.

Verwendet ein Schüler beispielsweise urheberrechtswidrig eine geschützte Hintergrundgrafik auf seiner Homepage, weil er sich über die Rechtslage nicht im klaren ist, so liegt ein „Handeln im geschäftlichen Verkehr“ bereits dann vor, wenn der Schüler auf seiner Homepage Werbebanner einblenden lässt oder Hilfe beim Rasenmähen anbietet. Eine „Rechtsverletzung in gewerblichem Ausmaß“, die einen Auskunftsanspruch rechtfertigen könnte, ist hingegen in solchen Fällen sicherlich nicht gegeben.

Im Entwurf des „Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums“ muss daher festgelegt werden, dass ein Auskunftsanspruch nur zur Ermittlung von Rechtsverletzungen in gewerblichem Ausmaß besteht. Die Passage „in Fällen, in denen der Verletzte gegen den Verletzer Klage erhoben hat“ muss daher richtig lauten: „in Fällen, in denen der Verletzte gegen den Verletzer wegen einer in gewerblichem Ausmaß begangenen Rechtsverletzung Klage erhoben hat“ (insbesondere § 101 UrhG-E).

C. Zusammenstellung der Forderungen

I. § 53b StPO-E [Schutz von Berufsgeheimnisträgern]

Wir fordern, das Erhebungs- und Verwertungsverbot des § 53b Abs. 1 StPO einheitlich auf alle Zeugnisverweigerungsberechtigten nach den §§ 52-53a StPO zu erstrecken.

II. § 100a StPO-E [Telekommunikationsüberwachung]

1. Anwendungsbereich: Wir fordern, den staatlichen Zugriff auf Informationen über die Kommunikation und die Kommunizierenden („Verkehrsdaten“, „Bestandsdaten“) den gleichen Voraussetzungen zu unterwerfen wie den Zugriff auf die Inhalte der Kommunikation. Dazu sind Verkehrs- und Bestandsdaten in den Anwendungsbereich der §§ 100a, 100b StPO einzubeziehen.
2. Eingriffsvoraussetzungen: Wir fordern, den Anwendungsbereich des § 100a StPO anhand der zu erwartenden Strafe zu regeln. Der heimliche Zugriff auf die Telekommunikation zwecks Strafverfolgung ist auf Fälle organisierter oder gewerbsmäßiger Kriminalität zu beschränken, in denen eine höhere Strafe als vier Jahre Freiheitsstrafe zu erwarten ist.
3. Fehlende Erfolgskontrolle (§ 100b Abs. 6 StPO-E): Wir fordern, zumindest die noch im Referentenentwurf vorgesehenen Informationen über Umfang und Ergebnis der Überwachungsmaßnahmen in die Statistik nach § 100b Abs. 6 StPO-E aufzunehmen.

III. § 100g StPO-E [Erhebung von Verkehrsdaten]

1. Fehlende Beschränkung auf schwere Straftaten: Falls die Richtlinie zur Vorratsdatenspeicherung überhaupt umgesetzt wird, fordern wir, den Zugriff auf vorratsgespeicherte Verkehrs- und Bestandsdaten auf die Verfolgung schwerer Straftaten zu beschränken, wie es die Richtlinie vorsieht. Als schwere Straftaten sind Fälle organisierter oder gewerbsmäßiger Kriminalität anzusehen, in denen eine höhere Strafe als vier Jahre Freiheitsstrafe zu erwarten ist.
2. Fehlende Bestimmung der maßgeblichen Straftaten: Wir fordern eine klare Umschreibung der maßgeblichen Straftaten durch Bezugnahme auf die jeweils zu erwartende Strafe.
3. Eingriffsschwelle: Wir fordern, den staatlichen Zugriff auf Informationen über die Kommunikation und die Kommunizierenden („Verkehrsdaten“, „Bestandsdaten“) den gleichen Voraussetzungen zu unterwerfen wie den Zugriff auf die Inhalte der Kommunikation. Der Zugriff zwecks Strafverfolgung sollte dabei beschränkt sein auf Fälle organisierter oder gewerbsmäßiger Kriminalität, in denen eine höhere Strafe als vier Jahre Freiheitsstrafe zu erwarten ist.
4. Bewegungsprofile bei betriebsbereiten Mobiltelefonen: Falls § 100g StPO neben § 100a StPO überhaupt beibehalten wird, fordern wir, diesen weiterhin auf die im Falle einer Verbindung anfallenden Verkehrsdaten zu beschränken.
5. Erweiterung in Datenerhebungsbefugnis: Falls § 100g StPO überhaupt beibehalten wird, fordern wir, dass die Vorschrift weiterhin auf Verkehrsdaten beschränkt bleibt, die der Anbieter ohnehin im Zuge der Bereitstellung und Abrechnung des Dienstes speichert.
6. Ausweitung auf inhaltsbezogene Verkehrsdaten: Wir fordern, die niedrigere Eingriffsschwelle des § 100g StPO – wenn überhaupt – weiterhin nur für die in § 100g Abs. 3 StPO abschließend bestimmten Verkehrsdaten beizubehalten.
7. Fehlende Erfolgskontrolle: Die Erfolgskontrolle nach § 100b Abs. 4 S. 2 StPO-E muss auch für den Zugriff auf die näheren Umstände der Telekommunikation gelten. Die Rückmeldungen analog § 100b Abs. 4 S. 2 StPO-E müssen auch in die Statistik nach § 100g Abs. 4 StPO-E einfließen.
8. Verkehrsdaten über Unbeteiligte: § 100g Abs. 1 S. 2 StPO muss beibehalten werden.

IV. § 101 StPO-E [Allgemeine Verfahrensregelungen bei verdeckten Ermittlungsmaßnahmen]

1. Benachrichtigung der von Telekommunikationsüberwachung Betroffenen: Wir fordern die Streichung des § 101 Abs. 4 S. 4 und 5 StPO und die Sicherstellung der Benachrichtigung der Betroffenen durch Aufnahme einer Regelung über elektronische Benachrichtigungen.
2. Frist zur gerichtlichen Überprüfung: Wir fordern die Streichung der vorgesehenen Zweiwochenfrist.
3. Folgen rechtswidriger Ermittlungsmaßnahmen: Wir fordern eine Pflicht zur sofortigen Vernichtung sowie ein Verwertungsverbot für Informationen, die durch rechtswidrige verdeckte Ermittlungsmaßnahmen erlangt worden sind. Ferner fordern wir die Aufnahme eines ausdrücklichen Anspruchs der von rechtswidrigen Ermittlungsmaßnahmen Betroffenen auf angemessene Entschädigung.

V. § 110 StPO-E [Durchsicht von Papieren]

Wir fordern eine normenklare und vor allem nicht überschießende Umsetzung der Cybercrime-Konvention in § 110 Abs. 3 StPO-E.

VI. § 96 TKG-E [Verkehrsdaten]

Wir fordern, die ursprüngliche Fassung des § 96 Abs. 2 S. 1 TKG wieder herzustellen.

VII. § 110 TKG-E [Umsetzung von Überwachungsmaßnahmen, Erteilung von Auskünften]

Wir fordern, die vorgesehene Ausweitung des § 110 TKG zu streichen.

VIII. § 111 TKG-E [Daten für Auskunftsersuchen der Sicherheitsbehörden]

1. Identifizierungspflicht für Telefon, Handy und Internet (§ 111 Abs. 1 TKG): Wir fordern die Aufhebung des § 111 Abs. 1 TKG.
2. Zwangserhebung auch von Internet-Kundendaten und von Gerätenummern (§ 111 Abs. 1 S. 1 Nr. 1 und 5 TKG-E): Für den Fall, dass § 111 TKG nicht gänzlich gestrichen wird, fordern wir dessen unveränderte Beibehaltung bis zur Entscheidung des Bundesverfassungsgerichts über die anhängige Verfassungsbeschwerde.
3. Online-Identifizierung auch von E-Mail-Nutzern (§§ 111 Abs. 1 S. 3, 112 TKG-E): Für den Fall, dass § 111 TKG nicht gänzlich gestrichen wird, fordern wir dessen unveränderte Beibehaltung bis zur Entscheidung des Bundesverfassungsgerichts über die anhängige Verfassungsbeschwerde.
4. Vorratsspeicherung von Bestandsdaten (§ 111 Abs. 4 TKG-E): Wir fordern die Streichung des § 95 Abs. 3 TKG und des § 111 Abs. 4 TKG-E, andernfalls jedenfalls die Beschränkung der Speicherdauer auf sechs Monate.
5. Kostenerstattung (§ 111 Abs. 5 TKG-E): Der Ausschluss einer Entschädigung für die Vorratsdatenerhebung ist verfassungswidrig.

IX. §§ 112, 113 TKG [Auskünfte über Bestandsdaten]

Wir fordern, die Abfrage von Bestandsdaten nach den §§ 112, 113 TKG auf die Verfolgung schwerer Straftaten zu beschränken, wie es die Richtlinie 2006/24/EG und das deutsche Verfassungsrecht vorgeben. Außerdem fordern wir, die Anzahl der Auskunftsanforderungen nach § 113 TKG statistisch erfassen zu lassen.

X. § 113a TKG-E [Speicherungspflichten für Verkehrsdaten] und § 113b TKG-E [Verwendung der nach § 113a gespeicherten Daten]

1. Verfassungswidrigkeit: Wir fordern, Artikel 2 des vorliegenden Gesetzentwurfs zu streichen und die anstehende Entscheidung des Bundesverfassungsgerichts zur Vorratsspeicherung von Telekommunikations-Bestandsdaten sowie die Entscheidung des Europäischen Gerichtshofs über die Wirksamkeit der Richtlinie 2006/24/EG abzuwarten, bevor der massive Grundrechtseingriff einer Protokollierung des Telekommunikationsverhaltens der gesamten Bevölkerung beschlossen wird.
2. E-Mail-Dienste (§ 113a Abs. 3 TKG-E): Falls eine Vorratsdatenspeicherung trotz ihrer Verfassungswidrigkeit beschlossen wird, fordern wir, die Speicherung von IP-Adressen in § 113a Abs. 3 TKG-E nicht vorzusehen.

3. Anonymisierungsdienste (§ 113a Abs. 6 TKG-E): Wir fordern, § 113a Abs. 6 TKG zu streichen.
4. Überschießende Speicherfrist (§ 113a Abs. 2 TKG-E): Falls eine Vorratsdatenspeicherung trotz ihrer Verfassungswidrigkeit beschlossen wird, fordern wir die unverzügliche Löschung der gespeicherten Daten nach Ablauf von sechs Monaten.
5. Verwendung der Vorratsdaten (§ 113b TKG-E): Für den Fall, dass die verfassungswidrige Vorratsdatenspeicherung überhaupt eingeführt wird, fordern wir, die Verwendung vorratsgespeicherter Daten auf die Verfolgung schwerer Straftaten zu beschränken. Als schwere Straftaten sind Fälle organisierter oder gewerbsmäßiger Kriminalität anzusehen, in denen eine höhere Strafe als vier Jahre Freiheitsstrafe zu erwarten ist. Wir fordern außerdem ein Verbot der Weiterverwendung übermittelter Vorratsdaten zu anderen Zwecken.
6. Kosten der Vorratsdatenspeicherung: Der Ausschluss einer Entschädigung für die Kosten der Vorratsdatenspeicherung ist verfassungswidrig.

XI. § 150 TKG-E [Übergangsvorschrift]

1. Verfrühte Vorratsdatenspeicherung im Internetbereich (§ 150 Abs. 12b TKG-E): Wenn überhaupt eine Vorratsdatenspeicherung beschlossen wird, fordern wir, dass diese im Internetbereich erst ab dem 15.03.2009 erfolgen darf.
2. Verfallklausel bei Nichtigerklärung der Richtlinie 2006/24/EG: Für den Fall, dass eine Vorratsdatenspeicherung trotz ihrer Verfassungswidrigkeit eingeführt wird, fordern wir die Aufnahme einer Bestimmung, der zufolge Artikel 2 des vorliegenden Gesetzesentwurfs außer Kraft tritt, sobald der Europäische Gerichtshof die Richtlinie 2006/24/EG für nichtig erklärt hat

XII. Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums

1. Wir fordern, aus dem Entwurf des „Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums“ die Passage „In Fällen offensichtlicher Rechtsverletzung oder” zu streichen, so dass nur „in Fällen, in denen der Verletzte gegen den Verletzer Klage erhoben hat” verbleibt (§§ 140b Patentgesetz-E, 24b Gebrauchsmustergesetz-E, 19 MarkenG-E, 101 UrhG-E, 46 Geschmacksmustergesetz-E, 37b Sortenschutzgesetz-E).
2. Im Entwurf des „Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums“ muss festgelegt werden, dass ein Auskunftsanspruch nur zur Ermittlung von Rechtsverletzungen in gewerblichem Ausmaß besteht. Die Passage „in Fällen, in denen der Verletzte gegen den Verletzer Klage erhoben hat“ muss daher richtig lauten: „in Fällen, in denen der Verletzte gegen den Verletzer wegen einer in gewerblichem Ausmaß begangenen Rechtsverletzung Klage erhoben hat“ (insbesondere § 101 UrhG-E).

6. September 2007

Dr. Patrick Breyer (P.Breyer @ vorratsdatenspeicherung.de)

in Zusammenarbeit mit

Arbeitskreis Vorratsdatenspeicherung

Netzwerk Neue Medien e.V.

Neue Richtervereinigung e.V.