

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

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

Zusammenfassung

Der Referentenentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung sieht vor, Telekommunikationsunternehmen ab Herbst 2007 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 sollen 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 werden. 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 grundsätzlich 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 Nichtigklärung 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.....	4
I. Inhalt und Auswirkungen des Gesetzesentwurfs	4
II. Rechtliche Problematik.....	5
III. Keine Pflicht zur Umsetzung der Richtlinie 2006/24/EG	6
1. Formelle Rechtswidrigkeit.....	6
2. Materielle Rechtswidrigkeit.....	8
3. Schwere und Offensichtlichkeit der Fehler.....	8
4. Fehlende Umsetzungspflicht nach Völkerrecht	9
IV. Position des Deutschen Bundestags.....	9
V. Rechtsprechung des Bundesverfassungsgerichts	10
VI. Lösung.....	12
VII. Einordnung des Gesetzesentwurfs in die Sicherheitspolitik der letzten Jahre.....	12
B. Zu einzelnen Vorschriften des Gesetzesentwurfs.....	13
I. § 100a StPO-E [Telekommunikationsüberwachung]	13
1. Anwendungsbereich.....	13
2. Eingriffsvoraussetzungen.....	14
II. § 100g StPO-E [Erhebung von Verkehrsdaten].....	15
1. Fehlende Beschränkung auf schwere Straftaten.....	15
2. Fehlende Bestimmung der maßgeblichen Straftaten.....	16
3. Eingriffsschwelle	16
4. Bewegungsprofile bei betriebsbereiten Mobiltelefonen	17
5. Erweiterung in Datenerhebungsbefugnis	17
6. Ausweitung auf inhaltsbezogene Verkehrsdaten	18
7. Fehlende Erfolgskontrolle.....	18
8. Verkehrsdaten über Unbeteiligte.....	18
9. Beteiligung des Bundesrats.....	19
III. § 101 StPO-E [Allgemeine Verfahrensregelungen bei verdeckten Ermittlungsmaßnahmen]	19
1. Benachrichtigung der von Telekommunikationsüberwachung Betroffenen.....	19
2. Frist zur gerichtlichen Überprüfung.....	19
3. Folgen rechtswidriger Ermittlungsmaßnahmen	20
IV. § 110 StPO-E [Durchsicht von Papieren]	20
V. § 96 TKG-E [Verkehrsdaten].....	21
VI. § 110a TKG-E [Speicherungspflichten für Verkehrsdaten] und § 110b TKG-E [Verwendung der nach § 110a gespeicherten Daten]	22
1. Verfassungswidrigkeit	22
a) Mangelnde Effektivität	22
b) Risiko falscher Verdächtigung	23

c) Abschreckung erwünschten Verhaltens.....	24
d) Dambruch	24
e) Ergebnis	25
2. Anonymisierungsdienste	26
3. Überschießende Speicherfrist.....	27
4. Eigene Auskunftregelung	27
5. Verwendung der Vorratsdaten	27
6. Kosten der Vorratsdatenspeicherung	27
VII. § 111 TKG-E [Daten für Auskunftsersuchen der Sicherheitsbehörden]	29
1. Identifizierungspflicht für Telefon, Handy und E-Mail (§ 111 Abs. 1 TKG).....	29
2. Zwangserhebung auch von E-Mail-Kundendaten und von Gerätenummern (§ 111 Abs. 1 S. 1 Nr. 5 und S. 3 TKG-E).....	29
3. Vorratsspeicherung von Bestandsdaten (§ 111 Abs. 4 TKG-E)	30
4. Kostenerstattung (§ 111 Abs. 5 TKG-E).....	30
VIII. §§ 112, 113 TKG [Auskünfte über Bestandsdaten]	30
IX. § 150 TKG-E [Übergangsvorschriften]	31
1. Recht zur Vorratsdatenspeicherung im Internetbereich (§ 150 Abs. 11a TKG-E)	31
2. Verfallklausel bei Nichtigerklärung der Richtlinie 2006/24/EG.....	31
X. Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums	32
1. Fehlende Beschränkung auf anhängige Gerichtsverfahren.....	32
2. Fehlende Beschränkung auf gewerbsmäßige Rechtsverletzer	33

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 (§§ 110a, 110b TKG). 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 will der Gesetzesentwurf das Angebot anonymer E-Mail-Postfächer verbieten (§ 111 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 minutiös 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 Berufsgeheimnistägern 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 Vgl. S. 146 des Referentenentwurfs.

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 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“.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 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.

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

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.

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

Am 06.07.2006 hat Irland Nichtigkeitsklage gegen die Richtlinie 2006/24/EG eingereicht⁸ mit der Begründung, die Vorratsdatenspeicherung diene einer verbesserten Strafverfolgung und habe deswegen nicht im Wege einer EG-Richtlinie beschlossen werden können.

Am 03.08.2006 hat der Wissenschaftliche Dienst des Bundestages ein Rechtsgutachten vorgelegt⁹, 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.

Bei dem Bundesverfassungsgericht ist derzeit eine Verfassungsbeschwerde gegen Vorschriften des Telekommunikationsgesetzes (§§ 95 Abs. 3, 111-113 TKG) anhängig¹⁰, die Telekommunikationsanbieter zur Erhebung und Vorratsspeicherung von Telekommunikations-Bestandsdaten verpflichten.

III. Keine Pflicht zur Umsetzung der Richtlinie 2006/24/EG

Art. 2 des vorliegenden Gesetzesentwurfs ist durch die Richtlinie 2006/24/EG jedenfalls insoweit nicht vorgegeben als er über die Vorgaben der Richtlinie hinaus geht. Dies ist insbesondere bei § 111 TKG-E der Fall. Die Richtlinie 2006/24/EG 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. Auch eine Verpflichtung von Anonymisierungsdiensten zur Vorratsdatenspeicherung ist in der Richtlinie nicht vorgesehen.

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

Der Referentenentwurf vertritt unter Hinweis auf Art. 242 EG die Auffassung (S. 64), bis zur Entscheidung des Europäischen Gerichtshofs über Irlands Nichtigkeitsklage¹¹ 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 grundsätzlich die Vermutung der Rechtmäßigkeit.¹² 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.¹³ In einem solchen Fall ist der Rechtsakt von vornherein inexistent und erzeugt keine Befolungs- oder Umsetzungspflicht.

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

1. 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.

8 Az. C-301/06.

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

10 1 BvR 1299/05, <http://www.tkg-verfassungsbeschwerde.de>.

11 Az. C-301/06

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

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

Kommission, Europaparlament und Rat stützen die Richtlinie 2006/24/EG auf Art. 95 EG als Rechtsgrundlage. Sie begründen dies mit Rechtsgutachten, die im Auftrag der Kommission¹⁴ und des Rates¹⁵ 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.¹⁶ Im Juli 2006 reichte Irland beim Europäischen Gerichtshof eine Nichtigkeitsklage gegen die Richtlinie zur Vorratsdatenspeicherung ein (Az. C-301/06). Stützen kann es sich dabei auf die zwischenzeitlich ergangene Entscheidung des Europäischen Gerichtshofs zur Fluggastdatenübermittlung in die USA.¹⁷ 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.“*¹⁸

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.¹⁹

Der Generalanwalt hat 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.²⁰ Er hat sogar ausdrücklich auf die Vorratsdatenspeicherung Bezug genommen.²¹ Dies verdeutlicht, dass es auch der Richtlinie zur Vorratsdatenspeicherung an einer Rechtsgrundlage mangelt.

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

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

16 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.“

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

18 EuGH, Urteil vom 30.05.2006, Az. C-317/04 und C-318/04, Abs. 57.

19 Simitis, NJW 2006, 2011 (2013); Westphal, EuZW 2006, 555 (557).

20 Abs-Nr. 160 der Schlussanträge vom 22.11.2005.

21 Abs-Nr. 160 der Schlussanträge vom 22.11.2005.

2. Materielle Rechtswidrigkeit

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

Einen Teil des primären Gemeinschaftsrechts stellen die Gemeinschaftsgrundrechte dar, die der Europäische Gerichtshof als „allgemeine Grundsätze des Gemeinschaftsrechts“²² aus den Rechtstraditionen der Mitgliedstaaten entwickelt hat. Der Europäische Gerichtshof wendet dabei in der Regel die Europäische Menschenrechtskonvention (EMRK) in ihrer Auslegung durch den Europäischen Gerichtshof für Menschenrechte an.²³ Entsprechend Art. 8 EMRK hat der Europäische Gerichtshof beispielsweise den Schutz der Privatsphäre als Gemeinschaftsgrundrecht anerkannt.²⁴

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.²⁵ Das Interesse des Staates muss gegenüber den Interessen des Einzelnen an der Achtung seiner Privatsphäre abgewogen werden.²⁶ Eingriffe sind zwar nicht auf das unerlässliche Maß beschränkt, aber ein bloßes Nützlich- oder Wünschenswertsein genügt nicht.²⁷

Die Abwägung ergibt, dass eine Speicherung des Kommunikationsverhaltens der gesamten Bevölkerung grob unverhältnismäßig ist. Die Strafverfolgungsbehörden würden nur einen kleinen Bruchteil (etwa 0,0004%²⁸) der anfallenden Kommunikationsdaten jemals nachfragen, während mehr als 99% der Betroffenen²⁹ vollkommen unschuldig, unverdächtig und ungefährlich sind.

3. 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.

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 Fluggastdaten-

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

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

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

25 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.

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

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

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

29 Schaar, <http://www.heise.de/ct/aktuell/meldung/62231>.

übermittlung in die USA.³⁰ Die dortigen Erwägungen sind wörtlich auf die Vorratsdatenspeicherung übertragbar. Die fehlende Rechtsgrundlage steht der Richtlinie 2006/24/EG „auf die Stirn geschrieben“.

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

4. 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 nämlich nicht gedeckt³¹, seien sie inexistent oder nicht. Die mit der Umsetzung befassten Staatsorgane sind aus verfassungsrechtlichen Gründen gehindert, diese Rechtsakte in Deutschland anzuwenden³², 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.“³³

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.³⁴

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.

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.“

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

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

31 BVerfGE 89, 155 (188).

32 BVerfGE 89, 155 (188).

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

34 BVerfGE 89, 155 (188).

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 einzu beziehen, 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 dieser veränderten Umstände kann an dem Bundestagsbeschluss vom 16.02.2006 weder politisch noch rechtlich festgehalten werden.

Im Übrigen widerspricht der vorliegende Referentenentwurf selbst diesem Bundestagsbeschluss, weil der Gesetzentwurf in Bezug auf E-Mail- und Anonymisierungsdienste über die Mindestvorgaben der Richtlinie 2006/24/EG hinaus geht.

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.

Dies gilt zum einen für das vom Bundesverfassungsgericht ausgesprochene „außerhalb statistischer Zwecke bestehende strikte Verbot der Sammlung personenbezogener Daten auf Vorrat“.³⁵ Entgegen der Ansicht der Verfasser des Referentenentwurfs (S. 69) gilt dieses Verbot nicht nur für eine Vorratsdatenspeicherung „zu unbestimmten oder noch nicht bestimmbar Zwecken“. Diese Einschränkung hat das Bundesverfassungsgericht in seinem Urteil zur Rasterfahndung aufgegeben und nicht mehr genannt.³⁶ Stattdessen hat das Gericht präzisiert, dass eine Vorratsdatenspeicherung nur zu statistischen Zwecken zulässig ist.

Unabhängig davon sieht der Referentenentwurf durchaus eine Datensammlung „zu unbestimmten oder noch nicht bestimmbar Zwecken“ im Sinne der Rechtsprechung des Bundesverfassungsgerichts vor. Eine allgemeine Aufgabenbeschreibung (z.B. „zu Strafverfolgungszwecken“, „zu Zwecken der Gefahrenabwehr“) stellt keine hinreichende Zweckbestimmung in diesem Sinne dar. 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.

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

36 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.“

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.“³⁷ „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.“³⁸

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 Referentenentwurfs 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.“³⁹

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.⁴⁰ Mit § 110a TKG-E ordnet der Staat die Aufzeichnung und Speicherung von Daten an, auf die er sich gleichzeitig Zugriffsrechte einräumt (§ 100g StPO). Dieses bloße „Outsourcing“ der Datenspeicherung an Private ist für die verfassungsrechtliche Beurteilung unerheblich. Entscheidend ist, dass die staatliche Speicherpflicht die spätere Kenntnisnahme der Daten durch staatliche Stellen ermöglicht.⁴¹ 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. Vorausgesetzt sind vielmehr eine Straftat von erheblicher Bedeutung, ein konkreter Tatverdacht und eine hinreichend sichere Tatsachenbasis.“⁴²*

Mit § 110a TKG-E ordnet der Staat eine Erfassung und Vorhaltung von Verbindungsdaten an, die nur allgemein der Strafverfolgung dienen soll (§ 110b 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

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

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

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

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

41 BVerfGE 107, 299 (314).

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

*Bestreben nach möglichst großer Effektivität der Polizeigewalt und Erleichterung der polizeilichen Überwachung der Bevölkerung widersprüche den Prinzipien des freiheitlichen Rechtsstaates.*⁴³

Die Vorratsdatenspeicherung geht weit über die Aufnahme von 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 straffprozessualen 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.“*⁴⁴

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.

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. 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 Be-

43 BVerwG, 1 C 57.66 vom 09.02.1967.

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

fugnissen der Eingriffsbehörden unabhängig ist.⁴⁵ 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.⁴⁶

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.

B. Zu einzelnen Vorschriften des Gesetzesentwurfs

I. § 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.

Wenn verbreitet angenommen wird, der Zugriff auf Kommunikationsinhalte sei eingriffintensiver als der Zugriff auf Verkehrsdaten, beruht dies auf einem Irrtum. Die Eingriffstiefe bestimmt sich laut Bundesverfassungsgericht nicht nach der Art der Daten, sondern nach deren Nutzbarkeit und Verwendungsmöglichkeiten.⁴⁷ 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.⁴⁸ Die österreichische Strafprozessordnung verfolgt diesen richtigen Ansatz bereits (§ 149a öStPO).

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

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

47 BVerfGE 65, 1 (45).

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

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 unmittelbaren Zugriff). Die Identität der Kommunikationspartner ist integraler Bestandteil der Kommunikation selbst. Dies wird näher erläutert auf Seite 30 dieser Stellungnahme.

2. 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 Strafverurteilung 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 benutzen 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.⁴⁹

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).

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

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.

II. § 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).

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 [...] Straftaten unter Einsatz von Telekommunikationseinrichtungen angemessen zu berücksichtigen“ haben.⁵⁰ 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.“⁵¹ Eine am Telefon ausgesprochene Beleidigung ist ebenso wenig eine schwere Straftat wie jede andere Beleidigung. Auch die in der Begründung des Referentenentwurfs angeführten Zweckmäßigkeitsargumente gegen eine Beschränkung auf die Verfolgung schwerer Straftaten (S. 115) überzeugen nicht, zumal der Referentenentwurf selbst darlegt, dass eine solche Beschränkung möglich ist.

Der Begriff der „schweren Straftaten“ beschreibt, in die Terminologie des Bundesverfassungsgerichts übersetzt, Straftaten im oberen Kriminalitätsbereich.⁵² 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 Bagatelldelikt 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.⁵³ Insoweit ist der neue Absatz 1a dieses Artikels zu beachten. Danach sind diejenigen Datentypen vor wei-

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

51 Pressemitteilung vom 21.02.2006, <http://www.bmj.bund.de>.

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

53 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 e-

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

Falls die Richtlinie zur Vorratsdatenspeicherung überhaupt umgesetzt wird, fordern wir, den Zugriff auf vorratsspeicherte Verkehrs- und Bestandsdaten auf die Verfolgung schwerer Straftaten zu beschränken, wie es die Richtlinie vorsieht.

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 Strafraum 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. 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. Gerade die jeweiligen Nutzungs- und Verwendungsmöglichkeiten bestimmen nach der Rechtsprechung des Bundesverfassungsgerichts die Schutzwürdigkeit eines Datums.⁵⁴

elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist.“

54 BVerfGE 65, 1 (45).

Die verbreitete Annahme, der staatliche Zugriff auf die näheren Umstände der Telekommunikation wiege weniger schwer als der Zugriff auf Telekommunikationsinhalte, ist unzutreffend.⁵⁵ 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.“*⁵⁶

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. Der Zugriff zwecks Strafverfolgung sollte dabei beschränkt sein auf Fälle organisierter 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.

Falls § 100g StPO überhaupt beibehalten wird, fordern wir, dass dieser weiterhin nur für die im Falle einer Verbindung anfallenden Verkehrsdaten gilt.

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 Referentenentwurfs räumt ein, dass diese Gesetzeslage auch unter Berücksichtigung der Cybercrime-Konvention beibehalten werden kann (S. 60 und 109 f.).

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

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

§ 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 Referentenentwurf 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 Eingriffsschwelle.

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

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 Referentenentwurf nennt keine praxisrelevanten Beispiele „sonstiger Verkehrsdaten“, für welche die Eingriffsvoraussetzungen des § 100g StPO-E angemessen wären (S. 111).

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-E sieht 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.

9. Beteiligung des Bundesrats

Ausweislich der Begründung (S. 70) unterliegt das geplante Gesetz der Mitbestimmung des Bundesrates, weil es die Länder in § 100b Abs. 5 und 6 sowie in § 100g Abs. 4 StPO-E abweichungsfest zur Erhebung von Statistiken verpflichtet.

Das Mitbestimmungsrecht des Bundesrates, der den Interessen der Eingriffsbehörden erfahrungsgemäß ein unangemessenes Gewicht zumisst, lässt eine weitere Verschärfung des Gesetzesentwurfs im Laufe des Gesetzgebungsverfahrens erwarten, und zwar auch in Bereichen, welche die Länder nicht berühren.

Wir fordern daher, entweder die zustimmungsbedürftigen Regelungen des vorliegenden Gesetzesentwurfs in einen gesonderten Gesetzesentwurf auszugliedern oder aber Abweichungen durch die Länder zuzulassen.

III. § 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 Justizvergütungs- 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).

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 Wei-

se 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.

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. 138). 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.

IV. § 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.

Unbestimmt ist die Regelung, soweit von „Betroffenen“ die Rede ist. 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 besondere Anordnung bedarf, über die im Regelfall der Richter entscheidet.

Über die Konvention hinaus geht § 110 Abs. 3 StPO-E in mehrfacher Hinsicht. 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 nur für Fälle, in denen die Strafverfolgungsbehörde nach bestimmten Daten suchen. Diese Einschränkungen sucht man in § 110 Abs. 3 StPO-E vergeblich. Unter anderem soll die Vorschrift für alle „elektronischen Speichermedien“ gelten und nicht nur für „Computersysteme“. Sie würde also beispielsweise auch Audio-CDs abdecken. § 110 Abs. 3 StPO-E soll allgemein und nicht nur dann gelten, wenn die Behörden vergeblich nach bestimmten Daten gesucht haben. Schließlich erlaubt Art. 19 Abs. 2 CCC nur die Durchsuchung von Datenbeständen, die „von dem ersten System aus recht-

mäßig 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. 136). 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.

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

V. § 96 TKG-E [Verkehrsdaten]

Es ist zu begrüßen, dass der vorliegende Gesetzesentwurf die ursprüngliche Fassung des § 96 Abs. 2 S. 1 TKG wieder herstellen soll.

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

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 Auskunft- 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“. Es darf hier keine weitere Vorratsdatenspeicherung durch die Hintertür eingeführt werden, zumal dies nach der Entwurfsbegründung nicht beabsichtigt war.

§ 96 Abs. 2 TKG sollte stattdessen wie folgt 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.

VI. § 110a TKG-E [Speicherungspflichten für Verkehrsdaten] und § 110b TKG-E [Verwendung der nach § 110a 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 2005⁵⁷ 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.

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.“*⁵⁸

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 erfolversprechender Ermittlungen abschneidet. Klaus Jansen, Vorsitzender des Bundes Deutscher Kriminalbeamter, klagt bereits heute: *„Da es sich herumgesprochen hat, dass Telefongesprä-*

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

58 Pressemitteilung vom 02.06.2005, <http://snipurl.com/m82z>.

*che relativ leicht abgehört werden können, reden die Verdächtigen nur noch selten offen am Telefon“.*⁵⁹ 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 der Daten zu anderen Zwecken verworfen. Es hat dies begründet mit dem Argument, die Regelung beeinträchtigt die „Bereitschaft, wahrheitsgemäße Angaben zu machen“ und gefährde damit die „Funktionsfähigkeit der amtlichen Statistik“.⁶⁰ In ähnlicher Weise gefährdet die Vorratsspeicherung von Verkehrsdaten die Funktionsfähigkeit der Strafverfolgung, die auf die Möglichkeit einer erfolgreichen Telekommunikationsüberwachung angewiesen ist.

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, Fehlernährung 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.⁶¹ Es ist bekannt, dass 89% der Fälle organisierter Kriminalität einen internationalen Bezug aufweisen.⁶² In 80% der von der deutschen „Zentralstelle für anlassunabhängige Recherchen in Datennetzen“ eingeleiteten strafrechtlichen Ermittlungsverfahren sind Zugriffe auf im Ausland gespeicherte Verkehrsdaten erforderlich.⁶³ 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.⁶⁴ 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 ver-

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

60 BVerfGE 65, 1 (50 und 64).

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

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

63 BMI/BMJ, Sicherheitsbericht 2001, 203.

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

dächtigt 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.⁶⁵ 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.“⁶⁶ Die ehemalige Präsidentin des Bundesverfassungsgerichts Jutta Limbach wird noch deutlicher: „Eine demokratische politische Kultur lebt von der Meinungsfreiheit 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.“⁶⁷

d) Dambruch

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.

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

65 Segeberger Zeitung vom 02.08.2005, <http://segeberger.nordclick.de/news/archiv/?id=1688548>.

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

67 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.

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.

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 Dammbbruch 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“ wird 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 wird. 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 wird das Beispiel der Vorratsdatenspeicherung Schule machen. Die Vorratsspeicherung von Flugreisen und Nahverkehrsfahrten, von Fahrzeugbewegungen auf Autobahnen, von Aufzeichnungen privater Überwachungskameras, 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 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 des Betroffenen, dem aus der Aufbewahrung personenbezogener Daten schwere Nachteile entstehen können.

e) Ergebnis

Eine Vorratsspeicherung der Telekommunikation bietet keinen verbesserten Schutz vor Kriminalität. Die Strafverfolgungsbehörden würden nur einen kleinen Bruchteil (etwa 0,0004%⁶⁸) der gespeicherten Kommunikationsdaten jemals nachfragen, während mehr als 99% der von einer Vorratsspeicherung Betroffenen unschuldig wären.⁶⁹ Eine solche Maßnahme kann nicht mehr als verhältnismäßig angesehen werden.⁷⁰ Das Bundesverfassungsgericht wird dementsprechend die §§ 110a, 110b TKG-E für verfassungs-

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

69 Schaar, <http://www.heise.de/ct/aktuell/meldung/62231>.

70 Bäumler/v. Mutius-Bäumler, Anonymität im Internet (2003), 8; 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); 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

widrig erklären, wenn sie Gesetz werden. Der Entwurf einer entsprechenden Verfassungsbeschwerde, verbunden mit einem Antrag auf einstweilige Aussetzung des Gesetzes wegen offensichtlicher Verfassungswidrigkeit, liegt bereits vor.⁷¹ Schon mehrere tausend Bürger haben einen Rechtsanwalt mit der Erhebung der Verfassungsbeschwerde beauftragt.⁷²

In den nächsten Monaten ist überdies eine Entscheidung des Bundesverfassungsgerichts zur Vorratsspeicherung von Telekommunikations-Bestandsdaten (§§ 95 Abs. 3, 111 TKG) zu erwarten.⁷³ Diese Entscheidung wird wegweisend auch für die Verfassungsmäßigkeit des vorliegenden Gesetzesvorhabens sein.

Wir fordern, diese Entscheidung des Bundesverfassungsgerichts und die Entscheidung des Europäischen Gerichtshofs über die Wirksamkeit der Richtlinie 2006/24/EG abzuwarten, bevor ein massiver Grundrechtseingriff wie die Protokollierung des Telekommunikationsverhaltens der gesamten Bevölkerung beschlossen wird.

2. Anonymisierungsdienste

Der Referentenentwurf geht in Bezug auf Anonymisierungsdienste über die Richtlinie 2006/24/EG hinaus und widerspricht insoweit den Vorgaben des Bundestagsbeschlusses vom 16.02.2006.

Ausweislich der Entwurfsbegründung (S. 146) sollen auch Anonymisierungsdienste zur Vorratsdatenspeicherung verpflichtet werden. Dies ist in der Sache 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 betrifft Anonymisierungsdienste nicht. Dies wäre auch sinnlos, weil im Ausland betriebene Internet-Anonymisierungsdienste kostenfrei zur Verfügung stehen (z.B. „TOR“) und eine Vorratsdatenspeicherung in Deutschland ohne Weiteres umgangen werden könnte. 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“*.

Im Übrigen deckt der Wortlaut des § 110a TKG-E entgegen der Entwurfsbegründung Anonymisierungsdienste nicht ab. § 110a Abs. 1 TKG-E sieht eine Speicherpflicht nur „nach Maßgabe der folgenden Absätze“ vor, also nur für die in den Absätzen 2-6 genannten Dienste. Anonymisierungsdienste sind dort nicht aufgeführt. Insbesondere handelt es sich nicht um Internetzugangsdienste (§ 110a Abs. 4 TKG). Anonymisierungsdienste bieten keinen Internetzugang an, sondern setzen umgekehrt eine bereits bestehende Internetverbindung voraus. Erst nach Herstellung eines Internetzugangs über einen anderen Anbieter lassen sich Anonymisierungsdienste nutzen. Dass § 110a Abs. 4 TKG Anonymisierungsdienste nicht erfasst, ergibt sich auch daraus, dass „eine eindeutige Kennung des Anschlusses, über die die Internetnutzung erfolgt“ gespeichert werden soll (§ 110a Abs. 4 Nr. 2 TKG-E). Die Kennung des vom Kunden genutzten Telekommunikationsanschlusses steht aber nur dem Internetzugangsanbieter zur Verfügung und nicht dem Anbieter eines Anonymisierungsdienstes.

Wir fordern, die Anonymisierungsdienste betreffende Passage in der Entwurfsbegründung zu streichen.

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; für Bestandsdaten schon Rieß, DuD 1996, 328 (333).

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

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

73 1 BvR 1299/05, <http://www.tkg-verfassungsbeschwerde.de>.

3. Überschießende Speicherfrist

§ 110a 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: § 110a 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.

4. Eigene Auskunftregelung

§ 110b Abs. 1 S. 1 TKG-E sieht eine besondere Pflicht zur Auskunftserteilung über vorratsgespeicherte Verkehrsdaten vor. Ausweislich der Entwurfsbegründung (S. 150) ist dies aber nicht beabsichtigt.

Schon § 100g Abs. 2 S. 1 i.V.m. § 100b Abs. 3 StPO-E verpflichtet Anbieter zur Auskunftserteilung. § 110b Abs. 1 S. 1 TKG-E macht daneben nur dann Sinn, wenn er über § 100g StPO-E hinaus gehen soll. Dies aber wäre inakzeptabel, zumal schon § 100g StPO-E zu weit gefasst ist.

Somit ist § 110b Abs. 1 S. 1 TKG-E überflüssig. Es gibt auch keine vergleichbare Vorschrift für andere Verkehrsdaten oder für Inhaltsdaten. Die gesonderte Regelung von Erhebungsbefugnis und Auskunftspflicht widerspricht dem Gebot der Normenklarheit.

Wir fordern die Streichung des § 110b Abs. 1 S. 1 TKG-E.

5. Verwendung der Vorratsdaten

§ 110b Abs. 1 TKG-E beschränkt die Verwendung vorratsgespeicherter Daten im Wesentlichen auf Zwecke der Strafverfolgung.

Die Regelung mildert den massiven Grundrechtseingriff einer systematischen Vorratsdatenspeicherung zwar etwas ab, greift aber zu kurz. Die Vorratsdatenspeicherung erfolgt nach Art. 1 des Richtlinie 2006/24/EG nur für die Verfolgung schwerer Straftaten, weswegen konsequenterweise auch die Verwendung der gespeicherten Daten auf die Verfolgung schwerer Straftaten beschränkt werden muss. 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 Bagatelldelikten genutzt wird.

Für den Fall, dass die verfassungswidrige Vorratsdatenspeicherung überhaupt eingeführt wird, fordern wir, die Verwendung vorratsgespeicherter Daten auf die Verfolgung schwerer Straftaten zu beschränken.

6. Kosten der Vorratsdatenspeicherung

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

Die wirtschaftlichen Auswirkungen einer Vorratsdatenspeicherungspflicht sind enorm. Ihre Kosten werden etwa für Internetprovider auf einmalig 25 Mio. Euro und jährlich weitere zehn Mio. Euro Betriebskosten geschätzt.⁷⁴ Diese Zusatzkosten könnten die Internetnutzung für den Verbraucher um 15-20% verteuern⁷⁵ 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 gestellt 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

74 Rotert, <http://www.heise.de/newsticker/meldung/66367>.

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

führen, auch im internationalen Vergleich. Projekte wie FON, die zum Aufbau eines flächendeckenden Netzes kostenloser Internetzugänge in Deutschland führen sollten, stehen vor dem Aus.

Soweit die Begründung des Referentenentwurfs die Kostenschätzung eines großen Anbieters anführt, dürfte es sich um die Deutsche Telekom AG handeln, die die maßgeblichen Daten bereits heute speichert. Andere Anbieter von Internetzugängen speichern demgegenüber 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.⁷⁶

Die Verfassungsgerichte Österreichs und Frankreichs haben bereits entschieden, dass eine entschädigungslose Inpflichtnahme der Wirtschaft zu Strafverfolgungszwecken verfassungswidrig ist.⁷⁷ 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.⁷⁸

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 Referentenentwurfs 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. 145). 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 GlO). Diese Entschädigung deckt nur 2% der Kosten ab, die Telekommunikationsunternehmen durch ihre gesetzlich angeordnete Mitwirkung an der Telekommunikationsüberwachung entstehen.⁷⁹ Insbesondere eine Entschädigung für gesetzlich vorgeschriebene Überwachungsrichtungen und für sonstige Vorhaltekosten (z.B. Personalkosten) ist gegenwärtig ausgeschlossen (§ 110 Abs. 1 und Abs. 9 S. 2 TKG).

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.⁸⁰

Eine Verfassungsbeschwerde gegen den Ausschluss der Kostenerstattung ist anhängig.⁸¹

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

77 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.

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

79 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.

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

81 Initiative Europäischer Netzbetreiber (IEN), Pressemitteilung vom 10.11.2006, <http://www.ienerlin.de/resources/061110-PM-AKUE.pdf>.

VII. § 111 TKG-E [Daten für Auskunftersuchen der Sicherheitsbehörden]

1. Identifizierungspflicht für Telefon, Handy und E-Mail (§ 111 Abs. 1 TKG)

§ 111 Abs. 1 TKG zufolge setzt die Nutzung eines Telefon- oder Handyanschlusses sowie künftig auch eines E-Mail-Postfachs 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 E-Mail-Diensten).

Das Grundgesetz lässt solche Grundrechtseingriffe nur aus überwiegenden Interessen der Allgemeinheit zu. Hiervon kann bei der Identifizierungspflicht für Telefon, Handy und E-Mail 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.⁸²

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.

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

2. Zwangserhebung auch von E-Mail-Kundendaten und von Gerätenummern (§ 111 Abs. 1 S. 1 Nr. 5 und S. 3 TKG-E)

Die vorgesehene Erweiterung der Zwangserhebung von Bestandsdaten (§ 111 Abs. 1 TKG) auf die Gerätenummern von Mobiltelefonen und auf E-Mail-Dienste ist 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 Verfasser des Referentenentwurfs (S. 57): *„Zu berücksichtigen ist darüber hinaus, 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.“*

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.

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

Ernstzunehmende Kriminelle geben beim Kauf eines Mobiltelefons und 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 ausländischen E-Mail-Postfachs (z.B. Yahoo, Google), um die geplanten Regelungen zu umgehen. Diese sind mithin von vornherein untauglich. Sie schädigen im Wesentlichen nur die Privatsphäre unschuldiger Bürger, denen die Möglichkeit genommen wird, anonym per E-Mail 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 § 111 TKG der Warnung des Bundesverfassungsgerichts, von einer neuerlichen Ausdehnung von Grundrechtseingriffen zulasten unbeteiligter Dritter abzusehen.⁸³

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. 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 (§ 110a TKG-E). Zur Begründung wird auf die obigen Ausführungen Bezug genommen (Seite 22). 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, ansonsten jedenfalls die Beschränkung der Speicherdauer auf sechs Monate.

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

Der Ausschluss einer Entschädigung für die Vorratsdatenerhebung ist verfassungswidrig. Auf die diesbezüglichen Ausführungen zu § 110a TKG-E wird verwiesen (Seite 27).

VIII. §§ 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 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.

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

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.⁸⁴ 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.

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 § 110b 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 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.

IX. § 150 TKG-E [Übergangsvorschriften]

1. Recht zur Vorratsdatenspeicherung im Internetbereich (§ 150 Abs. 11a 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.

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 inakzeptabel, dass ohne Umsetzungspflicht schon vor dem 15.03.2009 eine Vorratsspeicherung im Internetbereich erlaubt werden 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.

Wenn überhaupt eine Vorratsdatenspeicherung beschlossen wird, fordern wir, dies im Internetbereich erst ab dem 15.03.2009 zu erlauben.

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.

84 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.

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

Der Entwurf eines Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums räumt Rechteinhabern zur zivilrechtlichen Verfolgung von Urheber- und anderen Rechtsverletzungen einen Auskunftsanspruch gegen Telekommunikationsunternehmen ein.

Dieser zivilrechtliche Auskunftsanspruch ist im Zusammenhang mit dem vorliegenden Gesetzesentwurf relevant. § 110b TKG-E beschränkt nämlich nur die Verwendung vorratsgespeicherter Verkehrsdaten auf Zwecke der Strafverfolgung, nicht aber die Verwendung vorratsgespeicherter Bestandsdaten. Eine Vorratsspeicherung von Bestandsdaten sieht § 111 TKG-E vor, indem er die Erhebung und Speicherung betrieblich nicht erforderlicher Bestandsdaten anordnet. Eine Vorratsdatenspeicherung für rein staatliche Zwecke erfolgt insbesondere bei vorausbezahlten und kostenlosen Diensten (z.B. Prepaid-Handykarten, kostenlose E-Mail-Konten).

Der Gesetzesentwurf des Bundesjustizministeriums zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums⁸⁵ soll Telekommunikationsanbieter nun verpflichten, an Inhaber von Patent-, Urheber- und anderen Rechten Auskunft über die Bestandsdaten ihrer Kunden zu erteilen, wenn dies zur Verfolgung von Rechtsverletzungen erforderlich ist. Dazu ist dazu Folgendes anzumerken:

1. Fehlende Beschränkung auf anhängige Gerichtsverfahren

Erstens sieht die umzusetzende Durchsetzungsrichtlinie zur Gewährleistung der Privatsphäre der Betroffenen und der Verhältnismäßigkeit eine Auskunftserteilung ausdrücklich nur im Rahmen gerichtlicher Verfahren und auf gerichtliche Anordnung vor.⁸⁶ Der deutsche Gesetzesentwurf verzichtet demgegenüber auf diese Einschränkungen und will jede „offensichtliche Rechtsverletzung“ genügen lassen. Zur Begründung heißt es, „*dass Rechteinhaber durchaus ein berechtigtes Interesse auf Auskunft haben können, um den Verletzer überhaupt erst ermitteln zu können.*“ Rechteinhabern 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.⁸⁷ wie auch das Oberlandesgericht Hamburg⁸⁸ eine Auskunftspflicht von Internet-Zugangsvermittlern verneint. Allenfalls, wenn schon ein gerichtliches Verfahren gegen den Verletzer anhängig ist, ist ein Auskunftsanspruch angemessen. So regelt es auch die Durchsetzungsrichtlinie. Ein allgemeiner Auskunftsanspruch würde dazu führen, dass Verbraucher mit Abmahnungen und Prozessen überzogen werden, wenn sie – selbst unabsichtlich – eine „offensichtliche Rechtsverletzung“ begehen.

Aus dem Entwurf muss daher die Passage „In Fällen offensichtlicher Rechtsverletzung oder“ gestrichen werden, 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).

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-Zugangsprouder 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

85 <http://www.urheberrecht.org/topic/enforce/bmj/2006-01-03-DurchsetzungsG-E.pdf>.

86 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 wahren Antrag des Klägers hin anordnen können, dass Auskünfte [...] erteilt werden [...]“.

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

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

vor, beschränkt die zulässigen Verwendungszwecke aber auf die Verfolgung von Straftaten (§ 110b TKG-E). Der zivilrechtliche Auskunftsanspruch macht hier also ebenfalls keinen Sinn.

2. Fehlende Beschränkung auf gewerbsmäßige Rechtsverletzer

Weiter heißt es in der Entwurfsbegründung: *„Der Drittauskunftsanspruch setzt nicht nur voraus, dass die Mitwirkungshandlungen des Dritten ein gewerbliches Ausmaß erreicht haben. Vielmehr muss auch die Rechtsverletzung selbst in gewerblichem Ausmaß begangen worden sein.“* (S. 78). Diese Einschränkung ist richtig und notwendig. Man sucht sie im Gesetzestext aber vergeblich. Der vorgeschlagene Gesetzestext lässt 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.

Im Gesetzestext muss daher klargestellt 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“. (§§ 140b Patentgesetz-E, 24b Gebrauchsmustergesetz-E, 19 MarkenG-E, 101 UrhG-E, 46 Geschmacksmustergesetz-E, 37b Sortenschutzgesetz-E).

19. Januar 2007

Arbeitskreis Vorratsdatenspeicherung

Netzwerk Neue Medien e.V.

Neue Richtervereinigung e.V.